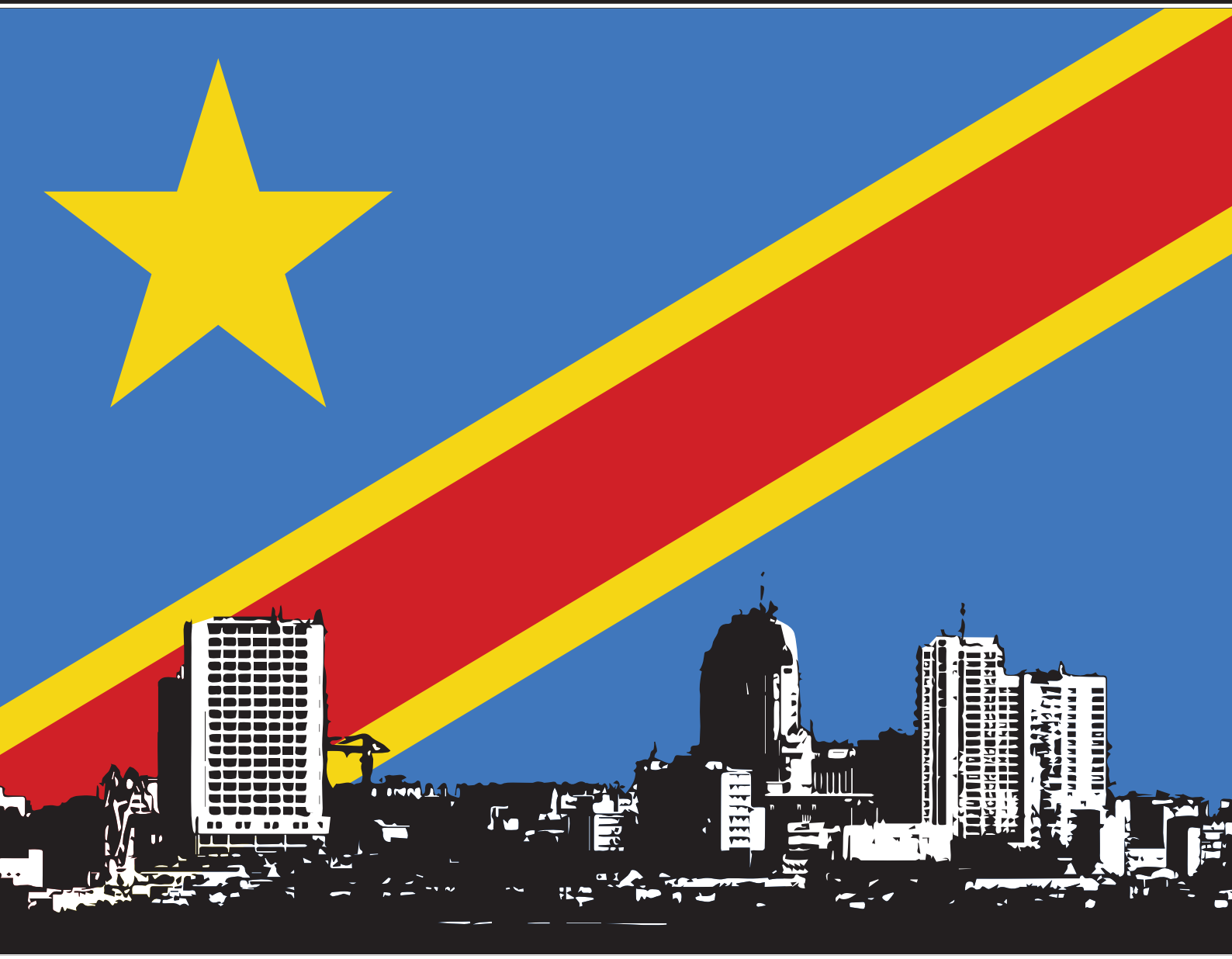
Surveillance of public spaces and communications in the Democratic Republic of the Congo



Arsène Tungali

May 2021

Surveillance of public spaces and communications in the Democratic Republic of the Congo

Arsène Tungali

This report was commissioned by the Media Policy and Democracy Project (MPDP). Supported by a grant from Luminate

The MPDP is a joint project of the University of Johannesburg's Department of Communication and Media and the University of South Africa's Department of Communication Science.

