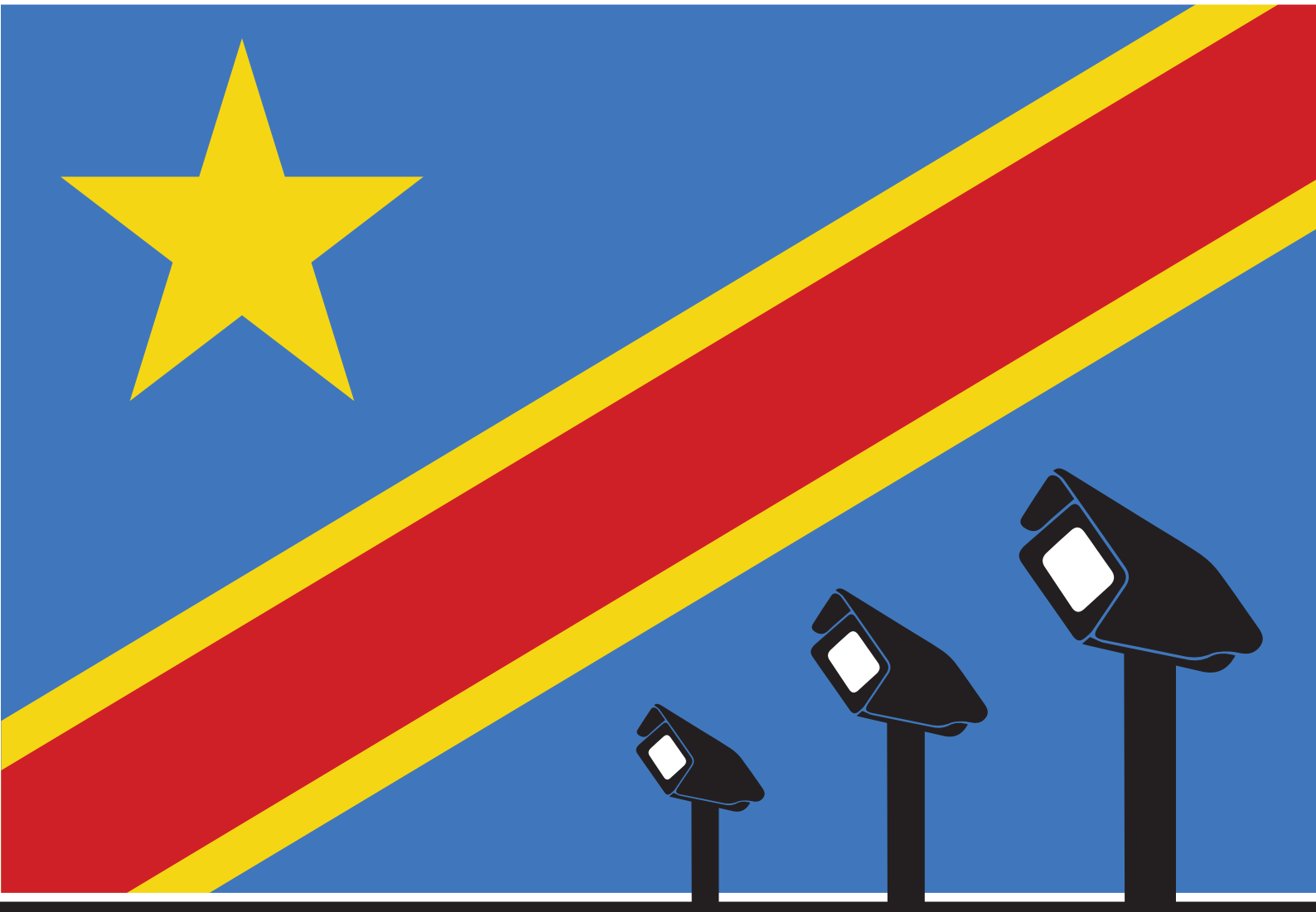
Digital Surveillance and Privacy in DRC: Balancing National Security and Personal Data Protection



Trésor Maheshe Musole
Jean-Paul Mushagalusa Rwabashi

December 2021

Digital Surveillance and Privacy in DRC: Balancing National Security and Personal Data Protection

A report for the Media Policy and Democracy Project by

Trésor Maheshe Musole
Jean-Paul Mushagalusa Rwabashi

Trésor Maheshe Musole is Professor of International Law at the Faculty of Law of the Université Catholique de Bukavu and Advocate at the Bar of Bukavu, Democratic Republic of the Congo.

Jean-Paul Mushagalusa Rwabashi teaches at the Université Catholique de Bukavu.

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 Studies and the University of South Africa's Department of Communication Science.

December 2021

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

Table of Contents

Acronyms and Abbreviations

ANR	Agence National de Renseignement
ARPTC	Autorité de Régulation des Postes, des Télécommunications et des Technologies de l'Information et de la Communication au Congo
CEIR	Central Electronic Identity Register
CSAC	Conseil Supérieur de l'Audiovisuel de la Communication
DEMIAP	Détection Militaire des Activités Anti-Patrie
DGM	Direction Générale des Migrations
DPS	Document de Politique Sectorielle (DPS)
FAI	Fournisseur d'Accès Internet
GEC	Groupe d'Étude sur le Congo
IMEI	Identité Internationale d'Équipement Mobile/International Mobile Equipment Identity
LUCHA	Lutte pour le Changement
MPDP	Media Policy and Democracy Project
NSA	National Security Agency (NSA)
NTIC	Nouvelles Technologies de l'Information et de Communications
ORM	Opérateur de Réseau Mobile
RAM	Registre des Appareils Mobiles/Mobile Device Registry
RDC	République Démocratique du Congo
RFI	Radio France International
RTNC	Radiotélévision Nationale Congolaise
UIT	Union Internationale des Télécommunications

Executive summary

This report explores the state of digital surveillance and privacy in order to locate a possible balance between national security and personal data protection in the DRC. The study describes and documents the actors, practices and targets of such surveillance and analyses their compliance with international human rights instruments binding on the DRC. It also identifies the perceptions of various actors of these practices and the means they have developed to counter this digital surveillance. More specifically, the study seeks to find out whether the Congolese state uses technological means of surveillance, the motive behind this use and its consequences. To this end, the study provides an overview of digital surveillance practices in the DRC, analyses the legal framework that underpins it, and the capacities of the actors involved, including state security services, telecommunications companies, states and foreign intelligence companies.

Based on a systemic analysis of texts and documents on digital surveillance, and qualitative data from interviews and focus groups with various actors and targets of digital surveillance in the DRC, the study revealed that despite the lack of an appropriate legal framework on digital surveillance, certain practices used by the authorities, communications companies, states and foreign companies constitute cases of intrusion into the privacy of individuals. These practices are multifaceted and include, among others, targeted wiretapping, blocking of websites, use of telecommunications companies and social networks and abuse of the courts to stifle dissenting voices.

This digital surveillance remains real in the DRC, notably though not only access to personal data but also to citizens' conversations. The ambiguity of the legal framework applicable in this area, especially Law No. 20/017 of 25 November 2020 on telecommunications and information and communication technologies and Decree-Law 003-2003[1] on the creation and organisation of the National Intelligence Agency (ANR), is further evidence of this. The exceptions provided for in these texts, based on reasons of public security, territorial defence or the interest of public service, lead the state authorities to carry out surveillance of citizens. For these reasons, the government of former President Kabila had equipped itself with various technological means, which allowed it to wiretap opponents and activists, especially during electoral periods characterised by a dizzying increase of human rights (GEC, 2018). Several international media, including RFI, TV5 and France 24, reported the involvement of Black Cube, a private Israeli intelligence company in carrying out this targeted surveillance since 2015. In addition, since May 2020, the government has been accessing certain network parameters of millions of mobile phones in order to collect International Mobile Equipment Identities (IMEI), through the Mobile Device Registry (RAM/MDR). In addition, cameras are used by some banking institutions to monitor their customers during deposit and withdrawal operations.

In general, the study shows that digital surveillance in the DRC, in all its forms, is contrary to the international human rights instruments ratified by the DRC. Indeed, while these instruments do not prohibit digital surveillance in principle, they make it subject to the principles of necessity and proportionality. Neither the Congolese legal framework nor the practices described meet this threshold. Based on the data obtained from the interviewees, the study formulates a series of recommendations addressed to the Congolese state (political, intelligence and administrative institutions), to telecommunications companies, to the victims of espionage practises, to civil society and to human rights NGOs for digital surveillance that reconciles national security and human rights.

1 DECREE-LOI No. 003-2003 on the creation and organisation of the National Intelligence Agency, available at https://www.leganet.cd/Legislation/Droit%20Public/Ordre/DL.11.01.2003.htm.

1. Introduction and background to the study

Currently, the rapid development of New Information and Communication Technologies (NICTs) has, in almost all countries, revolutionised all human activities. NICTs have been viewed as a powerful and indispensable tool for both companies and individuals to advance human progress. Once conceived as a working tool, particularly for the military and scientists, the Internet has now, thanks to the Web, become part of the daily life of hundreds of millions of people (Salvas, 2001; Camilla, 2020; Cornut St-Pierre, 2019; Sfetcu, 2020; Vuilleumier, (n.d.); Viana, 2021). The use of communication networks, and in particular the Internet, has enabled the deployment of unimaginable services while increasing the efficiency and accessibility of traditional services (De Terwangne, 2019). This importance is even more visible as the processing of personal data and the audience of social networks continues to grow at a considerable pace (APC and Hivos, 2014; Boenisch & Bigot, 2011; DCAF, 2019; Henno, 2016).

Therefore, technological and digital advances are being used by states to conduct preventive surveillance in the name of national security in general, and in particular, in the name of counterterrorism (Navarrete, 2015; Ndiaga, 2020; Forget, 2016; Vuilleumier, n.d.). To do so, they comb through written and oral communications on the Internet, telephone calls and postal mail. Indeed, the connection data, exchange information with foreign governments are collected and monitored for a search of premises. Public spaces are not exempt from this surveillance: cameras, sometimes equipped with facial recognition systems, are omnipresent (Sanija, 2021; Anissa, 2016; Agar, 2003; Ball, Haggerty, & Lyon, 2012; Larsen & Piché, 2009; Nicolas, et al., 2012). The fight against the pandemic in Covid 19 has made things even more complex. Several countries are using digital population technologies to stop the spread of the virus (Ndiaga, 2020; Viana, 2021).

