# Surveillance Law in Africa: a review of six countries

# Senegal country report

Ridwan Oloyede

DOI: 10.19088/IDS.2021.059

# Introduction

Different countries deploy surveillance and interception of communications to combat crimes and ensure national or economic security (Chris 2005). The emergence of serious crimes such as terrorism has increased governments' appetite to conduct communications surveillance. The United Nations (UN) Human Rights Council defines communications surveillance as, 'the monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks' (UNHRC 2013). Nonetheless, government surveillance must meet the minimum human rights standards and individuals must be protected against arbitrary interference with their right to privacy (Privacy International 2018a). Unfortunately, failure to adhere to these human rights norms and principles could erode the rights to privacy, expression and assembly (Media and Democracy 2016).

Senegal, a former French colony, has enjoyed an uninterrupted constitutional democracy since independence in 1960, compared to neighbouring countries (Freedom House 2021). The Constitution of Senegal guarantees the right to privacy of communication and prohibits surveillance. However, violations of these rights by the government have been reported (Amnesty International 2020). Senegal has adopted a series of international human rights instruments that reinforce these guarantees (Claiming Human Rights 2011). According to the explanatory statement of Intelligence Services Law, 'intelligence must play a vanguard role in the national security system'. Nonetheless, there have been documented instances of state use of surveillance capability.

A report by non-profit association OSIRIS cited instances of citizens' conversations on telephone lines being monitored (Osiris 2021). In 2010, the United Sates (US) Department of State reported that illegal telephone monitoring by security services was common practice in Senegal. However, the threat of terrorism and availability of digital technologies has provided new impetus to monitor communications (US Department of State 2011). The Government of Senegal has used insecurity around the Sahel region as a reason to introduce internal security legislation (Counter Extremism Project 2020). In addition, a military expedition against the separatist movement in the country's Casamance region has added to the mix of violence confronting the country (Africanews 2021). These perceived threats led the government to amend the Penal Code and Code of Criminal Procedure, creating new terrorism-related offences, increasing the powers of investigating authorities (Amnesty International 2016), legitimising interception of communications and imposing stiffer penalties

for terror-related activities and unlawful interception (Lequotidien – Journal d'information Générale 2017). There are plans to amend both laws further to address terrorism (BBC News Afrique 2021).

In 2016, Senegalese authorities arrested 11 people linked to Nigerian-based terror group Boko Haram, including one individual, Momodou Ndiaye, who was reported to have been tracked through his activities on Facebook (Reuters 2017). 'In 2016, Senegalese authorities also arrested Moustapha Diatta, who ran a Facebook page called 'Proselytise Senegal'. Diatta reportedly helped Senegalese individuals – including three of his children – travel to Libya to fight for ISIS'[1] (Institute for Global Change 2017).

Beyond security threats, other factors are driving wider adoption of surveillance in Senegal. The European Union (EU) is funding a national biometric identity programme worth €28 million to control immigration (Privacy International 2018b). The grant is part of the EU's Emergency Trust Fund for Africa, which was launched in 2015 to stop 'irregular' migration, 'enforcing the rule of law through capacity building supporting security and development and law enforcement, including border management migration-related aspects' (Privacy International 2020). According to telecommunications company Orange's Transparency Report on Freedom of Expression and Privacy Protection in 2016, the Senegalese government made the second-highest number of customer data interception surveillance requests in Africa (Orange 2017).

Senegal has mandatory requirements to register mobile device SIM cards (Privacy International 2019a). The mandatory requirement to register SIM cards erodes anonymity and negatively impacts the right to privacy of communications. Senegal has also been accused of purchasing FinFisher surveillance malware capable of monitoring communications (Privacy International 2015). Some laws allow the government to carry out surveillance, enable monitoring capability and increase investigatory powers.

This report looks at these laws and evaluates them against the UN Draft Legal Instrument (2018) on state surveillance, which allows targeted surveillance. The report sets out how the laws apply in practice and concludes with specific recommendations for different stakeholders. The remainder of this report is organised as answers to 12 questions about surveillance law in Senegal.

1 Islamic State of Iraq and Al-Sham – a global terrorist group responsible for attacks in many parts of the world.

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

Like many other countries, the Senegalese government's primary driver for surveillance is national security, according to the explanatory statement of the Law on Intelligence Services. Increasing terrorism activities in neighbouring countries and the Sahel region, and insurrection in the country's Casamance region, have also been drivers. As a result, the government enacted an anti-terror law that empowers law enforcement agencies to intercept communications. However, the state has reportedly used surveillance outside the legitimate purpose advanced by the government. For example, the government has reported purchasing surveillance tools to monitor citizens (The Africa Report 2020). Similarly, EU funding to control immigration has given the government a more comprehensive capability to monitor people (Privacy International 2019c). Health and disease surveillance was also deployed to combat the coronavirus (Covid-19) pandemic when the government declared a state of emergency and conducted contact tracing (DHIS 2 2021).