May 2021

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

List of Acronyms

ANR	National Intelligence Agency
CCTV	Close-Circuit Television
CIPESA	The Collaboration on International ICT Policy for East and Southern Africa
DEMIAP	Military Detection of Anti-Patriotic Activities
DGSN	General Directorate of the National Security
DRC	Democratic Republic of the Congo
FARDC	Armed Forces of the Democratic Republic of Congo
GNI	Global Network Initiative
ICT	Information and Communication Technologies
RFI	Radio France Internationale

Table of Contents

Introduction and background

This report is about the Democratic Republic of the Congo (DRC), the second largest country on the Africa continent, with nearly 85 million inhabitants. It draws attention to the practice of surveillance, focusing on surveillance conducted over public spaces as well as surveillance of personal communications.

Using a qualitative approach that included a literature review, policy and legal analysis as well as key personal interviews, this report aims to analyse the practice of surveillance in the DRC in terms of the law. It presents the legal environment as well as specific provisions in the law that do or do not justify these practices. It then looks at the main actors or state agencies involved in surveillance practices, and speaks about some of those actors and entities considered as targets of surveillance.

This report also provides facts on how telecom companies are participating in the surveillance of DRC citizens' personal communications. It also tries to understand the actual practice of surveillance versus available legal provisions, verifying the assumption that says there is generally a disjunction between the two in many countries.

Based on the findings of the research, the report concludes by presenting specific recommendations to different stakeholders, namely the government, the Parliament, civil society groups, and telecommunication companies, on how surveillance can best be used, while caring for citizens' rights, including their right to privacy.

Study rationale and justification

This is an exploratory research that aims at collecting and providing the necessary data to allow anyone willing to understand the practice of surveillance and how it is conducted in the DRC. It also aims at providing the necessary information to human rights activists to support their advocacy work, as well as to State authorities to encourage them to better regulate this sector and adopt up-to-date legislation that supports the practice of surveillance in the country.

With the hope that this report will help future researchers to have a starting point as they try to go deeper into specific issues that we have touched upon but not developed sufficiently, we therefore look forward to supporting any future work in this sector.

Methodology

This study employed a qualitative approach including a literature review, policy and legal analysis, and key respondent interviews. Reports of previous studies, online sources, media reports, academic works, government documents, and other literature were reviewed.

The literature review generated an understanding of the past and current debates, trends and issues in the DRC with regard to surveillance and data privacy. The analysis included a review of the political, economic, social, legal, technological and cultural contexts in which surveillance measures have been implemented in the DRC.

Some key respondents were chosen and approached for interviews, and their inputs helped to enrich and confirm the outcomes of the document analysis initially conducted and to give an idea about how citizens react to these surveillance practices. All of the respondents chose to stay anonymous.

The practice of surveillance in the Democratic Republic of the Congo

Overview of the telecoms, ICT, policy and legislative environments

The Constitution of the DRC, the law of laws, was first adopted in 2006, then updated in 2011 through Act No. 11/002 of 20 January 2011, revising certain articles of the DRC Constitution of 18 February 2006.[1] This Constitution is the supreme law and the main legal instrument from which most of the country's other laws, dealing with specific issues, take their source.

In the DRC, the postal, telecommunications and ICT sectors underwent their first reform of the legal and institutional framework in 2002, with the adoption and promulgation of Law No. 012/2002 on the Post, the Framework Law No. 013/2002 on Telecommunications, and Law No. 014/2002 creating the Regulatory Authority, all of them on October 16, 2002. This reform updated and improved the former framework of 1940 on telecommunications and that of 1968 on the Post Office.