Nevertheless, while it is undeniable that NICTs can be used for very positive purposes, they also carry very significant risks for human dignity, autonomy and privacy, as well as for the exercise of human rights in general, if not managed with the utmost care (UNHCHR, 2018; Castagnino, 2018; Abu-Laban, 2014; Amnesty International, 2021; Corentin, et al., 2018; Casilli, 2014). Indeed, the evolution of NICTs has narrowed the notion of privacy, especially with regard to the protection of personal data (Henri & Kalika, 2001; Maignien, 2012; Forget, 2016). This restriction is even more exacerbated in our era of the so-called "surveillance society" (Castagnino, 2018), marked by revelations in terms of spying practices in the service of states, corporations and individuals. These gained momentum on the night of 5–6 June 2013, when the British newspaper The Guardian made public the archives stolen from the National Security Agency (NSA) by the famous American whistleblower Edward Snowden, detailing in an unprecedented way the large-scale spying capabilities of the United States and the United Kingdom.[2]

In countries with "authoritarian" governance such as the Democratic Republic of Congo (DRC), digital surveillance is used as both a repressive and destructive lever of power. Indeed, having become independent in 1960, the DRC, like all other states in the world, is on the hunt for digital technology. Recent studies have shown that the use of NICTs is growing steadily. Indeed, with a population of 88.11 million and an urbanisation rate of 44%, the mobile penetration rate is estimated at 40%, internet penetration at 19% and 3.5% of active social media users (AE, TP, & Ritimo, 2020; CIPESA, 2016). The DRC has developed a Telecommunications Sector Policy document (DPS) since 2009 and plans to computerise all its services by 2030 and connect 90% of its population by 2050 (Plan national du numérique, 2019).

2 M. Untersinger, « Ce que les « révélations Snowden » ont changé depuis 2013 », *Le Monde*, 13 September 2019.

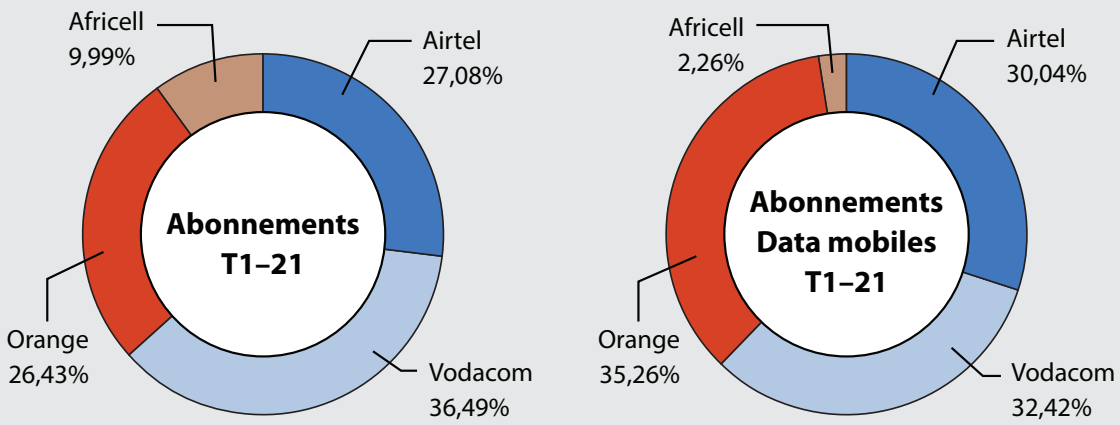
Studies reveal that state authorities, often assisted by foreign companies, "spy" on individuals though there is no appropriate legal framework for digital surveillance in the DRC, (CIPESA, 2016; AE, TP & Ritimo, 2020; Owenga, 2001; Harivel, 2018; Yende, et al., 2020). These states intercept not only personal data, but also and above all the conversations of citizens (AE, TP, & Ritimo, 2020; Owenga, 200; Yende, et al., 2020). In most cases, these processes are legitimised for reasons of national security. Decree-Law No. 003-2003 on the creation and organisation of the National Intelligence Agency (ANR) is one such example. According to its article 3, "the intelligence services (ANR) ensuring internal and external security of the State. Then, the surveillance of persons or groups of nationals or foreigners suspected of carrying out an activity likely to endanger the security of the State is listed among its attributions (Art.3.3)".

This broadly worded and ambiguous provision was used as leverage by the government of former President Joseph Kabila, which had wiretapped some political party officials, particularly those of the opposition in 2019 (AE, TP, & Ritimo, 2020; Murray & Admire, 2020).

Several international media outlets, including RFI, TV5, and France 24 revealed that a private Israeli intelligence company had spent many months investigating and wiretapping Congolese opposition officials. Moreover, since May 2020, the government has been accessing certain network parameters of millions of mobile phones in order to collect IMEI, through the Registry of Mobile Devices (RAM). More recently, revelations of spying on journalists, activists and politicians by some countries via the Pegasus software demonstrate the persistence of these practices. These various intrusions into private life reinforce the idea that governments are monitoring citizens, and restrictions in this regard are increasing.

In addition to state authorities, some private companies intervene or facilitate the surveillance of citizens' digital data. The most involved are often those operating in the telecommunications field. There are five telecommunication operators in the DRC: Vodacom, Airtel, Orange, Africell and Standard Telcom Congo (SA).[3] Four of them are mainly owned by foreign companies, respectively South African (Vodacom), Indian (Airtel), French (Orange) and American (for Africell). According to its report published in the first quarter of 2021, data from the Mobile telephone observatory, a structure of ARPTC (Regulatory Authority for Post and telecommunications in Congo), situate the overall penetration rate of mobile telephony at 47.1% and that of mobile internet at 24.6% (ARPTC, 2021). All of them offer call and data services, which gives them access to the personal data of their subscribers, i.e., 47.1% of the approximately 80 million Congolese. The following diagrams represent the percentages of internet and mobile phone subscribers by operator:

3 More details on https://www.stelecom.cd/.



Source: ARPTC report 2020, available at http://arptc.gouv.cd/wp-content/uploads/2021/09/ARPTC_Rapport-du-1er-trimestre-2021.pdf.

For example, the Orange company received up to 385 requests annually for personal customer information from the Congolese government. However, these statistics should be taken with caution, notably because many of these requests often go unreported. The requests include details of calls (duration, persons called, etc.), caller identification data (name, address, date of birth, etc.), customer GPS data, billing information, etc. (CIPESA, 2016). The monitoring carried out by banking institutions cannot also be put into perspective. Most of them use cameras to monitor their customers, usually during deposit and withdrawal operations. All these illustrations show that digital surveillance practises in the DRC are increasing, in the absence of relevant legislation to regulate such practices.

In 2020, after long hesitations on the part of the government in place since 2018, the DRC adopted new legislation in the field of telecommunications and new technologies, through Law No. 20/017 on 25 November 2020. Unlike the old legislation of 2002, this new text integrates a new dimension relating to the protection of privacy, particularly personal data. It applies to persons under public law and prohibits certain surveillance practices such as tapping, recording, interception, etc. Despite such innovations, the 2020 Act[4] has a limited scope of applications to surveillance practices in the field of telecommunications and information and communication technologies. Other practices, such as those related to surveillance cameras, are not covered by the law. Furthermore, the exceptions allowed by this law, especially for the benefit of certain services, often lead to arbitrariness.

This report explores the state of Digital Surveillance and Privacy: Towards a Balance between National Security and Personal Data Protection in the DRC. To do so, it first describes the actors and surveillance practices commonly used in the DRC. Then, the legal framework and its adequacy with regard to human rights are analysed. Finally, in the face of this shortcoming, the report proposes possible solutions that should make it possible to control surveillance practices and to make them part of the protection of national security and not to "spy" on citizens.

4 Loi n° 20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

2. Methodology

To achieve the results of our study, an appropriate, rigorous and operational methodological approach was put in place according to the state of the legal framework, the empirical findings, the theoretical orientation and the objectives. The entire methodological approach is based on the systemic approach (Donnadieur & Karask, 2002; Cambien, 2008); through the examination of Congolese legislation on digital surveillance and its conciliation with respect for privacy, the analysis of the desk review or existing literature is done through an analytical compilation of scientific works and reports from various state and private actors acting in this area. This analysis has made it possible to draw up a fairly exhaustive inventory of the issue, which was completed by empirical data from the actors involved.

Methods and techniques for collecting and analysing qualitative data through two main techniques were used in this field: individual interviews and focus groups. These techniques enabled us to deepen our analyses through the questionnaire survey, administered to the various targets during the individual interviews and focus groups. In total, five targets, divided into eighteen key informants, were interviewed (either through key individuals or in focus groups). They included state services working on security, telecommunications companies, political parties (three from the opposition and three from the presidential majority), citizen movements and the media. These targets were chosen mainly on the basis of their active (perpetrators) or passive (victims) involvement in digital surveillance. Except for the necessity of the category of actor, the questions in the individual interviews and focus groups were almost identical for the purpose of triangulating the information. The systemic analysis was imperative for us because of the need to determine and analyse the connection networks, the actors, their positions and practices around digital surveillance, and thereby identify possible solutions for digital surveillance that serves national security rather than spying on citizens.

For data processing and analysis, a compilation sheet was put in place which allowed us to capture the deeper meanings, the associations that exist between the respondents' views in relation to the themes of the exchanges in the individual interviews and the FGs, our content analysis being concerned with qualitative analysis. This then allowed us to isolate specific themes, words or concepts that appeared in a question that was discussed. The emphasis on the search for meanings of concepts and words by the speakers in the discussions facilitated the consideration of the context in which the concept was used. The compilation sheet (annexed below) provides information on how the information collected in the interviews and FGs was processed in order to facilitate a qualitative process of data processing. Following the interviews and FGs with each target group, specific categories were drawn up for the different discussion themes in the evaluation sheet, in addition to the compilation of a database of transcripts of the interviews and FGs.

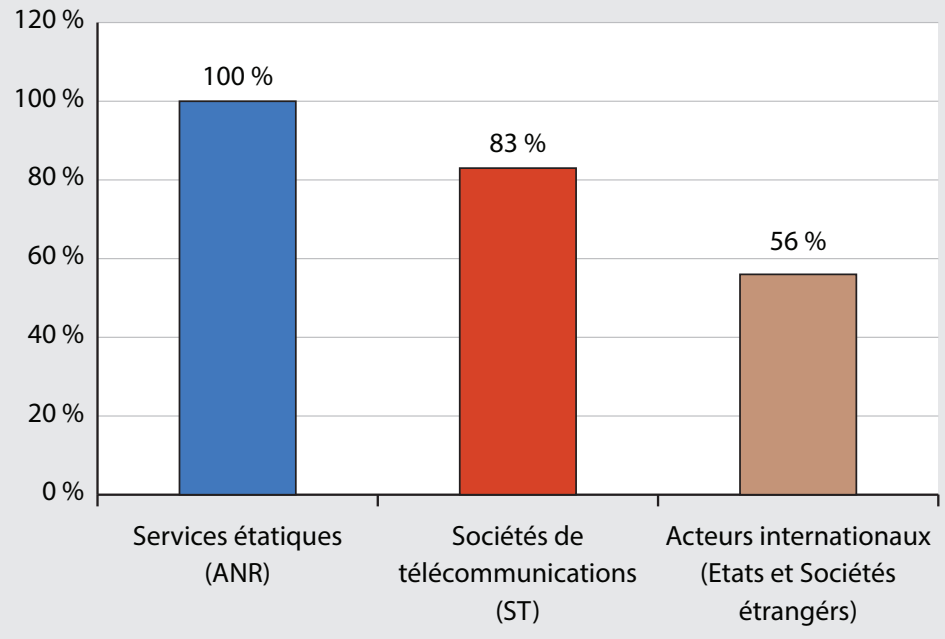
Finally, it is worth noting a number of difficulties encountered during these data collection processes, notably the reluctant cooperation of the telecommunications companies and the state security services. The latter required us to pre-file our survey questionnaire for review, to which some only provided responses after several days, while others did not even respond. This disrupted our research schedule from what we had originally planned.