# 2. Which international conventions protecting privacy has Senegal adopted?

The country has ratified or signed several international instruments, some of which are listed below.

a. **African Charter on the Rights and Welfare of the Child (1999)**

Article 10 of the charter guarantees African children's right to privacy. Accordingly, a Senegalese child enjoys the protection of the law over their communications and correspondence, which cannot be unduly interfered with.

b. **Universal Declaration of Human Rights (1948)**

Article 12 provides that no one should be subjected to arbitrary interference in their privacy and correspondence. Thus, all Senegalese enjoy legal protection against such arbitrary interference.

c. **African Union Convention on Cybersecurity and Protection of Personal Data (Malabo Convention) (2014)**

The convention establishes a baseline for legislation to protect personal data in Africa. Senegal is a signatory and although it is one of the African countries that ratified the Malabo Convention early, the convention has yet to take effect because it requires ratification by 15 countries; it has only been ratified by ten (African Union 2021).

d. **Economic Community of West African States Supplementary Act on Personal Data Protection (2010)**

The act creates a legal framework for the protection of personal data in the subregion. Senegal is a signatory to the act.

e. **International Covenant on Civil and Political Rights (1966)**

Article 17 of the covenant protects Senegalese citizens from arbitrary and unlawful interference with their communications and correspondence.

f. **Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Modernised Convention no. 108) (1981)**

The convention provides a framework for the protection of personal data. It is the only binding data protection instrument globally and Senegal has acceded to the instrument.

g. **Convention on Cybercrime of the Council of Europe (Budapest Convention) (2001)**

The convention is the only binding international instrument on cybercrime. It prescribed the framework for countries to legislate on cybercrime. Article 21 of the convention provides for the interception of content data. Therefore, countries should adopt the legislation necessary for severe offences to empower their competent authorities to intercept content data. The power to intercept is subject to article 15 of the convention, which prescribes that countries should adopt safeguards.

### Other international commitments

Senegal is also committed to the African Charter on Human and Peoples' Rights, which established the African Commission on Human and Peoples' Rights (ACHPR), a quasi-judicial body responsible for the protection and promotion of human and peoples' rights. The ACHPR reviews the state's reports concerning its human rights situation and decides on complaints of alleged violations. Additionally, Senegal has accepted the jurisdiction of the African Court on Human and Peoples' Rights to hear complaints presented by the commission (International Justice Resource Center 2017).

These international commitments set out established principles that guide the Senegalese government. Article 79 of the Constitution of Senegal stipulates that international law takes precedence over domestic law. Consequently, international human rights instruments are part of the domestic law of Senegal and take precedence over any discriminatory state law (Privacy International 2013). Consequently, there is a solid legal framework that protects the privacy of communications and correspondence from arbitrary and unlawful interference by the government or any other entity.

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

a. **Constitution of Senegal 2001**

Article 13 of the Constitution of Senegal establishes the right of citizens to privacy, stating that 'the secrecy of correspondence and electronic communications is inviolable. A restriction on this inviolability can only be ordered following the law.' This is in accord with the recommendation of the International Principles on the Application of Human Rights to Communications Surveillance that any surveillance that interferes with the right to privacy must be expressly allowed and defined in law (EFF 2014).

b. **Intelligence Services Law 2016**

Article 10 defines a limited number of 'legitimate aims' for surveillance, such as the threat of terrorist attack. The law makes it possible for Senegal's special intelligence services to conduct surveillance if there are no other ways to address the threat. In such cases, Article 10 makes it legal to resort to technical, intrusive surveillance or location procedures to gather valuable information to neutralise the perceived threat. Similarly, Article 8 provides that investigating entities may, with authorisation from and under the control of a competent public prosecutor, resort to the means of investigation under Article 10. The evidence duly collected by these means is admissible in court and is left to the discretion of the competent criminal court. Article 9 stipulates that in executing their mission, intelligence services must have recourse to the legality of the means employed and proportionality to the seriousness of the threat. This is consistent with the international principle of proportionality. Article 14 provides that an administrative body will be responsible for controlling the activities of the intelligence services. The public prosecutor is designated as the administrative oversight authority; there is no judicial intervention or oversight as prescribed under the International Principles.

c. **Protection of Personal Data Law 2008, and Decree Concerning Law Enforcement 2008**

Article 1 sets out the objective of the law, which is to protect the right to privacy. Article 35 prohibits the misuse of personal data. The law also creates specific obligations on public and private authorities to implement data protection principles. Significantly, data-processing activity must be lawful. The law established the Data Protection

Commission (CDP), which acts as the data protection authority responsible for enforcing the law. The law puts in place safeguards to preserve data protection rights, but allows derogations in cases of public interest, national security or investigation of crime, as contained in Article 40 of the Decree.