On 25 November 2020, the Framework Law No 20/17 on Telecommunications and ICT was promulgated, almost three years after it was adopted by Parliament in May 2018. This law is intended to replace the Telecommunications framework of 2002 but is yet to come into full force because it has to be published in the Official Gazette. For the sake of this report, we will make reference to the 2002 framework (as the Telecommunications Act) which is still in force, although outdated and mostly focusing on the telecommunications sector, not taking into account the rapidly evolving ICT sector.

1 Democratic Republic of the Congo (2011). The Constitution of 2011. Available from: https://tinyurl.com/2d4xh8j2

Surveillance and the law

On the privacy of communications

The DRC Constitution guarantees citizens the right to privacy. Article 31 states, "Everyone has the right to respect for their private life and to the secrecy of correspondence, telecommunication or any other form of communication. This right may be infringed only in cases provided for by law." With this, the Constitution opens up the door to the legislature to define instances when this right may be infringed.

The Telecommunications Act is the supreme law in the sector, despite the fact that it was enacted in 2002; it speaks to this question as well through its different provisions.

Article 52 of the Telecommunications Act protects the privacy of correspondence. It states: "The secrecy of correspondence issued by telecommunications is guaranteed by law. This secrecy can be infringed only by the public authority, only in cases of necessity of public interest provided by the law and within the limits fixed by it."

The law goes on, giving more details about who is responsible of the protection of citizens' privacy and therefore banning surveillance of their communications. It is stated in Article 53 that "The public operators, concessionary operators of public telecommunications services and other providers of telecommunications services and members of their staff are obliged to respect the confidentiality of communications".

Article 54 gives clarity on what is forbidden by the law and provides that any interception must be authorised by the Attorney General of the Republic: "The interception, tapping, recording, transcription and disclosure of correspondence sent by means of telecommunications, subject to the prior authorisation of the Attorney General of the Republic".

Article 55 provides more context on circumstances which would authorise the Attorney General to perform any tapping; the law says: "Only information necessary for the ultimate manifestation of the truth in a judicial file may authorise the General Prosecutor of the Republic to prescribe the interception, recording and transcription of correspondence sent by telecommunication means".

As a complement to Article 54 authorising the Attorney General to grant interception rights and Article 55 clarifying under which circumstances, Articles 59 and 60 add another layer of authorisations, which include some specific government ministers as well as the intelligence services.

> *Article 59: "Exceptionally, interceptions may also be authorised for the interception of correspondence sent by telecommunications for the purpose of seeking information of interest to national security, safeguarding essential elements of the DRC's scientific, economic or even cultural potential, or preventing organised crime and delinquency".*

> *Article 60: "Authorisation is granted by a written and reasoned decision of the Minister in charge of Internal Affairs, based on a written proposal from the Minister in charge of Territorial Defense and Security or the Chief Intelligence Officer".*

One thing to note here is that the law does not clearly define what "national security" means, leaving it open for misinterpretation. Also, the law does not say whether this layer of authorisation applies to all interception applications.

On surveillance of public space

Neither the Constitution nor the Telecommunications Act explicitly mention or regulate the area of surveillance of public spaces by cameras or through video surveillance. The practice of video surveillance, in many countries around the world, is mostly run through CCTV (Close-Circuit Television) which is formed of four elements: cameras, video signal transmission lines, monitors that display the images and a recording device for storing the images.

In the DRC, the CCTV system has been adopted and is being used by banks, and other financial institutions, and is also used at airports, and on private properties (homes) such as at the main entrance, to better control entries and exits, etc. But what does the law say about this? Is this practice covered by the Congolese legislation?
Our research found no legal provision for the use of camera surveillance in public or private spaces. But what is known is that security agencies (such as the police) and intelligence services who are in charge of protecting citizens are implicitly allowed, as part of their duties and responsibilities, to install surveillance equipment.