3. Presentation of results

This section presents the results of our study on digital surveillance in the DRC. These results enabled us to identify the profile of digital surveillance actors in the DRC (3.1), to describe the usual surveillance practises (3.2), the tools of digital surveillance (3.3), to highlight the lack of awareness among victims of the existence of these practices (3.4), and to present the state of the legal framework that underpins these practices (3.5).

3.1 Profile of actors involved in digital surveillance in the DRC

This section presents the profiles of actors identified during the interviews as being involved in digital surveillance. These include state services (3.1.1), telecommunications companies – TCs (3.1.2) and international actors (states and foreign companies) (3.1.3). Out of a total of 18 interviewees, eighteen confirmed the involvement of state services, i.e., 100%, fifteen argued that telecommunications companies also engage in digital surveillance, i.e., 83%, and ten acknowledged the role played by international actors, i.e. 56%. Statistically, the degree of involvement of each actor in proportion to the interviewees is represented in the following bar chart:



3.1.1 State services involved in digital surveillance

The involvement of state services in the surveillance of citizens in the DRC is provided for in certain legal texts, all under the authority of the National Security Council (CNS) (4.1.1.1). State agencies that can "legally" monitor citizens' communications include the National Intelligence Agency (ANR) (4.1.1.2); the military Detection of Anti-homeland Activities (DEMIAP) (4.1.1.3) and the Superior Council of Audiovisual Communication (CSAC) (4.1.1.4). However, and more broadly, other state services are directly involved in this digital surveillance including the General Directorate of Migration (DGM) (4.1.1.5), National Police (4.1.1.6).

3.1.1.1 The National Security Council (CNS)

Located at the summit of the pyramid of state security services in DRC, the CNS was created under Ordinance 86–306 of November 24, 1986.[5] According to article 1 of Ordinance 87–032 on January 22, 1987, on the rules of procedure of the National Security Council, "the CNS ensures, under the authority of the President of the Republic, the centralisation and efficient use of documents and information from the various 'ad hoc' specialised services, in this case the ANR, the DDM, etc."[6]

3.1.1.2 The National Intelligence Agency (ANR)

The ANR created under Decree-Law No. 003-2003 is RDC National Intelligence Agency. Historically, however, the origin of the ANR dates back to 1960, with the country's accession to independence and had many different appellations depending on the period.

- Nation Security Service (SSN), 1960–1970
- National Documentation Centre (CND), 1970–1985
- National Documentation Agency (AND), 1985–1990
- National Intelligence and Protection and Protection Service (SNIP), 1990–1996
- Directorate General of National Security (DGSN), from 1996 to May 1997
- National Intelligence Agency (ANR), from 1997 till now (Kapinga, Kadda, et al., 2021).

According to Decree-Law No. 003-2003, the mandate of ANR is to research, centralise, interpret, use and disseminate political, diplomatic, cultural, scientific and other interesting information on the internal and external security of the State. Then, the ANR can legally monitor individuals or groups of individuals, regardless of their nationality, suspected of carrying out an activity that could undermine state security. In this way, such surveillance is part of its overall mission to seek out, centralise, interpret, exploit and disseminate political, diplomatic, strategic, economic, social, cultural, scientific and other information relevant to the internal and external security of the State.[7] However, missions to be carried out abroad of the DRC require judicial cooperation with the State requested for the purpose or be carried out via an international organisation such as Interpol.

The form of this surveillance is not specified, which makes it possible to include digital surveillance. Moreover, on numerous occasions, the ANR has been criticised by several independent reports for engaging in the practice of digital "spying" on opponents and activists of citizen movements (FIDH, 2016; CIPESA, 2016; Kapinga, Kadda, et al., Juin 2021). Contrary to what the law provides, the people targeted often do not represent any real threat to state security, which should be the basis for its action, as the recent lawsuit against Moïse Katumbi proved.[8]

5 This Ordinance is available at https://www.droitcongolais.info/files/412.11.86-Ordonnance-du-24-novembre-1986_Conseil-national-de-securite.pdf .

6 Order 87-032 of 22 January 1987 on the internal regulations of the National Security Council, available at http://www.leganet.cd/Legislation/Droit%20Public/Ordre/O.87.032.22.01.1987.htm

7 Art 3 of the Decree-Law n°003-200, especially point 3.

8 VOA Afrique, DRC: Opposition politician Katumbi to be tried for undermining state security (https://www.voaafrique.com/a/

3.1.1.3 The Military Intelligence Staff (MIS)

The Military Intelligence Staff (MIS), better known by its former appellation "The Military Detection of Anti-Patriotic Activities" (DEMIAP),[9] is a military intelligence service created under decree 018/2002,[10] As an intelligence service, it has regularly been pinned down for notably its involvement in the repression of the opposition and activists (FIACAT; ACAT, 2016; Amnesty International, 2007). Therefore, digital surveillance is one of the methods used by this service for accomplishing its missions and tool for the DRC government for muffling civil society and the opposition (CIPESA, 2016).

3.1.1.4 The Superior Council of Audiovisual Communication (CSAC)

The Superior Council of Audiovisual Communication (CSAC) facilitates activities of digital surveillance in the DRC. Indeed, the CSAC exercises, by virtue of the Constitution, the power of regulation over the means to be used for this surveillance, in particular of the media.[11] Many local media actors interviewed during our surveys, in particular independent media, stressed the CSAC'S support to the government by censoring their media.

3.1.1.5 General Directorate of Migration (DGM)

The General Directorate of Migration (DGM) created under decree 002/2003[12] is a state security service. Article 3 of this decree provides that "subject to other assignments conferred or to be conferred on it by specific laws, the General Directorate of Migration (DGM) is responsible for matters relating to collaboration in search of criminals or wrongdoers or people suspects reported by Interpol". Broadly worded, this formulation would imply consequently the use of all means to carry out this research, among others digital surveillance.

3.1.1,6 National Congolese Police (PNC)

Within the Congolese national police, there is an intelligence body called "General Directorate Intelligence and Special Police Services" – better known by its French appellation "Direction des renseignements généraux et services spéciaux de la police" (DRGS). Although the DRGS is the official police body, it occasionally acts as an intelligence service. Moreover, the DRGS is headed by a commission made up of security advisers, among others, those under the presidency as well as other intelligence agencies. Like other intelligence services described above, the DRGS has been singled out, especially in many independent reports, for engaging through various means including digital surveillance, in the arrest of political opponents and civil society activists (Amnesty International, 2007; Mayamba, 2012).

In short, the DRC has several intelligence services with overlapping functions. The separation of powers between those services remains unclear and leads to rivalry including lack of cooperation. For more detail, see the organigram relating to the organisation of DRC police:

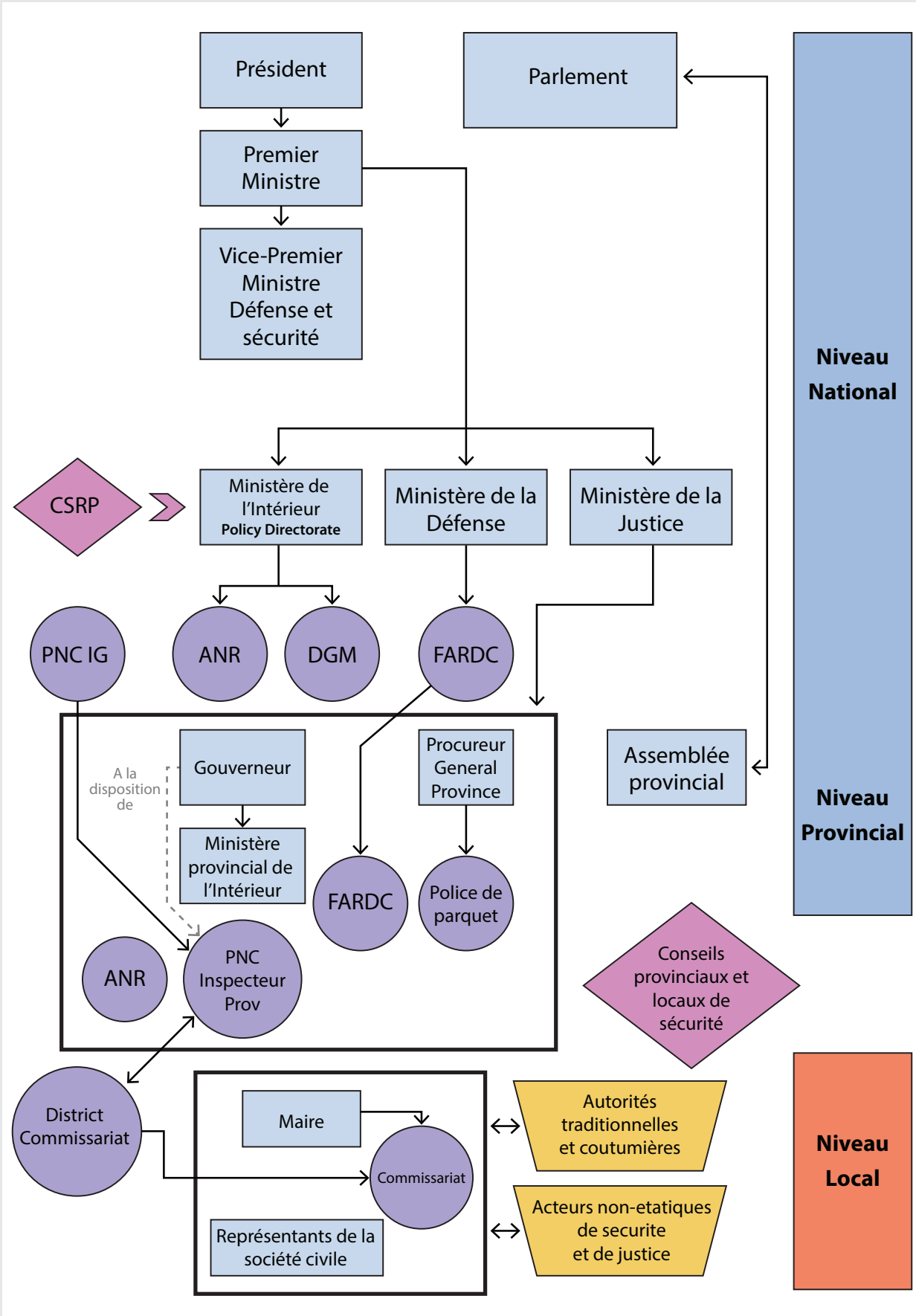
rdc-lopposant-katumbi-sera-juge-pour-atteinte-a-la-surete-de-l-etat/3337796.html).

9 Canada: Immigration and Refugee Board of Canada, Democratic Republic of Congo (DRC): Détection militaire des activités anti-patrie (DEMIAP), including its organisational structure, activities, role and that of a "commander" within DEMIAP; information on whether DIMIAP members have committed serious human rights violations, including torture and crimes against humanity (2000–2002), 7 July 2003, RDC41693.F, disponible sur https://www.refworld.org/docid/3f7d4e092a.html [accessed 23 August 2021].