### d. Code of Criminal Procedure Law 2016

Combatting terrorism was set out as the legitimate aim of the legislation. Article 90-2 empowers the investigating authority to search computer systems if it is essential for investigating a crime. However, the search is subject to international commitments in force in Senegal. Articles 90-4 and 90-17 empower the investigating authority to decrypt encrypted data for investigation. According to Amnesty International,

> these articles are loosely worded and appear to extend the investigative judge's powers of investigation beyond specific data concerning a targeted individual allegedly linked to the criminal activity in question. These powers seem to extend to the very functioning of the computer system, which compromises all the data relating to it.
> (Amnesty International 2016)

Article 90-16 empowers the investigating authority to conduct interception of communications under a judicial authorisation. The order must specify the communications to be intercepted, the offence motivating the interception and the duration of the interception The planned investigative measures must be proportionate to the seriousness of the offence. However, the exercise of this power is not subject to judicial appeal.

Article 90-11 provides that if the necessities of the search for evidence so require, the investigating authority in the execution of a judicial directive may use appropriate technical means to collect or record in real time data relating to the content of specific communications transmitted using a computer system or oblige a service provider, within the framework of its technical capabilities, to collect or record computer data, or assist the competent authorities in collecting or recording the data. Article 90-10 permits the investigating judge for the purpose of investigation to direct the installation of software to intercept, which is contrary to the international principle of integrity of communications system.

e. **Code of Electronic Communications 2018**

Article 27 allows the government to oversee traffic management, surveillance and potential blocking of services. The code also expanded government oversight on intermediaries, which could lead to monitoring and violation of privacy rights. Article 36 of the code imposes the obligation on service providers to guarantee the privacy and data protection of users.

f. **Law on Cryptography 2008**

Article 12 provides that private individuals have the right to use encryption. However, its use is subject to the standard set by the National Cryptology Commission (NCC) (article 16). In such an instance, encryption is only permitted if the encryption key length is less than or equal to 128 bits. The NCC is responsible for setting the maximum length of encryption keys. The use of encryption with a longer key requires authorisation from the NCC (Global Partners Digital 2018). The purpose of encryption is to ensure the confidentiality of communications, which is guaranteed under the constitution. Individuals have an inviolable right to the privacy of their communications and private correspondence. However, this law appears to curtail the exercise of this law by imposing a limitation on the quality of encryption that individuals can use. In addition, the Code of Criminal Procedure empowers the investigative judge to decrypt encryption. Thus, while on the one hand, it appears to uphold the international principle of security of communications, it also creates a loophole to violate that right.

g. **Telecommunications Code 2011**

Article 7 mandates service providers to protect consumers' privacy and personal data, and it can only be waived by a provision of a law. Article 12 provides that,

> [a] judge or judicial police officer, for the needs of the prosecution or an investigation, or the enforcement of a judicial ruling, may require that telecommunications operators and service providers or telecommunications networks make available helpful information stored in the computer systems they administer. Telecommunications operators and service providers of telecommunications networks are required to submit the required information to the authorities.

The provision empowers the investigating authority to request that telecommunications companies make information on computer systems available to the investigating authority to investigate crime. In addition, the provision allows the authority to request the companies to grant access to communications. Nonetheless, the provision does not provide

other safeguards, such as notifying individuals that they are under surveillance, or clarify whether the powers apply to minor crimes or only the most severe crimes.

### h. Cybercrime Law 2008

Article 667-38 empowers the investigating authority to use appropriate technical means to record content data or specific communications in real time. Service providers are obliged to support investigating authorities in intercepting communications data. Article 677-36 allows the investigating authority to intercept communications data stored in Senegal that are important to an investigation. Disclosure under the law is subject to secrecy. The exercise of investigative power under these provisions is subject to the judicial supervision of an investigating judge.

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

Some African countries have been reported to engage in arbitrary mass surveillance (CitizenLab 2020). In addition, there are fears that several governments are procuring surveillance tools to monitor dissidents, political opponents, human rights defenders and journalists. Algeria, Botswana, Côte d'Ivoire, Egypt, Ghana, Malawi, Nigeria, Rwanda, South Africa, Tanzania, Uganda, Zambia and Zimbabwe were reported to have procured and deployed surveillance tools (Jili 2020). In July 2021, after a forensic investigation, the Guardian and other media outlets reported the use by some African countries such as Rwanda, Togo, and Morocco of Israeli company NSO Group's malware, Pegasus, which allows security agencies to listen to phone calls, intercept messages, and also to track individuals (Damien 2021). The malware has been reportedly used to spy on dissidents, opposition, journalists, and foreign leaders (Lynsey 2021). Although Rwandan and Moroccan governments have denied the claim (Kirchgaessner 2021, Shaquile 2021), in 2019, dissident and human rights activists from Rwanda and Morocco were privately warned by communication giant WhatsApp that they were victims of cyber-attacks designed to infiltrate their phones by an NSO Group malware (Kirchgaessner *et al.* 2019).