Main actors engaged in surveillance practices

> *"Time has proven that in the DRC, the tate can contract the technical capabilities of whatever service or company, be it national or foreign, when it is about securing its citizens. There are a number of officially known state services (entities) and others who are not known but who have been involved in surveillance practices", said Franck (name changed), a Congolese telecommunications expert.*

This section focuses on a handful of national bodies that are reportedly involved in some form of surveillance or intelligence practices. Some are military focused whereas others are citizen focused, with a high potential of overlapping in their activities.

This section will try to understand how well their surveillance activities are backed by the law and whether these are part of their official mandate. The security and intelligence services that this section focuses on are:

- The Congolese National Police
- The National Intelligence Agency
- The DEMIAP.

No data is available to assess the capabilities or the technologies used by these three agencies. One would describe this as some state secrets!

The Congolese National Police

The Congolese National Police (referred to as the Police) was instituted by Decree No. 002/2002 of January 26, 2002 on the establishment, organisation and functioning of the Congolese National Police.[2]

As part of its mission, Article 5 says the following (emphasis mine): "The national police force is a force responsible for ensuring public security and tranquillity and for maintaining and restoring public order. It protects people and their property. Continuous surveillance constitutes the very essence of its mission."

It is clear here that the Police are responsible for "continuous surveillance", even if this decree law does not specify the remit of this surveillance nor does it speak much about how this is to be carried out.

2 Democratic Republic of the Congo (2002). - Decree- No. 002/2002 of January 26, 2002 on the creation of the National Police. Available from: https://tinyurl.com/sqjvjcn

When Article 25 says: "The national police are responsible for anti-terrorist operations in all its forms."; and further down, one reads the following in Article 26: "The national police assist the specialised bodies and services competent in this area in monitoring points of entry into the national territory, searching for illegal immigrants and usurpers of Congolese citizenship", it is no wonder the Police will use all possible means, including communication or public surveillance, in order to better counter terrorism in the country and to protect its borders.

Article 18 also states the following: "The national police are in charge of the traffic police. They maintain, at all times, communications and free passage and ensure free movement." With this, it is clear that the Police are responsible for any cameras that are installed on the roads and used for traffic control.

The National Intelligence Agency

Known in French as the Agence Nationale de Renseignement (ANR), this is the specialised state agency in charge of all intelligence activities in the country. The Agency has existed since May 1997 as a replacement of the former General Directorate of National Security (DGSN) that was responsible for security and intelligence under former President Mobutu.

On January 11, 2003, it was then instituted through Decree No. 003/2003, establishing and organising the National Intelligence Agency,[3] and putting it under the authority of the Head of State, as stated in Article 2 of this decree.

Article 3 speaks about its mission (emphasis mine): "Subject to other tasks conferred upon it and to be conferred upon it by specific texts, the mission of the National Intelligence Agency is to ensure the internal and external security of the State."

And further in the same article, point 3 speaks about its surveillance attribution: "… surveillance of national or foreign persons or groups of persons suspected of carrying out an activity of such a nature as to undermine State security". It is no wonder that here the Agency would use all possible means in order to rightfully carry out its duties and responsibilities.

The Agency has competence both on national and international levels through its various departments, one dealing with internal and the other with external security. The support department includes the "Centre for Telecommunications, Computing and Documentation", as stated in Article 13 of the same decree; which, although, not explicitly mentioned, obviously would be responsible for all digital or telecommunications related surveillance activities.

On its personnel, it is said in Article 22 that: "The agents and officials of the National Intelligence Agency shall, in the performance of their duties, have the right to special assistance and protection of their identity, their person and their property", which, as we will see in this report, gives them super power, linked to the fact the Agency is directly overseen by the Office of the President.

The DEMIAP

The Military Detection of Anti-Patriotic Activities, the DEMIAP, is the military intelligence section of the Armed Forces of the Democratic Republic of the Congo (FARDC). In 2003, it became the Military Intelligence (MI) workforce.[4]

The DEMIAP is officially under the authority of the Deputy Chief of Staff for Operations and Intelligence of the national army, FARDC. It is divided into two departments: internal (domestic) and external intelligence.