10 DECREE 018/2002 24 February 2002 creating a specialised service of the Congolese Armed Forces called the General Directorate for the Military Detection of Anti-Patriotic Activities, "DGDEMIAP", in acronym. (Presidency of the Republic) https://www.leganet.cd/Legislation/Droit%20Public/Defense/D.018.02.24.02.02.htm.

11 See art 212 of the Constitution as amended by la Loi n° 11/002 du 20 janvier 2011 portant révision de certains articles de la Constitution de la République Démocratique du Congo du 18 février 2006 and art 8 of the Loi organique n° 11/001 du 10 janvier 2011 portant composition, attribution et fonctionnement du Conseil Supérieur de l'Audiovisuel et de la Communication

12 Décret-Loi no. 002/2003 du 11 janvier 2003 portant création et organisation de la Direction Générale de Migration.



Source: (Mayamba, 2012).

This organogram shows that stakeholders of the security and police sectors of the DRC are linked together in a web of complex and dynamic systems, characterised by the discrepancies between theory and practice. These interlocking and multifaceted systems are in constant conflict and fuelled by relations of power, tacit agreements and collusion, constraints and opportunism as it has been highlighted in several previous studies (Mayamba, 2012; (Mayamba, 2013).

3.1.2 Telecommunications companies (TCs)

Telecommunications companies in DRC proceed, or at best helping the government to conduct digital surveillance of their subscribers. Indeed, these companies regularly record subscribers' personal data and are invited, if so requested, to communicate them to government or another official service. Moreover, this obligation is legally provided by new law and expressly worded in their operating licences under pain of penalties. In most cases, however, these telecommunications companies or internet providers comply with the government requests for information to this effect (CIPESA, 2016; AE, TP, & Ritimo, 2020).

3.1.3 International actors

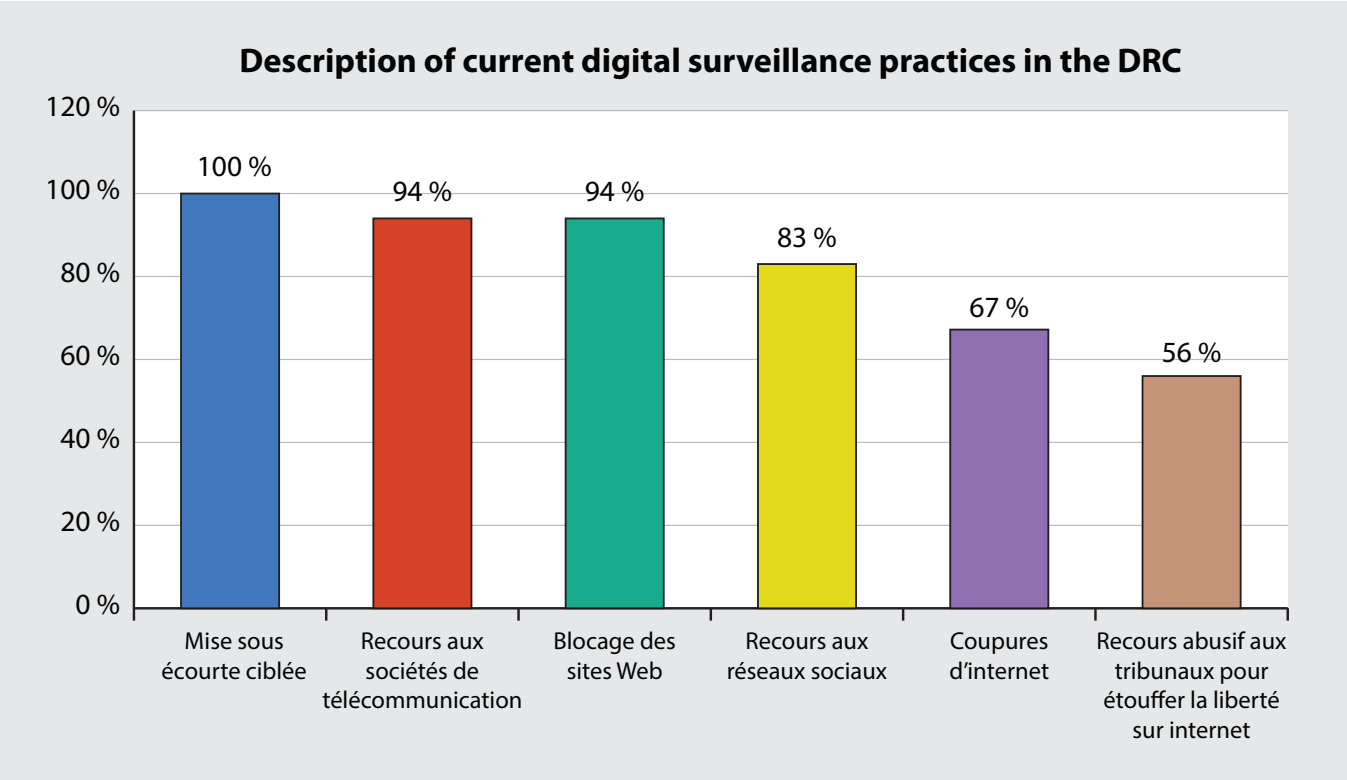
International actors especially state foreign private companies as well was foreign State companies also carry out digital surveillance target the DRC country or its citizens, either with or against state intelligence services[13]. Indeed, since the revelations resulting from the Edward Snowden document's leak, several international media including Le Monde and Intercept sites looking at documents relating to Africa, have reported that the continent has been of more interest to the American and British intelligence services for years and that in addition, the Democratic Republic was at the top of the 20 countries spied on. Furthermore, the damning revelations accusing former President Joseph Kabila of recruiting former Mossad members via Black Cube (a private Israeli intelligence company) in carrying out this targeted surveillance since 2015 shed light these digital surveillance practises.[14]

3.2 Description of digital surveillance practises commonly used in the DRC

Our study reveals that the Congolese state is regularly involved in digital surveillance, with the help or assistance of telecommunications companies, multinational corporations, banks and even private individuals. The study identified a variety of common practices, including targeted wiretapping, online monitoring and blocking of websites, use of telecommunications companies, use of social networks and abuse of the tribunals and courts to stifle internet freedom, all of which are usually carried out without the knowledge of the victims of surveillance. Out of 18 interviewees on the existence of these practices, eighteen acknowledged the existence of targeted wiretapping, i.e., 100%, seventeen acknowledged the use of telecommunications companies, i.e., 94% and the blocking of websites, i.e. 94%, fifteen acknowledged the use of social networks, i.e. 83%, twelve acknowledged the cutting off of the internet, i.e. 67% and ten acknowledged the abuse of the courts to stifle internet freedom, i.e. 56%. The following graph represents these practices in terms of their existence:

13 https://www.lemonde.fr/afrique/article/2016/12/08/la-rdc-etroitement-scrutee-par-les-espions-britanniques-et-americains_5045622_3212.html.

14 For more details information is available on https://www.france24.com/fr/20190610-rdc-joseph-kabila-accuse-avoir-recrute-anciens-mossad-espionner-opposition.



3.2.1 Targeted wiretapping

Targeted wiretapping was considered by all our interviewees to be the classic means used by the security services, particularly the National Intelligence Agency (ANR), to spy on opponents, civil society's leaders and citizens' movements or any other voice that is discordant with the government. As a classic means, through his phone, the person to be bugged is identified, including by an IMEI number. Therefore, the person can be followed directly (through their personal conversations) or be listened to via a server. In addition, automatic recording can be triggered without the person's knowledge. A micro camera or chip can also be placed at home, in the car or anywhere else. More concretely, phone tapping is also facilitated upstream by installing a micro-transmitter on the phone (Harivel, 2018).

Most of our participants pointed to the existence of appropriate technology at the NRA to facilitate wiretapping. These findings are corroborated by thematic studies dealing with the issue. Although old, it is said to have increased during the government of former President Kabila, who had wiretapped the leaders of some opposition political parties in 2019, as reported by several international media (RFI, TV5, France 24). According to the latter, the Black Cube – a private Israeli intelligence company as mentioned above – had spent many months in Kinshasa investigating and bugging Congolese opposition leaders.

The step taken in May 2020 could further aggravate the situation, as the government now has access to certain network parameters of millions of mobile phones in order to collect_IMEIs. Indeed, since September 2020, the government announced the creation of the Mobile Divice Registry (RAM). According to the Minister, the database linked to this registry will allow the government to limit the market for counterfeit mobile devices, to fight against the theft of mobile devices and to improve the quality of the mobile phone network by blocking devices that do not comply with international standards. However, it is likely to increase privacy intrusions as governments increasingly monitor citizens.

3.2.2 Online monitoring and blocking of websites

During our survey, respondents underlined that the DRC government, through its security services, uses specific algorithms to analyse URLs consulted by internet users and to identify some websites considered to be critical of the regime of former DRC's President Joseph KABILA (AE, TP, & Ritimo, 2020) (CIPESA, 2016). However, security services interviewed during our survey denied those affirmations, arguing that the DRC does not have the technical tools for the purpose.

Nonetheless, the practice of blocking websites remains an obvious reality in the DRC. Indeed, when monitoring electronic content, the Congolese government often targets certain websites it considers critical and blocks them. These forms took a trend towards the years 2016, with the government ordering the blocking of certain sites, among others, www.descwondo, www.vacradio.com, for their alleged attachment to the opposition. In addition, the websites of some media outlets, notably Voice of Africa in Canada (VOAC), were also blocked during the same period (CIPESA, 2016).

3.2.3 Use of telecommunications companies

The DRC has also seen a proliferation of telecommunications companies. Five mobile operators: Vodacom, Orange, Aitrel, Africell and Standard Telecom operate in the DRC, with an 80% share of the internet market. The assistance of these companies to the government-led digital surveillance was confirmed by all our interviewees, and reported in several national and international reports, conducted by independent structures (AE, TP, & Ritimo, 2020). On the one hand, our study revealed that all calls are stored and that these companies proceed, upon request from the government, to the "telephone records" (number called or of the caller, duration and time of the call, etc.) of the tapped person.

3.2.3.1 The duration of data storage

The duration of data storage varies according to the types of information available to the telecommunications company.

With regard to subscription data, the retention period is provided for by an interministerial order[15] setting the conditions for subscribing to a telephone subscription in the Democratic Republic of Congo According to Article 11 of this order,

> *The operator of a network or the provider of telecommunications services open to the public shall keep the identification elements of subscribers in physical format, in accordance with the law. However, he is obliged to keep the identification elements of his subscribers as well as the IMEI details attached to the number or connection, in digital format for the entire duration of the subscription.*

However, the identification elements of subscribers in electronic format may be removed from the database 6 months after the effective termination of the subscription, cessation of supply or of any activity on the operator's or supplier's network.

In all cases, the operator of a network or the provider of telecommunication services open to the public is required to communicate with the competent public services the identification elements of the subscribers contained in its database, prior to any deletion, withdrawal or overwriting. This provision distinguishes between identification elements in paper format and those in electronic format. In the case of the electronic format, the telecommunications company must keep the data for a period of 6 months after the termination of the subscription. In any case, the company is obliged to communicate the information to the state services before any deletion.