The pervasive practices appear to go unchallenged due to vague laws that are subject to abuse, codification of state power to conduct mass monitoring, the absence of independent oversight bodies, and weak legal frameworks and institutions. For example, in Uganda facial recognition has been deployed to monitor protesters (Quartz Africa 2020).

Nonetheless, there are examples of progressive practices on the continent. In South Africa, the Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA) is the primary law on surveillance. The RICA creates an oversight body and puts in place several safeguards contained under the International Principles. However, the law also omits some safeguards. The laws in Senegal and South Africa are silent on the role of transparency from investigating authorities (Privacy International 2019b). In addition, the RICA prohibits the disclosure of demands for communications data under the law, further hampering transparency. Furthermore, there is no statutory requirement to publish a public annual report. Finally, the laws in both countries omit the obligation to notify individuals that they are or have been under surveillance, denying

the targeted individuals the opportunity to challenge an interception or seek redress.

The laws in Senegal and South Africa have the requirement to specify the category of offence before requesting a judicial authorisation. There also appears to be a normative condition to establish a legitimate aim before conducting surveillance. However, some existing practice falls short of the requirement under the International Principles. For example, in 2021 South Africa's Constitutional Court delivered a landmark judgment outlawing mass surveillance in the country. In *Amabhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services (CCT 278/19),* the court held that the government should no longer conduct mass surveillance of citizens. The court also declared certain parts of the RICA unconstitutional (BusinessTech 2021). Notably, the court stated that the RICA fails to provide sufficient safeguards to preserve the right to privacy, the law did not provide adequate protection or relief for persons subjected to surveillance, and the law did not make provision for individuals subjected to surveillance to be notified after the fact, among other issues.

Nonetheless, South Africa has a specific surveillance law as suggested by the UN Draft Legal Instrument. This could be considered preferable to having contradictory legitimate aims and safeguards specified in different pieces of legislation. South Africa has a more explicit definition of tests for a judge to assess before issuing authorisation, which is not evident in the Senegalese framework. South Africa has an 'independent oversight board' as conceptualised under the International Principles. The law in South Africa also has the advantage of being challenged and tested in court by civil society in ways that have identified flaws, clarified provisions and provided enhanced privacy protections.

# 5. How does Senegalese surveillance law compare with the UN Draft Legal Instrument and international Principles

The existing legal framework in Senegal contains some of the elements suggested in the UN Draft Legal Instrument and the International Principles. For example, the Penal Code Law provides a safeguard against illegitimate access or interception by private entities: article 431-12 of the law carries a prison term of 1–5 years for unlawful interception of communications, which is consistent with the international principle of safeguards against illegitimate access. However, many elements are absent. These omissions relate mainly to the lack of safeguards and imprecise definitions, leaving the law open to abuse in the hands of a repressive government or officials.

Conversely, under the Code of Criminal Procedure, investigative measures must be proportionate to the seriousness of the offence and are subject to the necessity of investigation under the judicial supervision of an investigating judge. However, the exercise of power to intercept communications under article 90-16 of the Code of Criminal Procedure is not subject to appeal, which violates one of the principles of the UN Draft Legal Instrument: that, as soon as is practical, the subject of surveillance should be notified that they have been under surveillance and have the legal right to information and ability to appeal. The UN Draft Legal Instrument prescribes that the individual should be informed ahead of the surveillance activity to be able to contest it (except in specified urgent circumstances). The investigating authority is also expected to notify the CDP when there has been a data breach. Unfortunately, the Protection of Personal Data Law does not include the obligation to notify the CDP when there has been a data breach.

Requirements such as conducting a human rights impact assessment before deploying surveillance tools are not contained in any legislation. The law also enables the weakening of encryption and the cryptography law prescribes the standard of encryption. Furthermore, encryption is tied to freedom of expression and privacy; restricting the standard of encryption restricts these rights. According to the United Nations Educational, Social and Cultural Organisation (UNESCO), 'strong encryption is needed to protect privacy and freedom of expression in the digital age' (UNESCO 2016). Lastly, there is no requirement for transparency. For example, investigating authorities

are not required to publish a public annual report. As a result, much of the surveillance capability of the state is shrouded in secrecy.