3 Democratic Republic of the Congo. Decree No. 003/2003 establishing the National Intelligence Agency. Available from: https://tinyurl.com/r7x3dk8

4 Wikipedia (2020). DEMIAP (Détection Militaire des Activités Anti-Patrie). Available from: https://en.wikipedia.org/wiki/DEMIAP

It is clear from the above that the army has an active intelligence service and therefore performs surveillance practices, mostly related to the armed forces and any military-related activities.

Targets of surveillance practices

As seen in this report, the various state agencies or services officially involved in surveillance and interception are mandated to do it in order to protect the state and its citizens.

As an example, it was said about the Police that, "…continuous surveillance constitutes the very essence of its mission", meaning that the Police will always be involved in surveillance practices in order to protect citizens and their belongings.

Article 24 of the decree establishing the Police also says, "The national police is specifically responsible for the custody and security of the heads of the constituent bodies and senior officials."; this would mean that they are supposed to ensure the security and safety of officials and therefore would be conducting surveillance activities on anyone who might be seen as dangerous.

Many human rights related reports rightly mention that a good number of measures that were taken during the last years of President Kabila's term were more directed towards protecting his contested presidency; therefore, a number of surveillance practices were directed at his political opponents in an attempt to control their movements, as we will see further in this report.

In the next section, we will mention various instances when security services have been involved in surveillance and interception practices, violating the law and the legal provisions in place in this area, and show that the law is weak and not explicit enough, leading to various interpretations of the same provisions.

Activism against surveillance in the DRC

Critics of the Telecoms Act of 2002

The Telecommunications Act, the main legal instrument governing the whole telecommunications sector, was enacted in 2002. It is focused on telecoms and speaks little about the information and communications technologies (ICT), and hardly covers issues such as cybersecurity, privacy and data protection and therefore, digital surveillance (or interception of private communications). One of the reasons for this is that in 2002 the ICT sector was less developed and the country had barely 1% internet penetration rate[5] as of the year 2000.

This legal framework has been criticised[6] by various digital rights activists as not being sufficiently explicit on some of its provisions, leaving them open to possible violations.

As an example, Article 52 guarantees the secrecy of emails sent through telecommunication services and says this privacy can be infringed in "only cases

5 CIPESA (2020). State of internet freedom – Democratic Republic of the Congo 2019: Mapping trends in government internet controls, 1999-2019. Available from: https://cipesa.org/?wpfb_dl=408

6 CIPESA (2016). State of internet freedom in the Democratic Republic of the Congo 2016: Charting patterns in the strategies African governments use to stifle citizens' digital rights. Available from: https://tinyurl.com/qu89epe

of necessity of public interest" but does not make explicit what "public interest" means or when this is applicable. Also, Article 55: "Only information necessary for the ultimate manifestation of the truth in a judicial file may authorise the General Prosecutor of the Republic to prescribe the interception…"; however, the phrase "ultimate truth" is open to misinterpretation and abuse.

This situation and similar instances were mentioned by civil society organisations (under the leadership of Rudi International) as part of their recommendations sent to the Senate in June 2018.[7] This effort was part of the public consultation on the draft Telecoms and ICT law that was then submitted for consideration to the Parliament and the Senate.

The Law was promulgated on 25 December 2020 but is yet to be published in the Official Gazette for it to be legally binding.

7 Rudi International (2018). The Congolese Senate received inputs to the Telecom and ICT draft bill. Available from: https://rudiinternational.org/2018/07/20/the-congolese-senate-received-inputs-to-the-telecom-and-ict-draft-bill/

The practice of digital surveillance in the DRC

On whether the law is followed, Justin one of our interviewees, who has consulted for the Congolese government more than once, said the following:

> *In a state where official documents are not always accessible and the unavailability of digital copies of many of these court orders or other correspondences; it is not obvious that one would be able to clearly assess whether the law was followed or official authorisations were granted when it is about surveillance of public spaces or interception of digital communications.*

In the DRC, terms such as "national security" that are mentioned in many legal instruments have led to a good number of procedural violations because, for national security reasons, everything may be done to preserve the peace and stability of the state. Many in power have used it as a reason to bypass some requirements and then justify their actions and activities as legitimate.