15 Interministerial order No. 25/CAB/VPM/MIN/ INTERSEC/024/2015, No. 003/ CAB/VPM/PTNTIC/ 2015, no. DMNAC- RCAB/009/2015, No. 004/CAB/MIN/ J&DH/2015,no. CAB/MIN. FINANCES/2015/0144 n° 008/CAB/MIN/CM/LMO/2015 of 19 May 2015 amending and supplementing interministerial Decree n° 068/CAB/MIN/ INTERSEC/2009, n° 212/CAB/MIN/J/2009, n°CAB/MIN/PTT/011/2009 21 December 2009.

As regards connection or traffic data, telecommunications companies must keep them for a period of 6 months. This follows from Article 142 of the new ICT law. According to this provision,

> *Network operators and service providers are obliged to keep connection and traffic data for a period of twelve months and to install mechanisms for monitoring data traffic on their networks.*
>
> *The connection and traffic data kept may be accessible during judicial investigations, under the conditions set by the laws and regulations in force.*

Our respondents also felt that in order for wiretapping to be successful, it is necessary to be a worker of these telecommunications companies or at least to involve them. To do this, the government either collaborates directly with these companies or goes through one of their technicians without the company's knowledge to monitor someone. The other way is to order these companies to suspend the internet and short message service (SMS), especially during times of political turbulence. This includes the suspension decided on 19 January 2015, in relation to the protests against the draft electoral law.

3.2.4 Use of social networks

As in almost every country in the world, social networks have become one of the means of mass communication in the DRC. Similarly, their use often takes on a political connotation through which government and opponents wage war. The government therefore often monitors certain profiles and does not hesitate to censor publications on social media. In most cases, these publications lead to arrests, often carried out by the security services, in this case the ANR, without going through a judge. Emblematic cases of these practices took place on 20 June 2015, when people were arrested and charged because of their publications on social media. These include the case of Godefroid Mwanabwato, a member of the citizen movement Filimbi. At his hearing, the ANR stressed that his arrest was linked to a Facebook status published the day before, which denounced the arrests of other activists, including Fred Bauma and Yves Makwambala. In addition, Mwanabwato had been sentenced to two years in prison for insulting the "President on Facebook'.

On 24 December 2018, the day after the presidential election, the Autorité de régulation de la poste et des télécommunications du Congo (ARPTC) asked internet operators to "restrict access to videos and images" on the social networks Facebook, WhatsApp, Viber, YouTube, Twitter".[16] All of this provides ample evidence of the large-scale digital surveillance practiced by the security services, particularly the ANR.

3.2.5 Misuse of the courts to stifle the internet

In principle, courts are not directly involved in digital surveillance. Their main role is limited to authorising interceptions of correspondence, voice calls content or even data, according to the laws in force. However, the study found that monitored activists and opponents are sometimes brought before the courts as a result of simple posts on social media. Previous reports have highlighted that since 2015, the NRA has been making untimely arrests of activists without court orders. This is the case of the arrest of Godefroid Mwababwato of the Filimbi movement (CIPESA, 2016), based solely on Facebook status. In addition, in 2016 the journalist Patient Ligodi, co-founder of politico.cd, was also arrested following his coverage of a demonstration, which had itself been annotated on Facebook and Whatsapp.

16 See lettre N/réf n°ARPTC/PRES/767/2018 portant « mesures préventives, suspension momentanée des accès vidéos et images des réseaux sociaux ».

After the change of the Kabila government, these practices are currently continuing. Several cases of arrest have been reported, based solely on online communications allegedly intercepted by the security services, which regularly conduct large-scale online surveillance and even excessive activism and propaganda.

The case of Heri Kalemaza against the Governor of South Kivu is an example of surveillance justified by Congolese courts.

By his request for the setting of a hearing of 30 April 2020[17], the Officer of the Public Prosecutor's Office at the Court of Appeal of South Kivu brought the accused Heri Kalemaza Nicodème to trial for several facts constituting an offence of damaging the imputation. Indeed, the accused Heri Kalemaza Nicodème is accused of having in Bukavu, on 26 December 2019, 27 January 2020 and in January 2020, in the social media WhatsApp called "Unis par le Droit/UOB", published several messages discrediting the governance undertaken by the Governor of the province of South Kivu, Mr. Théo Ngwabije Kasi.

In his plea, while relying on the report of the AIRTEL company which showed that the number used to send the incriminated messages belonged to another person and on the testimony of witnesses who confirmed having studied with three persons answering to the name of Kalemaza, the accused remains constant in his denials and considers that the intimate conviction of the Court will not be enlightened, because no informant has proved that the messages produced by the prosecution came from him. As a result, the accused considers that there is still a serious doubt as to the existence of the constituent elements of the offences with which he is charged. He concluded by asking the Court to declare the offence of damaging imputation in his case not established in fact and in law and consequently, to acquit him for lack of evidence and/or doubt and to dismiss him from all legal proceedings, to declare the claim for compensation of the civil party unfounded and to charge the costs of the proceedings to the Treasury.

In its judgement on 30 September 2020, the Bukavu Peace Court considered that the offences of damaging imputations against the defendant were established in fact and in law.

In view of the above, the Court finds that the fourfold offence of damaging imputations committed by the accused is established both in fact and in law, in that he perpetrated these facts with the sole intention of undermining the honour and consideration of the civil party, and sentences him to a single penalty of 250,000 Congolese francs in fines payable within the legal time limit, or failing this, to 15 days of subsidiary penal servitude. Then, it declared the constitution of the civil party admissible and founded and consequently condemned the accused to pay damages of one American dollar payable in Congolese francs in favour of the civil party NGWABIJE KASI Théo as requested by the latter. Finally, the court will charge the costs of the proceedings to the defendant or, if he fails to pay them within the legal time limit, he will be subject to five days' imprisonment.

17 Request for the setting of a hearing date n° 1202/ RMP 1314/ PG.074/ NDK/ SEC/ 2020 of 30 April 2020

4. Tools used in digital surveillance

It is difficult to describe the tools used in digital surveillance in the DRC. Despite the refusal of public service to confirm the existence of surveillance techniques, the data collected from other targets is unanimous on the existence of technology within these services that allow them to monitor people, while admitting that they do not have sophisticated surveillance tools. Apart from public service, telecommunications companies also carry out electronic surveillance at the request of the government. A distinction must therefore be made between public service and telecommunications companies.

As regards telecommunications companies, they have computer programs that enable them to carry out telephone tapping by installing a micro-transmitter in the telephone of the person being monitored, in particular by means of his IMEI number, to monitor his direct line by means of key words using algorithms, the use of servers to store, retain and filter information, cryptology means, etc. These practices are generally carried out at the request of the government. These practices are generally carried out at the request of public service following a requisition from a judicial authority. By law, for reasons of national security or a court case, these companies are obliged to communicate the identity of subscribers to the authorities. The same applies to calls and money transactions via Airtel money, Orange money and M-pesa, whose daily basket is capped at two thousand five hundred US dollars (USD 2 500). Moreover, the involvement of the latter in the creation and application of the Mobile Divice Registry (RAM) is expressly provided for by law. Another tool of this monitoring is the establishment of an electronic visa announced since 2019 by the President of the Republic and involving a digital identification system (AE, TP, & Ritimo, 2020).

In addition to the tools mentioned above, the communications companies have management software (database) for all the Sim cards with access rights that differ according to the grades of the agents responsible for using this software. These management systems have performances ranging from the creation of a telephone number, the masking of the calling number (unknown number), the identification of the user, the recording of all the activities carried out by the Sim card (recording of logs of all calls made and received, SMS sent and received with flawless chronological accuracy) to the deletion of the number. This software varies from one telecom company to another. The company Vodacom uses South African ICAP software. Airtel uses the American software AGYLE. Orange uses MYPOS or Zsmart software.

As far as the public service is concerned, they claim that they do not have the technological tools to monitor citizens. They claim to use telecommunications companies. Data collected from other targets show that these services have such tools. They use wiretapping software. This software is a small computer program, also known as spyware, which gives the user the opportunity to monitor, intercept and listen to all incoming and outgoing mobile phone calls. This monitoring is done without the knowledge of the owner of the phone. It works on all types of platforms, both IOS (iPhone) and Android (Samsung, Huawei, Xiaomi...).

This software collects recordings of voice calls throughout their duration, including call information such as the date and time, as well as the number. Telephone calls can be monitored remotely from a control panel or customer area, or from your own telephone.

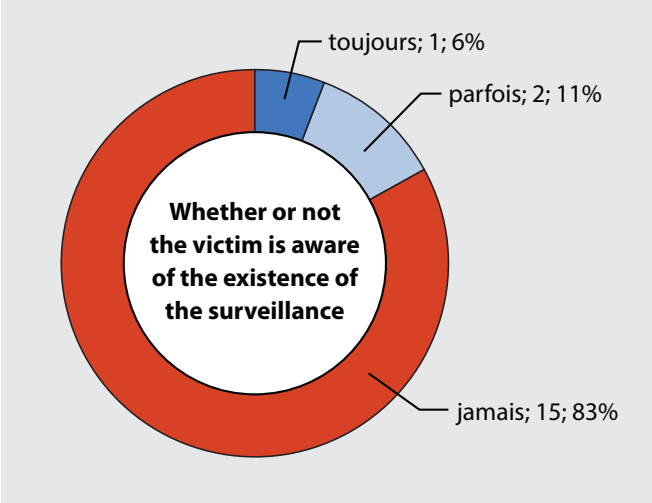
According to the information obtained, the public services use two companies to obtain this software.

On the one hand, they buy from the Israeli firm NSO GROUP, which markets the Pegasus spying software. Apart from the DRC and other authoritarian regimes, this software is also used by democratic states to monitor journalists, political opponents and human rights activists. The software can be installed remotely through phishing. It has extensive remote control capabilities and access to phone data, including SMS and messages (including encrypted) sent and received, and address books. The software can activate microphones and cameras, capture GPS location data and allow the recording of phone calls. It can also access social media posts, photos, videos and recordings. It has access to internet browsing history. It can also trace the user's route. For example, Pegasus is able to capture data from applications such as WhatsApp, Skype, Facebook or Gmail. It can also record all the characters typed on the phone or photograph the screen.

On the other hand, the public service would have used the German group PKI Electric Intelligence GmbH. This group manufactures several software products, one of which is involved in digital surveillance. This is the PKI 1800, which is a complete, state-of-the-art end-to-end solution for monitoring, processing, analysing and disseminating intercepted telecommunication interactions. It can monitor ISDN, digital, PCM30 and all other forms of communication, whether voice, fax, modems, radio or other data transfers. Based on a single, unified platform, the ICP 1800 handles all types of telephone and Internet data, offering unprecedented functionality. It provides security agencies with the flexibility, reliability and versatility to intercept and analyse signal intelligence. The main feature of the PKI 1800 is its flexibility and extraordinary storage capacity, linked to its ability to instantly recall intercepted phone calls via the displayed data management software without interrupting the recording and archiving process on the digital tape. This allows the operator to perform an interception and playback from a single system or, optionally, using a separate playback unit. This means that highly classified and prioritised intercepts can be configured to be transferred by authorised users in real time to a selected location, ensuring that the right people are informed in time.