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

Phrases like 'national security,' 'reasonable suspicion' or 'interception' are hardly defined or centred on respect for human rights. The Penal Code sets out prevention of terrorism as its legitimate aim. The failure to define these words leaves room for potentially arbitrary abuse. However, a semblance of how the terms should work is found in some laws. For example, the Code of Criminal Procedure sets out prevention of terrorism as a legitimate aim and provides context for what can be considered a severe crime under Article 90-16. The provision allows interception by investigating authorities:

> in felony matters, for a renewable period of four months; in misdemeanor matters when the minimum penalty is greater than or equal to five years' imprisonment, for a renewable period of four months; in a bid to investigate into the cause of death or disappearance, for a renewable period of two months; in the context of the search for a fugitive, for a period of two months.

Similarly, under the Code of Criminal Procedure, the interception decision must specify the offence, which has to be proportionate to the threat, and the duration of surveillance must be indicated.

The data protection law and the constitution impose the obligation to ensure the preservation of individuals' privacy and cannot be violated without a lawful basis. The constitutional guarantee is inviolable and serves as the basis to protect individuals against unwarranted surveillance. However, the constitutional provision is subject to derogations prescribed under a law. The Law on Intelligence Services allows for intrusive surveillance to neutralise a threat if it is the only means. Similarly, the Cybercrime Law allows surveillance for investigation of crimes. These legitimate surveillance aims are insufficiently defined. A constitutional provision cannot be considered inviolable if an official can waive it in the case of a petty crime or be justified concerning subjective issues of morality that are not defined in law.

Investigating authorities have an essential role in surveillance; they act based on judicial directives and supervision. However, under the Code of Criminal Procedure, decisions on interception are not subject to an appellate process. Therefore, notification of individuals ahead of surveillance is an effective tool to combat overreach but it is not required under any of the laws examined.

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

Under the International Principles, there are legal safeguards such as competent judicial authority, public oversight, transparency, and protection against illegitimate access. The role of independent oversight body is absent. There is no obligation or central oversight body concerning public disclosures of statistics on requests for and collection of communication data. Under the Law on Intelligence Services, the investigating authority determines what is proportionate to a threat and the decision is not subjected to a judicial decision-making process. Similarly, investigating authorities are not mandated to make public the details of legal requests or interceptions made. Safeguards such as conducting human rights impact assessments before deploying surveillance tools are not conducted. As a result, it is hard to know which law the government relies on to conduct surveillance. According to a report by the Association for Communications Progress (APC), 'the Government of Senegal never informs the population about how it concretely uses this legal framework of surveillance, a total opacity is maintained' (APC 2016).

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

The constitution and the law on the protection of personal data seek to protect individuals' privacy. Similarly, other laws reiterate the preservation of the right to privacy. The data protection law, for example, imposes many obligations on public and private authorities. This comprehensive data protection law covers the collection, processing, transmission, storage and use of personal data by legal entities under public or private law. In addition, Article 35 prohibits the misuse of data; and article 34 proscribes the collection of personal data without the knowledge of the data subject. The law also creates the obligation for public authorities to ensure data security, consistent with the international principle of the integrity of communications and systems.

Protection of Personal Data Law and the Decree Concerning Law Enforcement create derogations to the application of data protection law. Article 73 of the decree empowers a court to order necessary security measures in a period of emergency. Similarly, article 40 of the decree provides that the law will not apply to 'public security, defence, investigation and prosecution of criminal offences or the security of the State.' Similarly, the Protection of Personal Data Law empowers the CDP to impose administrative and penal sanctions for violation of the law. The Law on Cybercrimes provides a safeguard against illegitimate access or interception by private entities. Article 431-12 of the law carries a prison term of 1–5 years for unlawful interception of communications.

The state may carry out surveillance for legitimate aims such as preventing terrorism and other serious crimes (defined by the law). However, mass surveillance and monitoring of communications in violation of existing legal mechanisms and international human rights norms are considered intrusive, violating privacy and protection of personal data. Nevertheless, the Senegalese government is not transparent as it never informs the public how it uses the existing legal framework of surveillance in practice (GIS Watch 2014). This opacity is further reinforced by the lack of an obligation to publish public transparency reports on legal requests.

Despite a lack of resources, the CDP has been relatively efficient and transparent about its activities. It publishes a quarterly report highlighting its activities, which includes the number of public complaints on violation of

data protection rights received and resolved. However, the law was enacted in 2008 and has yet to be amended. It does not entirely address emerging modern concerns such as the requirement to conduct a data protection impact assessment, appointment of a data protection officer and data protection by design (Robertson 2020). Aside from these concerns, there are not sufficient safeguards around surveillance and the abuse and violations of rights that could accompany it. For example, the mandatory requirement to register SIM cards is not accompanied by sufficient data protection measures. According to a report by Privacy International, a non-profit watchdog (2019a):

> Mandatory SIM card registration laws require that people provide personal information, including a valid ID or even their biometrics before they can purchase or activate a prepaid SIM card for their mobile device. Such laws can allow the State to identify the owner of a SIM card and infer who is likely to be making a call, sending a message, in a particular location at any particular time.