It also known that the Congolese government and other public authorities are making official requests to telecom companies for either interception or for customer data. The Orange annual Transparency Reports on Freedom of Expression and Protecting Privacy share more on this for many countries where they operate, including in the DRC.

In their 2017 report,[8] they share a definition of "interception" as being "legally sanctioned official access to private communications". And for Orange to carry out these requests, they share that the request must meet three formal requirements:

- The authority making the request must have jurisdiction to do so
- The request must be made via formal channels
- The request must comply with the country's laws and regulations.

In this report, which is a requirement as part of their membership to the Global Network Initiative (GNI), it was reported that in 2017 alone, they received 981 customer data requests from the DRC authorities (compared to 43 requests in 2014)[9] and 26 interception requests in 2017. This indicator corresponds to the number of requests from a range of stakeholders, such as governments, judicial authorities, or the police, for a variety of data, including call details, customer identification data, geolocation, billing and payment data.

8 Orange (2017) Transparency Report. Available from: https://www.accessnow.org

9 Orange (2014) Transparency Report. Available from: https://www.accessnow.org

It is also worth noting that a single request may relate to many customers, and one customer may be the subject of successive requests over the course of the year.[10] Lastly, Orange also mentions that their table does not show figures for some countries. In some cases, this is due to the policies and laws in place, while in other cases, the authorities may have direct access to the content of communications, regardless of the technique used. And this might be the case for the DRC.

Another type of surveillance is the one that is targeting activists and human rights defenders and is conducted over social media sites. Many of these have found themselves being sentenced to jail due to their opinions expressed on social media, mainly over Facebook, WhatsApp and Twitter, all platforms widely used in the Congo.

Prince Murhula, a Congolese journalist, wrote[11] about how political leaders have been trying to stifle dissent by invading specific WhatsApp chat groups in order to control what's being said there and, when needed, to influence the course of discussions to favour certain opinions over others.

In that article, Murhula quoted an official of the Intelligence agency affirming they had been instructed to invade chat groups on WhatsApp and be present on Facebook, who said:

> *Personally, I've integrated about a hundred groups on social networks. Sometimes I pretend to be a journalist, a civil society activist or a member of a pressure group. So, it's easy to know where such action should be done, who the leaders are, where and how to stop them.*

Such practices were mostly noted during President Kabila's regime, especially between 2016 and 2018, the period during which he was supposed to organise elections but doing all he could to stay in power beyond the official term.

Social media platforms were intensively used at the time, until political leaders found themselves being threatened and had to find a way to counter the rise of citizens, who were also using them to prepare public demonstrations and disseminate calls for protests. The Government started thinking of how they could limit the use of social media, and started accusing them of spreading fake news; therefore, this needed a form of regulation, leading to censorship. That's when they decided to go the radical way by shutting down the internet in the whole country,[12] the latest being the one that happened the day after general elections in December 2018, and lasted nearly 21 days[13].

It is worth noting that no Internet shutdown has been done under President Tshisekedi, who took power in January 2019.

Surveillance of public spaces

It was in January 2016 that the DRC saw a massive deployment of video surveillance equipment in the capital city, Kinshasa, as reported by RFI, the French radio.[14] Quoted in that article, the police chief in Kinshasa, Celestin Kanyama, explains that these would help reinforce the security of the city, ensuring drivers are responsible on the road as well as to counter unethical conduct of some inhabitants.

But given the timing of this deployment, many observers believed it was a strategy by former President Kabila, who was at the end of his constitutional presidential term, to get ready to stifle dissent by controlling all movement and public demonstrations.