5. Victims' lack of awareness of the existence of surveillance

The field studies revealed that almost all of the people under surveillance are never informed of the existence of such surveillance, as the results of our field surveys reveal. Indeed, when asked whether or not the victims knew that they were being monitored, out of 18 interviewees, 15 (83%) said that the victim was "never informed", two (11%) said that the victim was "sometimes informed", and one (6%) felt that the victim was "always informed". The following diagram provides a statistical representation of these results:



There was also revealed in the study that digital surveillance and particularly interception is generally carried out upstream, at the level of internet access provider or telecommunication services. This practice violates human rights instruments, in particular the Malabo Convention of 27 June 2014, which stipulates that "the controller must inform the natural person whose data is being processed in the category of data covered by the processing, the purpose, the duration of its retention and any transfer to third parties'.[18] Generally, surveillance cases are revealed by international media, after leaks of investigative documents as explained above.

18 Art 16 de la African Union Convention on Cyber Security and Personal Data Protection, adopted in Malabo on 27 June 2014.

6. Analysis of the legal framework of surveillance in DRC

Having described the usual surveillance practises in the DRC, this section examines the legal texts that allow and encourage these practices. Indeed, on the internet as elsewhere, individuals are protected against interception of their information and communications, whether such interception is carried out by public authorities or private actors such as employers. However, this does not mean that all forms of surveillance are banned. However, interceptions are only allowed under strict conditions that protect society from the abuses of surveillance. The analysis of legal texts is relevant to this study, as the government regularly invokes them to justify its conduct. Like most states, the DRC is currently making several efforts to update its regulations in the field of NICTs. In our era, NICTs have become a powerful tool, particularly in terms of digital surveillance. To this end, several texts authorise the state to use surveillance. These include the Constitution of the DRC, Decree-Law No. 003-2003 on the creation and organisation of the National Intelligence Agency (ANR), Law No. 20/017 of 25 November 2020 on NICTs, the Ministerial Order of 2020

on the RAM, the Penal Code through the offence of undermining state security and Law n°18–019 on payment and securities settlement systems. Therefore, by focusing on the context in which they were drafted, the content of their substantive provisions and the objectives pursued by the legislature, we will determine whether these texts underpin the surveillance practises described above.

6.1 *Surveillance in the Congolese Constitution*

The protection of personal data is closely linked to the right to privacy, which is considered in the Congolese Constitution as an autonomous fundamental right. Under Article 31, the Constitution provides that "every person has the right to privacy and to the secrecy of correspondence, telecommunications or any other form of communication. These rights may not be infringed except in the cases provided for by the laws.[19] This protection is also a condition for the exercise of other fundamental rights.

Thus, it is now recognised that the protection of personal data plays a fundamental role in the exercise of the right to respect for private and family life. In addition, the processing of personal data may have an impact on other rights and freedoms that are intrinsically linked to them. This is particularly the case for the rights to freedom of expression,[20] information[21] and association,[22] which are also guaranteed by the Constitution. The first, i.e. the right to freedom of expression, implies the freedom to express one's opinions or convictions, in particular through speech, writing and images. The right to information includes freedom of the press, freedom of information and broadcasting by radio and television, the written press or any other means of communication. Freedom of association includes freedom of peaceful and unarmed assembly. Under the Constitution, restrictions may be placed on the exercise of these rights, but only in cases provided for by law, respect for public order and morality, and respect for the rights of others.[23]

6.2 *Decree-Law No. 003-2003 on the creation and organisation of the National Intelligence Agency (ANR)*

Contemporary society is marked by the adoption of legal and administrative restrictions on the protection of privacy, under the guise of the fight against insecurity and terrorism. These restrictions generally take the form of anti-terrorism laws which, in addition to granting exorbitant rights to the intelligence services, legalise practices already implemented by these services without legal basis. This is particularly true of communication surveillance. The means made available by the digital society facilitate this surveillance, whereas it is above all against the actions of the public authorities that the confidentiality of exchanges between individuals is to be guaranteed.

These features dominate Decree-Law No. 003-2003 on the creation and organisation of the National Intelligence Agency (ANR) in the DRC. According to its article 3, "the mission of the latter – the ANR – is to ensure the internal and external security of the State. In this respect, it has the following responsibilities (…) 3. Surveillance of national or foreign persons or groups of persons suspected of carrying out an activity likely to undermine state security (…)". Indeed, according to the law, this surveillance is part of its general mission to carry out "research, centralization, interpretation, exploitation and dissemination of political, diplomatic, strategic, economic, social, cultural, scientific and other information relevant to the internal and external security of the State". This broadly worded and ambiguous provision was used

19 Art. 31 of the 2006 Congolese Constitution as amended by Law n° 11/002 of 20 January 2011 revising certain articles of the Constitution of the Democratic Republic of Congo of 18 February 2006.
20 Art. 23, idem.
21 Art. 24, idem.
22 Art. 25, idem.
23 Articles 23, 24, 25 and 31 of the Congolese Constitution.

as leverage by the government of former President Joseph Kabila, which had wiretapped some political party officials, particularly those of the opposition, in 2019. Thus, as soon as the surveillance relates to the above-mentioned category of protected information, the ANR is empowered to proceed. The ANR has nothing to worry about because, under this text, it is placed directly under the authority of the president of the Republic (art. 2) and not under the authority of parliament, which could monitor its actions. Again, the law authorises the ANR to share this information, particularly in the context of judicial cooperation, either with other States or with international organisations such as Interpol (Article 3, points 6 and 7).

6.3 *Law No. 20/017 of 25 November 2020 on NICTs*

The new law No. 20/017 of 25 November 2020 on telecommunications and new information technologies in the DRC contains provisions that allow the digital surveillance practises described above. This law was adopted in response to the social, human and, above all, security issues and challenges raised by the former law No. 013/2002 on 16 October 2002, which had been overtaken by technical and societal developments in this area. It innovates by ensuring the protection of privacy and personal data, notions that have been led to evolve beyond their traditional understanding in the context of information and communication technologies, and specifically the Internet. It is part of the contemporary conception according to which private life is no longer conceived as limited to an intimate sphere to be shared, containing a set of private, even confidential, information that one wishes to keep hidden. This is clearly demonstrated by the establishment of a title on the protection of privacy and personal data of users of networks and services. In its article 126, it states that "Everyone has the right to the secrecy of correspondence transmitted by means of telecommunications and information and communication technologies". To this end, article 127 emphasises that,

> *The interception, listening, recording, transcription and disclosure of correspondence emitted by means of telecommunications and information and communication technologies, without prior authorisation from the Public Prosecutor's Office of the Court of Cassation, are prohibited, as are the emission of false or misleading alarm, emergency and distress signals the transmission of signals and communications likely to undermine State security or which are contrary to public order or morality or which constitute an insult to the convictions of others or an offence against a foreign State.*

Similar protection is afforded to personal data. According to Article 131 of the aforementioned Law No. 20/017 on 25 November 2020, "the confidentiality of personal data shall be guaranteed and protected, and their processing shall only be carried out with the consent of the person concerned or at the request of the public prosecutor". Article 132 completes this protection by stating that "the collection, recording, processing, storage and transmission of personal data shall be carried out with the authorisation of the user concerned or of the competent public authority, in accordance with Article 126 of this law. The collection and processing of personal data revealing racial, ethnic or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sex life, genetic data or, more generally, data relating to the state of health of the person concerned are prohibited".[24] Such a ban is not absolute. The law refers to a ministerial order which, on the proposal of the Regulatory Authority, will set the conditions and modalities for the collection, recording, processing, storage and transmission of personal

24 See art. 132.

data. However, this order is still pending.[25] This order will certainly authorise the collection of data in the field of the census or any other field requiring such collection.

Indeed, this law meets the requirements of the digital era, paper mail which was protected by seals or other encryption processes and their well-defined and criminally sanctioned misappropriation is becoming marginal. Messages are now exchanged via electronic messaging, e-mail, social networks or SMS or MMS messages in particular. However, although by virtue of the new law these exchanges by telecommunication are assimilated to private correspondence and, consequently, benefit from the same protection as recalled by the relevant provisions mentioned above, the numerous exceptions that this law abounds in and which specify the conditions under which an interception can take place weaken its protective character. These exceptions include the lifting of the secrecy of correspondence at the request of the public prosecutor's office or with the authorisation of the courts and tribunals in the context of a judicial investigation, and derogation from this secrecy by the competent services – including the ANR – for reasons of internal and/or external state security, national defence or public order (Article 126). Next, Article 127 provides that "only the needs of information motivated by the requirements of the ultimate demonstration of the truth in a judicial case may authorise the Public Prosecutor's Office at the Court of Cassation to prescribe the interception, recording and transcription of correspondence emitted by means of telecommunications and information and communication technologies". Article 129 goes further by empowering the public prosecutor's office at the Court of Cassation to request any agent of a service or body to install a device necessary to carry out the operations indicated in the previous Article 127 (1), while Article 128 provides that this decision may last for three months, renewable for the purposes of the investigation. The vagueness of these exceptions leads to disproportionate infringements of these rights in the Democratic Republic of Congo, which can be extended for as long as the person making the decision invoke the need for the investigation, as the number of renewals is not limited.

6.4 Ministerial Order of 10 June 2020 on the RAM

Ministerial Order No. CAB/MIN/PT&NTIC/AKIM/KL/Kbs/002 of 10 June 2020 on the establishment of a CEIR system in the Democratic Republic of Congo also allows the government to monitor mobile telephone subscribers. Setting up a CEIR system in the Democratic Republic of Congo also allows the government to monitor mobile phone subscribers. Indeed, this text sets up the Central Electric Identity Register (CEIR) in the DRC and defines the conditions for it. The official reason given for this is set out in Article 2 of the said decree, which considers that the database linked to this register will enable the government to limit the market for counterfeit mobile devices, to combat the theft of mobile devices and to improve the quality of the mobile telephone network by blocking devices that do not comply with international standards. However, through this registry, the government now accesses certain network parameters of millions of mobile phones in order to harvest IMEIs. This situation is bound to increase, as Article 4 makes identification by IMEI number a prerequisite for any user to gain access to any mobile phone networks open to the public. The other reason that could exacerbate this phenomenon is financial gain. The registration of mobile devices is carried out in return for payment of an "IMEI registration fee", the amount of which varies according to the type of device. This has been a reality since September 2020, when the government announced the creation of the Mobile Device Registry (RAM). Beyond

25 See art. 133.

the social discontent caused by the application of the RAM, it is highly likely that this technique will accentuate the intrusions into private life, as governments increasingly monitor citizens.