There is no reference to users' right to access their data or to rectify errors in their data. Operators are not obliged to inform users of how their data are used or how they are processed. No information is given to users on the procedures for deleting their data when they change operators. The lack of sufficient safeguards could enable the government to monitor communications arbitrarily under the guise of maintaining security.

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

Senegal's biggest domestic threat is the security situation in the Sahel region, which has required it to strengthen counterterrorism measures. Similarly, the country is confronting an insurgency in the Cassmance region (Freedom House 2021). The legitimate aim advanced under the Penal Code and Intelligence Law is prevention of terrorism. The capacity to conduct surveillance is found under different laws, but it is not easy to ascertain which law is being relied upon. The Code of Criminal Procedure makes it a requirement to specify the purpose of interception and it must be proportionate to the threat.

In appraising necessity, the UN Draft Legal Instrument has established that surveillance measures being deployed must be necessary and they can only be carried out when there are no other, less intrusive measures that could secure the same legitimate aim (such as foiling a terrorist attack). Article 10 of the Law on Intelligent Services provides that intrusive surveillance can only be conducted if there is no less intrusive way to carry out the investigation. The weakening of encryption infringes on freedom of expression and the right to privacy.

Surveillance under the Code of Criminal Procedure requires prior judicial authorisation, and measures adopted must be proportionate to the severity of the crime, which is consistent with the international principle of proportionality.

The EU-funded digital identity programme has raised many privacy concerns. Biometric information is a unique identifier; when it is combined with other data such as financial transactions, mobile location, or facial and vehicle recognition technologies, the government has the opportunity to build an extensive surveillance capability. A repressive government could abuse the capability to weaken encryption to conduct surveillance on activists and political opponents. Crackdowns on the opposition have increased in Senegal in the past few years and formed part of the most recent election cycle in 2019 (Amnesty International 2021).

# 10. How has surveillance law played out in court in Senegal?

Unlike other African countries, Senegal has enjoyed a democratic transition without military interference. The courts have been mainly independent and adequately run. However, there has been no documented case challenging the state over conducting surveillance. This may partly be the result of the secrecy over government surveillance, which is reinforced by the absence of the requirement to publish a transparency report. According to a report, Senegalese authority used intelligence to monitor the movement and phone conversations of Muktar Diokhane, a Senegalese linked to Boko Haram. The report also stated that Senegal tracks open-source information and social media, and collaborates with 'French and Nigerien authorities on tracking and monitoring the phone calls of suspects' (Zenn 2018). Diokhane was sentenced to twenty years' imprisonment. The evidence presented before the court was gathered through intelligence. Although surveillance of Diokhane was not directly challenged, the case demonstrated an instance where evidence gathered through surveillance was used for prevention of crime.

The Law on Protection of Personal Data empowers the CDP to impose administrative and financial sanctions for violating the law. The Penal Code creates several offences for abuse and misuse of personal data. The code imposes varying prison terms and financial sanctions. Individuals who perceive their rights have been abused can approach the court for relief.

A report by non-profit association OSIRIS cited instances of citizens' telephone conversations being monitored (Osiris 2021). Similarly, a telecommunications company was also found to be monitoring employees' communications (EnQuete+ 2019). However, the provisions of the Code of Criminal Procedure make it impossible to appeal against the decision to intercept communications, which could encourage the invasion of Senegalese citizens' privacy (Cio Mag 2019).

# 11. What is working? What gaps exist in existing policy, practice, knowledge and capacity?

Senegal has a long-running history of uninterrupted constitutional democracy. Many provisions of laws enabling surveillance are consistent with the UN Draft Legal Instrument. For example, the Code of Criminal Procedure has as its defined legitimate aim the prevention of terrorism. It adds other safeguards such as establishing the severity of the crime, the duration of surveillance and proportionality of the seriousness of the threat before carrying out surveillance, consistent with the international principles of legitimate aim, proportionality and reasonable grounds. It also safeguards against unlawful interception by penalising unlawful interception with imprisonment term, which is consistent with the international principle of safeguards against illegitimate access.

Another key point is the existence of the data protection law and establishment of the CDP. In addition, though, there are plans to amend the data protection law. The role of judicial supervision in the process also represents a trust-building process.