10 CIPESA (2020). State of internet freedom – Democratic Republic of the Congo 2019: Mapping trends in government internet controls, 1999-2019. Available from: https://cipesa.org/?wpfb_dl=408

11 Murhula, P. (13 April 2020). Threat of freedom of speech over social media in DRC. *Jambo RDC*. Available from: https://tinyurl.com/twebq59

12 Tungali, A. The evolution of internet shutdowns in DR Congo. CIPESA. Available from: https://tinyurl.com/v5azcao

13 Al Jazeera (20 January 2019). DR Congo internet restored after 20-day suspension over elections. Available from: https://tinyurl.com/3fqc5crz

14 RFI (2016). Les Kinois réagissent à la présence de caméras de surveillance ». Available from: https://tinyurl.com/39yrfhvh

Speaking[15] about the practice of video surveillance in the DRC, Jerome Kengawe Ziambi, shares his analysis in an article published on the Think Tank DESC website by Jean Jacques Wondo, a renowned Congolese analyst of socio-political, security and military issues. Ziambi says: "Video surveillance directly affects the rights and freedoms of citizens, particularly privacy and freedom of movement." These rights are protected by the Constitution in its Article 31.

He further argues that, video surveillance violates the freedom of movement of citizens, which is protected by the Constitution in its Article 30: "… all persons within the national territory have the right to move freely." And he clarifies that no Congolese law provides for the cases of restrictions to these constitutional rules.

Ziambi concludes:

In a simplified manner and for the case concerning the DRC, this mechanism does not a priori have any criminological objective. It only aims to control the crowd during demonstrations against Kabila's power, to dissuade and frighten the population. Consequently, this video surveillance system will only be used by the police and the various services within the framework of the maintenance and restoration of public order.

No data is available about how effective this video surveillance practice was, but citizens in Kinshasa believe it was just a waste of money because this equipment is today no longer in evidence in the capital city of the country.

John (name changed) who was working in the Prime Minister's office at the time of the deployment of this equipment, said in an interview with us:" There was no legal decision taken, from our office side, to cover or justify the deployment of this video surveillance equipment, because it was just security authorities trying to do their job, in a more fashionable way".

Since there is no legal provision covering the area of video surveillance, this question has led activists to speak about the need for a law on data protection in the country, which is still non-existent.

"When you enter a bank, you notice there are cameras in place to control all movements. But none of the bank's customers ask about that video recording: who has access to it", commented Lucie (name changed), a Congolese digital rights activist. "I understand, this is for their internal usage, but what about those cameras you find at the border or those on the streets in Kinshasa? Who is managing them? Where is this collected data stored? Who has access to it? And for how long is it stored?" she demanded.

15 Ziambi, J.K. (n.d.). Installation de caméras de surveillance en RDC. Available from: https://tinyurl.com/y3newtm5

Conclusion

This study was commissioned in order to help understand how the practice of surveillance of public spaces as well as of communications is conducted in the Democratic Republic of the Congo, looking at whether this area is regulated by the law and whether legal provisions are followed in actual practice.

It used qualitative research which allowed us to conduct desk research including reading previous reports touching some of the aspects of interest to the research, and press and media publications. We also approached some key respondents; many of whom declined the invitation, and the few who answered some of our questions requested to be quoted anonymously.

The legal analysis brought to our attention the fact that both the Constitution of the DRC as well as the Telecoms Act, the main legal instruments in this sector, strongly speak about the necessity to protect citizen's privacy, with regards to their personal communications. They however give clear instructions on how any interception of citizens' communications should be conducted, including, through clear and legal processes, that involve the judiciary system. It has been noted that many provisions within these instruments, not only they are outdated, but are not clear enough, leading to any kind of misinterpretation.

The result of our research helped us understand that there is no legal instrument that regulate the surveillance of public services, including the use of cameras (such as CCTV) on public spaces, even though our interviews brought to our attention that at some point, cameras were installed in Kinshasa, used by the Police in order to fulfil their duties, which are to protect citizens. And that it is possible that there are many more that we cannot see. Not much was found on how effective their use was.