6.5 *The Penal Code through the offence of attacks on State security*

The Congolese Penal Code, in Title VIII entitled "Attacks on State security", contains a series of offences considered by the legislature to jeopardise State security. The legislature distinguishes between attacks on the external security[26] of the State, on the one hand, and attacks on the internal security[27] of the State on the other. Although the legislature seems to have opted for an exhaustive wording with regard to the legal element of each of the offences referred to in this title, the prosecution regime devoted to them generally leads to an intrusion into the private lives of persons suspected of committing these offences. As a reminder, as soon as national or foreign persons or groups of persons are suspected of carrying out an activity that could undermine state security, the ANR is legally authorised to carry out surveillance.[28] In addition, certain public authorities may, even without the status of a judicial police officer and without a warrant, arrest persons who are guilty of the offence of undermining state security.[29] Finally, the derogatory regime allowing the Minister of the Interior to place these people under surveillance by a simple written decision[30] often leads to abuses, the "attack" on state security being a means of stifling political opponents, as revealed by the Moïse Katumbi trial.[31]

6.6 *Law 19-019 on payment and securities settlement systems*

Adopted in 2018, with the objective of regulating transactions based on new payment instruments, in particular payment cards and other similar electronic payment instruments,[32] this law authorises the government, through the central bank, to create and manage a register whose mission is to centralise information, in particular on customers, accounts, payment incidents and irregular payment instruments.[33] On the one hand, the central bank can delegate the management of this register, and on the other hand, article 76 of the said law recognises the right of access to the information contained in this register to certain officials. The latter could thus divert these data from their purpose by spying people monitored by the government.

26 Art. 181 to 192 of the Congolese Penal Code, Decree of 30 January 1940 as amended and completed to date, updated to 30 November 2004.
27 Art. 193 to 214 Congolese Penal Code, Idem.
28 Decree-Law No. 003-2003 on the creation and organisation of the National Intelligence Agency.
29 Decree of 16 May 1960 on the violation of public order and tranquility http://www.leganet.cd/Legislation/Droit%20Judiciaire/D.16.05.1960.htm
30 Decree-Law 1-61 of 25 February 1961 on State security measures.
31 https://www.voaafrique.com/a/rdc-lopposant-katumbi-sera-juge-pour-atteinte-a-la-surete-de-l-etat/3337796.html
32 Explanatory memorandum to Law No. 18-019 on payment and securities settlement systems, in J.O. RDC, 23 July 2018, special issue, col.53.
33 Art. 75, *Idem*.

7. Adequacy of the legal framework regarding human rights

After outlining the legal texts on which digital surveillance practises are based, the presentation will focus on examining their conformity with international human rights law. The DRC is party to several international treaties, including the International Covenant on Civil and Political Rights. These texts protect personal data through provisions relating to privacy.

The ICCPR protects privacy through Article 17. According to this provision,

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

This provision protects against digital surveillance. In its General Comment No. 16, the Human Rights Committee states that "[…] surveillance by electronic or other means, interception of telephone, telegraph or other communications, tapping and recording of conversations should be prohibited".[34] This provision imposes a negative obligation on the State, i.e. an obligation to abstain. The State is under an obligation not to interfere with correspondence. In the Estrella v. Uruguay case, the Committee recalls that electronic or other surveillance, interception of communications or listening and recording of conversations must be strictly limited.[35] In principle, surveillance is not prohibited. The Human Rights Committee subjects it to the authorisation and supervision of the judicial authorities.[36] In several concluding observations, the Committee remains attentive to cases where judicial authorisation and supervision are insufficient.[37]

In terms of domestic law, as in other countries, the Congolese legislature and sometimes the judge have intervened to respond to the challenges posed to privacy and the protection of personal data by the deployment of the Internet. A recent text, law No. 20/017 of 25 November 2020 on telecommunications and new information technologies, was adopted, renewing the original texts of 2002, which have been overtaken by technical and societal developments. This law devotes a title to the protection of privacy and personal data of users of networks and services. Article 126 of the law states that "Everyone has the right to the secrecy of correspondence sent by means of telecommunications and information and communication technologies". To this end, the interception. Listening, recording. transcription and disclosure of correspondence emitted by means of telecommunications and information and communication technologies, without the prior authorisation of the public prosecutor's office of the Court of Cassation are prohibited. Likewise, the emission of alarm, emergency and distress signals which are false or misleading, are prohibited, and the transmission of signals and communications which are likely to undermine state security or which are contrary to public order or morality or which constitute an insult to the convictions of others or an offence against a foreign state are prohibited. Only the needs of

34 HR Committee, General Comment 16.
35 HR Committee, Estrella v/ Uruguay, const. of 29 March 1983, communication n°74/1980.
36 HR Committee, Hulst v/ Netherlands, const. of 1 November 2004, communication n°903/1999, § 7.6 - 7.8.
37 HR Committee, Concluding Observations on Belarus, CCPR/C/79/Add.86, 1997, § 15; HR Committee, Concluding Observations on Jamaica, CCPR A/53/40, 1998, § 88; HR Committee, Concluding Observations on Poland, CCPR/C/79/Add.110, 1999, § 22; HR Committee, Concluding Observations on the Netherlands, CCPR/C/NLD/CO/4, 2009, § 15; HR Committee, Concluding Observations on Sweden, CCPR/C/SWE/CO/6, 2009, § 18; HR Committee, Concluding Observations on France, CCPR/C/FRA/CO/5, 2015, § 12; HR Committee, Concluding Observations on New Zealand, CCPR/C/NZL/CO/6, 2016, § 15; HR Committee Concluding Observations on Rwanda, CCPR/C/RWA/CO/4, 2016, § 35; HR Committee, Concluding Observations on South Africa, CCPR/C/ZAF/CO/1, 2016, § 43; HR Committee, Concluding Observations on Italy, CCPR/C/ITA/CO/6, 2017, § 36.

information motivated by the requirements of the ultimate demonstration of the truth in a legal case may authorise the Public Prosecutor's Office at the Court of Cassation to prescribe the interception, recording and transcription of correspondence sent by means of telecommunications and information and communication technologies.

Similar protection is afforded to personal data. According to article 131 of the aforementioned Law No. 20/017 of 25 November 2020,

> *The confidentiality of personal data is guaranteed and protected, and their processing is carried out only with the consent of the person concerned or at the request of the prosecutor. In addition, article 132 provides that "the collecting, recording, processing, storage and transmission of personal data take place with authorisation of the user concerned or the competent state authority, in accordance with the article 126 of this law. However, collecting and processing of personal data that reveal racial, ethnic or regional origin, parentage, political opinions, religious or political beliefs, trade union membership, sexual orientation, genetic data or more are prohibited.*

The law refers to a ministerial order which, on the proposal of the Regulatory Authority, will set the conditions and modalities for the collection, recording, processing, storage and transmission of personal data. However, this is still pending.

To assess the compliance of surveillance practises in the DRC, this paper examines three classic conditions for limiting human rights.

A The Condition of Legality

In the sense of human rights instruments, legality means "that which must be established by law".[38] As a condition of the limitation of substantive rights, legality frames state interference in the exercise of rights and freedoms. The condition of legality appears in most of the provisions enshrining relative rights through terms such as

"The law referred to in these instruments may be a law of the State". The law referred to in these instruments can be analysed from both a substantive and a formal perspective. In the formal sense, the law refers to "the work of the legislature" to the exclusion of any other state authority, in application of the principle of the separation of powers. In the substantive sense, legality must be understood as broadly as possible. It cannot be reduced to the mere existence of a written law emanating from parliament. The jurisprudence of the protection authorities interprets legality broadly, conditioning it on the requirements of clarity and accessibility.[39]

With regard to the formal requirement, some Congolese legal texts do not comply with this requirement. This is the case, for example, of Law No. 20/017 of 25 November 2020 on telecommunications and new information technologies. This law regulates privacy and personal data. It was adopted by the Congolese parliament in 2020. However, according to the Constitution, telecommunications and communication do not fall within the domain of the law. Articles 122 and 123 list matters that fall under the law and exclude "telecommunications" in particular and "communication" in general. Article 128 of the Congolese Constitution draws the consequence of such exclusion. According to this provision, "Matters other than those which failing within the scope of law are regulatory in nature. The legal texts regarding these matters may be amended by decree if the Constitutional Court, at the request of the Government, has declared that they are of a regulatory nature by virtue of the preceding paragraph".

38 Article 19, § 2, of the ICCPR.
39 J. Andriantsimbazovina (dir.), *op. cit.*, p. 605.

Some authors justify this situation by an oversight on the part of the legislature rather than a desire to exclude telecommunications and communication from the domain of the law.[40] This legal imbroglio may explain the fact that this law has never been published in the official journal until now. This lack of publication has two consequences. On the one hand, the law cannot impose obligations on individuals in the absence of publication. There is nothing to prevent individuals from taking advantage of an unpublished law. On the other hand, this law applies against the State because the latter cannot invoke the non-performance of its obligations in order to deprive individuals of the benefit of certain rights.[41] This reasoning is based on the adage "*nemo auditur turpitudinem suam allegans*". According to this principle, the state cannot rely on the provisions of a law against an individual when it has not published it in the official gazette.

On the substantive side, the Human Rights Committee had to specify the characteristics of the law. The Committee recommends that any interference with the right to privacy, family, home or correction is permitted by laws that: (i) are publicly available; (ii) contain provisions that ensure that the collection, access and use of communications data are tailored to specific legitimate purposes; (iii) are sufficiently precise and specify in detail the exact circumstances in which such interference may be permitted, the procedures for authorisation, the categories of persons who may be placed under surveillance, the limit for the duration of surveillance; the procedures for the use and storage of the data collected; and (iv) provide effective safeguards against abuse.[42] The legal texts on surveillance do not comply with the requirement of clarity and precision.

For example, Decree-Law No. 003-2003 on the creation and organisation of the National Intelligence Agency (ANR). According to its article 3, "the mission of the latter – the ANR – is to ensure the internal and external security of the State. In this respect, it is responsible for "[…] 3. surveillance of national or foreign persons or groups of persons suspected of carrying out an activitý likely to undermine state security […]". This provision is formulated in a general and ambiguous way. It does not frame the power of the NRA. It served as a lever for the government of former President Joseph Kabila, which had wiretapped some political party leaders, particularly those of the opposition in 2019.

The law on the RAM tax does not comply with this material requirement either. Indeed, since 2020, the government has been collecting IMEI, which is the identifying number of phones, from mobile phone users in the DRC through the Registry of Mobile Devices, RAM. However, the ministerial order does not provide for the procedures for using and storing the collected data, nor does it specify the duration of the exploitation of the data. As such, such a practice is contrary to Article 17 of the ICCPR.

40 P. Mbalanda Kisoka, L'exclusion des télécommunications du domaine de la loi: réflexion sur le bien-fondé d'une révision constitutionnelle, Kinshasa, MBM-Conseil SCA, 2008, p. 11.

41 ECJ, 14 July 1994, *Paola Faccini Dori v Recreb Srl*, Case C-91/92, Digital Rec:ECLI:EU:C:1994:292, § 23.

42 In this regard, see. HR Committee, concluding observations on the United States, CCPR/C/USA/CO/4, 2014, § 22.b; HR Committee, Concluding observations on Great Britain, CCPR/C/GBR/CO/7, 2015, § 24.