Some of the gaps the report identified are the absence of transparency, with the absence of a requirement to publish a report on legal requests and lawful interception. The failure to designate an independent agency to hold law enforcement agencies to account under the Intelligence Services Law is another gap. In addition, the legal framework for surveillance is not clear on the requirement to notify individuals they are or have been under surveillance. Finally, additional safeguards, such as conducting a human rights impact assessment before deploying surveillance tools, are not contained in any law.

# 12. What recommendations arise from this analysis for legislation, policy, practice or further research?

**For the government**

- The government should promote citizens' trust by being open and transparent and ensuring that surveillance measures are proportionate and within the ambit of the law. The government should publish an annual transparency report on the volume of requests and authorisations and instances of surveillance should be available publicly or accessible to the members of the public.
- The government should conduct a human rights impact assessment before deploying surveillance tools.

**For policymakers and legislators**

- The laws on surveillance should be enacted into a single law as recommended in the UN Draft Legal Instrument.
- The law should mandate the investigating authorities to notify individuals who are subject or have been subjected to surveillance of such a decision and give them chance to contest it or appeal against it. Finally, investigating authorities should be mandated to publish the details of interception requests.
- There should be strict rules concerning the purchase and deployment of invasive surveillance technologies. A human rights impact assessment should be made a mandatory requirement before deploying surveillance tools.
- Service providers should be mandated to publish a transparency report periodically.
- The law on personal data should be amended to address the requirement to conduct a data protection impact assessment before deploying surveillance tools for surveillance.
- The budget of the CDP should be increased and it should be more autonomous from government institutions.
- Terms such as 'national security' and 'interception' should be defined to be anchored in respect and protection of human rights.
- The Code of Criminal Procedure should be amended to ensure respect for the rights to privacy and freedom of opinion and expression.

The amendment should require the lifting of encryption only for the investigation of the most severe crimes.

- The restriction on using encryption software should be removed. The use of encryption technology should be accessible to all individuals.

**For civil society and activists**

- Activists and civil society organisations should actively campaign for amendments to the law through engaging with policymakers.
- Strategic litigation should be used to clarify the law, narrow down targets of surveillance, and protect and safeguard citizens' rights. Also, civil society organisations should challenge intelligence services over violations of the law or existing human rights instruments that Senegal is party to.
- Activists and civil society organisations should work to raise public awareness about privacy rights, surveillance and available protections.

**For researchers**

- It is recommended that more research is carried out to reveal new evidence relating to the various tools, methods and tactics employed by the government to conduct surveillance.

**For journalists**

- Journalists and other media personnel should do a lot more to raise public awareness through reporting on surveillance practices and their effects. More research needs to be done to understand the categories and volume of cases in which surveillance data are used as evidence.

# References

Africanews (2021) ***Senegal Says Troops Overrun Rebel Camps in Casamance Region*** (accessed 5 July 2021)

Amnesty International (2021) ***Call for justice for the violent crackdown on #FreeSenegal protests*** (accessed 10 July 2021)

Amnesty International (2016) ***Analyse Des Lois Modifiant Le Code Penal Et Le Code De Procedure Penale*** (accessed 28 July 2021)

Amnesty International (2020) ***Amnesty International Report 2020/21: The State of the World's Human Rights*** (accessed 9 July 2021)

Association for Communications Progress (APC) (2016) ***Surveillance Numérique Pour Combattre Le COVID-19 : Opacité Gouvernementale Au Sénégal*** (accessed 5 July 2021)

BBC News Afrique (2021)***Loi Contre Le Terrorisme Au Sénégal: Pourquoi C'est Si Controversé?*** (accessed 5 July 2021)

BusinessTech (2021) ***South Africa's RICA Law Is Unconstitutional: Court Ruling*** (accessed 28 July 2021)

Chris, B. (2005) ***Surveillance and the Interception of Communications***, Transnational Institute (accessed 20 July 2021)

Cio Mag (2019) ***Sénégal: Des Risques d'Atteinte à La Vie Privée, Après l'Adoption de La Stratégie Nationale de Cybersécurité*** (accessed 5 July 2021)

CitizenLab (2020) ***Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*** (accessed 1 July 2021)

Claiming Human Rights (2011) ***Claiming Human Rights – in Senegal*** (accessed 9 July 2021)

Counter Extremism Project (2020) ***Senegal: Extremism and Terrorism*** (accessed 10 July 2021)

Damien, G. (2021) ***Morocco, Rwanda, Togo...How Involved Is Africa in 'Pegasus Gate'?*** The Africa Report (accessed 28 July 2021)

DHIS 2 (2021) ***Harmonisation Dans La Collecte de Données Pour Une Meilleure Riposte Contre La COVID-19*** (accessed 11 July 2021)

Electronic Frontier Foundation (EFF) (2013) ***International Principles on the Application of Human Rights to Communications Surveillance*** (accessed 5 July 2021)