This led us to research on the main actors that are involved in surveillance practices in the DRC. These include the National intelligence service (ANR), the National Police as well as the DEMIAP, which is the specialised service of the army in charge of intelligence activities. Our research revealed that all of these services received specific missions, including the one to protect citizens by all means, including surveillance practices at their inception. Because there is no specific law that speaks of privacy and protection of personal data, this situation paves the way to all sorts of violations.

It has also been noted that political leaders have been using these state services at their own benefit, to conduct surveillance practices over their political opponents or as a way to stifle protest by surveilling opposition leaders' communications in order to understand their plans. These form the main targets of surveillance practices.

In order to solve the many issues found as part of this research, we have formulated bellow some specific recommendations to relevant stakeholders.

Recommendations

Several recommendations arise from the findings of this report, pertaining to the following entities in the DRC:

The government

Clearly define the roles and responsibilities of different actors involved in security and intelligence operations in the country. Put in place systems to better control their actions and punish those who may be tempted to use their power to violate citizens' privacy which is clearly protected by the supreme law, the Constitution.

Parliament

Update existing laws and adopt new ones that take into account the recent developments in the digital ecosystem, such as a law on privacy and protection of personal data. Use the role of control of public institutions and services that are misusing their legal prerogatives, undermining citizens' ability to enjoy the privacy of their communication as well as of their action. Parliament should also make sure the Telecommunications and ICT law is published in the Official Gazette for it to become legally binding.

Telecommunications companies

Follow the law and international standards into protecting their users' private communications and personal data. Refuse to attend to any illegal request by government institutions for users' personal data.

Civil society organisations

Continue playing their role of watchdogs, including monitoring the situation regarding surveillance in the country and raise the awareness of citizens as well as of political leaders, calling on everyone for the respect of citizens' human rights.

References

Al Jazeera (20 January 2019). DR Congo internet restored after 20-day suspension over elections. Available from: https://tinyurl.com/3fqc5crz

CIPESA (2016). State of internet freedom in the Democratic Republic of the Congo 2016: Charting patterns in the strategies African governments use to stifle citizens' digital rights. Available from: https://tinyurl.com/qu89epe

CIPESA (2020). State of internet freedom – Democratic Republic of the Congo 2019: Mapping trends in government internet controls, 1999-2019. Available from: https://cipesa.org/?wpfb_dl=408

Democratic Republic of the Congo (2003). Decree No. 003/2003 establishing the National Intelligence Agency. Available from: https://tinyurl.com/r7x3dk8

Democratic Republic of the Congo (2002). Decree No. 002/2002 on the creation of the National Police. Available from: https://tinyurl.com/sqjvjcn

Democratic Republic of the Congo (2011). The Constitution of 2011. Available from: https://tinyurl.com/2d4xh8j2

Murhula, P. (13 April 2020). Threat of freedom of speech over social media in DRC. Jambo RDC. Available from: https://tinyurl.com/twebq59

Orange (2014). Transparency Report. Available from: https://www.accessnow.org/transparency-reporting-index/

Orange (2017). Transparency Report. Available from: https://www.accessnow.org/transparency-reporting-index/

Rudi International (2018). The Congolese Senate received inputs to the Telecom and ICT draft bill. Available from: https://tinyurl.com/vpuenwr3

Tungali, A. (2017). The evolution of internet shutdowns in DR Congo. CIPESA. Available from: https://tinyurl.com/v5azcao

Wikipedia (2020). DEMIAP (Détection Militaire des Activités Anti-Patrie). Available from: https://en.wikipedia.org/wiki/DEMIAP

Ziambi, J.K. (n.d.). Installation de caméras de surveillance en RDC: Kabila le Big Brother raté. Available from: https://tinyurl.com/y3newtm5

Media Policy and Democracy Project

The Media Policy and Democracy Project (MPDP) was launched in 2012 and is a joint collaborative research project between the Department of Communication Science at the University of South Africa (UNISA), and Department of Journalism, Film and Television at the University of Johannesburg (UJ). The MPDP aims to promote participatory media and communications policymaking in the public interest in South Africa.

Visit mediaanddemocracy.com for more information.

This report was supported by a grant from Luminate.