EnQuete+ (2019) ***Les Enregistrements Téléphoniques Comme Moyens De Preuves : ''Illégaux'' et ''Irrecevables'', Selon Des Juristes'*** (accessed 9 July 2021)

Freedom House (2021) ***Senegal: Freedom in the World 2021*** (accessed 10 July 2021)

GIS Watch (2014) ***Communications Surveillance in the Digital Age*** (accessed 5 July 2021)

Global Partners Digital (2018) ***World Map of Encryption Laws and Policies*** (accessed 10 July 2021)

International Justice Resource Center (2017) ***Senegal Regional: African System*** (accessed 10 July 2021)

Jili, B. (2020) ***Surveillance Tech in Africa Stirs Security Concerns***, Africa Center for Security Studies (accessed 1 July 2021)

Kirchgaessner, S.; Hopkins, N. and Holmes, O. (2021) '**Hotel Rwanda Activist's Daughter Placed under Pegasus Surveillance'**, *The Guardian*, 19 July (accessed 29 July 2021)

Kirchgaessner, S; Hopkins, N. and Holmes, O. (2019) **'WhatsApp 'Hack' Is Serious Rights Violation, Say Alleged Victims'**, *The Guardian*, 1 November (accessed 29 July 2021)

Lequotidien – Journal d'information Générale (2017) ***REFORME – Modification Du Code Pénal et Du Code de Procédure Pénale : Amnesty International Met En Lumière Les 'Dispositions Liberticides'*** (accessed 10 July 2021)

Lynsey C (2021) ***Pegasus Lands in Africa*** (accessed 28 July 2021)

Media and Democracy (2016) ***Communications Surveillance and Privacy in South Africa*** (accessed 20 July 2021)

Orange (2017) ***Orange Transparency Report on Freedom of Expression and Privacy Protection*** (accessed 5 July 2021)

Osiris (2021) ***Écoutes et Espionnage Téléphonique au Sénégal/Une Pratique Sous Le Feu Des Radars : Outils De Dissuasion Ou Élément Redoutable Contre Les Infractions?*** (accessed 9 July 2021)

Privacy International (2020) ***Here is How a Well-Connected Security Company Is Quietly Building Mass Biometric Databases in West Africa with EU Aid Funds*** (accessed 9 July 2021)

Privacy International (2019a) ***Africa: SIM Card Registration Only Increases Monitoring and Exclusion*** (accessed 9 July 2021)

Privacy International (2019b) ***State of Privacy South Africa*** (accessed 10 July 2021)

Privacy International (2019c) ***The EU Funds Surveillance around the World: Here's What Must Be Done about It*** (accessed 11 July 2021)

Privacy International (2018a) ***Communications Surveillance*** (accessed 20 July 2021)

Privacy International (2018b) ***The EU's next Budget Threatens Privacy around the World for Decades to Come*** (accessed 10 July 2021)

Privacy International (2015) ***Ugandan Government Deployed FinFisher Spyware to 'Crush' Opposition, Track Elected Officials and Media in Secret Operation during Post-Election Protests, Documents Reveal*** (accessed 10 July 2021)

Privacy International (2013) ***The Right to Privacy in Senegal Stakeholder Report Universal Periodic Review 17th Session – Senegal*** (accessed 11 July 2021)

Quartz Africa (2020) ***Uganda Uses China's Huawei Facial Recognition to Snare Protesters*** (accessed 1 July 2021)

Reuters (2017) ***Senegal Arrests Three Suspected Foreign Jihadists*** (accessed 9 July 2021)

Robertson, T. (2020) ***Senegal to Review Data Protection Law, Collaboration on International ICT Policy for East and Southern Africa***, CIPESA (accessed 10 July 2021)

Shaquile, G. (2021) **'Pegasus Project: Morocco's Public Prosecutor Orders Probe into 'False Allegations''**, *Morocco World News*, 21 July (accessed 29 July 2021)

The Africa Report (2020) ***Inside Africa's Increasingly Lucrative Surveillance Market*** (accessed 9 July 2021)

Tony Blair Institute for Global Change (2017) ***Senegal, ISIS, and Al-Qaeda: A Terrorism Trifecta*** (accessed 10 July 2021)

US Department of State (2011) ***2010 Country Reports on Human Rights Practices*** (accessed 9 July 2021)

United Nations Educational, Social and Cultural Organisation (UNESCO) (2021) ***'Human Rights and Encryption'*** (accessed 10 July 2021)

United Nations Human Rights Council (UNHRC) (2013) ***Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*** (accessed 20 July 2021)

Zenn, J. (2018) ***'Boko Haram's Senegalese Foreign Fighters: Cases, Trends and Implications'***, The Jamestown Foundation (accessed 28 July 2021)