B The Condition of Legitimacy

Legitimacy is the second condition of restriction that any interference must meet. According to the dictionary of public international law, legitimacy is a generic term "referring to specific conditions or grounds enshrined in a rule of positive law".[43] The criterion of legitimacy is common to that of legality, namely positive law. The legitimacy or legality of an act is assessed in the light of positive law. To clarify this concept, it should be distinguished from that of legality. In human rights, there are several grounds for restricting rights and freedoms, including public order, public health, public morality, national security, public safety, the reputation of others, the rights and freedoms of others, etc. Article 17 of the ICCPR does not specify the grounds for interference, but it does prohibit "arbitrary interference" in its wording.

With regard to tapping, surveillance and searches, their legitimacy often lies in the prevention of crime and/or the preservation of national order or security.[44] The Committee most often criticises intrusive surveillance powers on the basis of broad and insufficiently defined objectives.[45]

Several reasons are usually given for such surveillance practices. Of these, the grounds of security and protection of territorial integrity coupled with the fight against terrorism are the most relevant. This feature is not specific to the Congolese government. Several countries whose similar practices have been revealed in recent years have stressed that they have proceeded for these same purposes. However, in the Democratic Republic of Congo, the study showed that these surveillance practices are recurrent, especially following political turbulence such those revealed by the clear intention of the regime of former President Kabila to retain power (AE, TP, & Ritimo, 2020). The regime has not hesitated to equip its intelligence services with the most modern technical means, or even to resort to foreign companies to spy on its opponents, activists and even some of the regime's most senior figures suspected of treason. The report further demonstrated that these practices continue under the current regime and are no longer limited to opponents or activists, but also include former leaders who were once perpetrators of such practices. The recent revelations of spying on former authorities, including the former minister of Communication and Media[46] illustrate this. In practice, the DRC uses surveillance to control opponents and spy on the population. As such, such practices do not meet the condition of legitimacy.

43 See. HR Committee, concluding observations on the United States, CCPR/C/USA/CO/4, 2014, § 22.b; HR Committee, Concluding observations on Great Britain, CCPR/C/GBR/CO/7, 2015, § 24.

44 HR Committee, Van Hulst v. Netherlands, const. of 1 November 2004, communication No. 903/1999, § 7.9.

45 HR Committee, Concluding observations on UK, CCPR/C/GBR/CO/7, 2015, § 24.

46 More details on https://www.politico.cd/la-rdc-a-la-une/2021/07/20/rdc-le-rwanda-a-utilise-pegasus-pour-espionner-lambert-mende-albert-yuma-et-jean-bamanisa.html/88863/

C The Proportionality Requirement

In human rights law, proportionality is defined as the balancing of conflicting interests by requiring "a reasonable relationship between the means employed and the end sought".[47] In other words, the measure creating the interference must be, on the one hand, appropriate to the achievement of the legitimate aim pursued (adequacy) and, on the other hand, is the least restrictive measure possible (necessity).

The surveillance measures are not adequate. The means used do not achieve the objective pursued, namely public order. To achieve such an objective, it is not necessary to monitor a large part of the population indiscriminately. The means used to contribute to the storage of data in a part of the population that does not constitute a danger to national security. This is the case, for example, of the IMEIs collected in the context of the RAM tax. Through this tool, the DRC collects the data of telecom users without their consent and in an unlimited manner. The Court of Justice of the European Union considers that "the interference that such a regulation entails on fundamental rights (…) is of a vast scale and must be regarded as particularly serious. The fact that the data is stored without the users of the electronic communications services being informed is likely to generate in the minds of persons concerned the feeling that their privacy is constantly monitored".[48]

Apart from adequacy, the measure is not necessary in a democratic society. Unlike the DRC, which is an authoritarian state, surveillance is used in democratic countries to ensure security and combat crime. In the case of *Hulst v. The Netherlands*, in which the author was convicted of participation in a criminal organisation, the author was subject to surveillance. The HR Committee considers the interception of conversations with his lawyer to be proportionate. According to the Committee, there was no disproportionate interference because the interceptions of the conversations with his lawyer only concerned those in which the lawyer himself was suspected, the professional conversations having remained confidential.[49]

47 J. Andriantsimbazovina (dir.), *op. cit.*, p. 811.

48 Court of Justice of the European Union, *Tele 2 Sverige AB v Post-och telestyrelsen*, judgment of 21 December, 2016.

49 HR Committee, Van Hulst v. Netherlands, const. of 1 November 2004, communication no. 903/1999, § 3, 7.

8. Conclusion and recommendations for surveillance practise that reconcile national security at citizens' rights

This study has shown that digital surveillance in the DRC is multifaceted and constantly increasing, particularly due to the proliferation of new information and communication technologies. Aware of this rapid development, the DRC recently adopted a new legal text, as the texts applicable in this area had become outdated and unsuitable. Although the DRC does not have a specific digital surveillance technology, the study found that some of the practices used by the government deserve to be described as such. In addition, the collaboration or involvement of foreign intelligence companies, particularly Israeli and internet giants Google and Facebook, further amplifies these practices.

Several reasons are generally given to justify this surveillance practises. Among these, the reasons of security and protection of territorial integrity coupled with the fight against terrorism are the most relevant. This feature is not specific to the Congolese government. Several countries whose similar practices have been revealed in recent years have stressed that they have proceeded for these same purposes. However, in the Democratic Republic of Congo, the study showed that this surveillance practises reached their peak in 2018, particularly following political turbulence motivated by the clear intention of the regime of former President Kabila to retain power. The regime has not hesitated to equip its intelligence services with the most modern technical means, or even to resort to foreign companies to spy on its opponents, activists and even some of the regime's most senior figures suspected of treason. The report further demonstrated that these practices continue under the current regime and are no longer limited to opponents or activists, but also include former leaders who were once perpetrators of such practices. The recent revelations of spying on former authorities, including the former minister of Communication and Media, illustrate this.

Finally, the study found that many of these practices conflict with the DRC's human rights obligations, particularly the protection of privacy, personal data, the right to information and freedom of association. Indeed, the exceptions contained in the new law on telecommunications as well as in certain framework laws creating intelligence services or technical services with the mission of monitoring individuals are sometimes misinterpreted, leading to an abuse of power. These findings were confirmed by field data and analysis of the past practices of the various actors involved in digital surveillance in the DRC. The least that can be said is that these practices do not meet the threshold of proportionality and necessity that, in a democratic society, would justify the state resorting to them. Moreover, the legal procedure that would legitimise such practices is not followed and the dangerous nature of persons who have been victims of espionage seems less convincing. In most cases, political differences have been the most decisive criterion for these practices, contrary to the requirements of the law. Therefore, in order to reconcile digital surveillance with the needs of national security and citizens' rights, we make the following recommendations:

8.1 To the Congolese State (political, intelligence and administrative institutions)

- Recognise the role that NICTs play in the promotion and protection of human rights, in particular the rights to privacy, protection of personal data, freedom of expression and information;
- Ensure strict compliance with the procedure established in the new law on telecommunications in any process of interception, storage and surveillance of persons;
- Carry out digital surveillance for the strict minimum of public safety and not to invade privacy or silence dissenting voices;
- Use objective criteria to determine whether a person is a threat to internal or external security, not just political differences;
- Humanise intelligence services, particularly the ANR, so that it is not a repressive machine against voices that dissent from the government, but a technical service at the service of the nation;
- The Regulatory Authority for Posts, Telecommunications and Information and Communication Technologies in Congo should be placed under the control of parliament and not the President of the Republic in order to guarantee its independence;
- The parliament should systematically examine laws that may infringe on privacy and other human rights and propose legal texts that strictly regulate exceptions to the interception and intrusion of personal data.

8.2 To telecommunications companies

- Propose a model general clause, to be signed by customers, which formally sets out the rights and duties of both parties, including the reasons why communications, personal data, etc., may be disclosed to third parties, including the government;
- Provide a mechanism for subscribers whose rights have been violated to obtain redress.

8.3 To the victims of espionage practises

- Be better informed and trained on their rights in the use of NICTs, digital security, particularly that of information relating to privacy, personal data, anonymity and protection against illicit attacks;
- Obtain regular assistance from a technician in order to detect and remedy any espionage practises that may have been committed without their knowledge;
- Take legal action whenever unjustified violations of their privacy or personal data occur, in order to dissuade the perpetrators of these practices and obtain compensation for the resulting damage.

8.4 To civil society and human rights NGOs

- Regularly monitor the development of surveillance practises employed by the government by reviewing their compliance with human rights;
- Conduct advocacy activities with various stakeholders such as the government, parliament, and telecommunications companies to sensitise them on the need for a legislative framework that balances the imperative of national security and human rights;
- Civil society activists should learn about more secure data storage and encryption techniques to counter malicious threats of espionage, wherever they may come from;
- In-depth studies should be conducted at academic institutions to document the existence and scope of digital surveillance practises of various actors and disseminate them to the public for their information;
- Human rights NGOs should assist victims in the quest for justice for damages resulting from digital surveillance practises, including legal support.

Bibliography

Abu-Laban, Y. (2014). Gendering Surveillance Studies: The Empirical and Normative Promise of Feminist Methodology. *Surveillance & Society*, 13, 1, , 44-56.

Agar, J. (2003). *The government machine: A revolutionary history of the computer*, Cambridge, MA: MIT Press.

Ai, I. A. (2021). *La situation des droits humains dans le monde. Rapport 2020-21*.

AE, A. E., TP, T. I., & Ritimo. (2020). RDC-Programme Protection: Fiche Pays sécurité numérique.

Amnesty International. (2007). *République démocratique du Congo Persistance de la torture et des homicides par des agents de l'État chargés de la sécurité*. EFAI.

Anissa, B. (2016). Mise en oeuvre et respect des droits humains à l'ère du numérique: La nécessité d'une évolution d'une évolution du cadre juridique international applicable aux Technologies de l'information et de la communication (TIC). Université du Québec à Montréal, Québec.

AssociAtion for Progressive Communications (APC); Hivos, HumAnist institute for cooPerAtion witH develoPing countries (Hivos). (2014). *Global InformatIon Soclety Watch 2014 Communications surveillance in the digital age*.

ARPTC. (2021). *Observatoire du Marché de la Téléhonie Mobile. Rapport du 1er trimestre 2021*. Kishasa.

Ball, K., Haggerty, K., & Lyon, D. (2012). Introducing surveillance studies, In K. H. Ball, *The Routledge Handbook of Surveillance Studies* (pp. 1-11). New York: Routledge.

Boenisch, G., & Bigot, C. (2011). "Médias et vie privée". *Questions de communication* (http://questionsdecommunication.revues.org/2813).

Cambien, A. (2008). *Une introduction à l'approche systémique : appréhender la complexité. [Rapport de recherche] Centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques (CERTU)*.

Camilla, P. (2020). Rendre visibles les conséquences de la surveillance numérique Le cas du « scandale » Cambridge Analytica. *Open Edition Journals*, 37(2),(https://doi.org/10.4000/communication.13252).

Casilli, A. (2014,). Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée. Jacky Richard et Laurent Cytermann. Etude annuelle 2014 du Conseil d'Etat "Le numérique et les droits fondamentaux". In R. Jacky, & L. Cytermann, *Étude annuelle 2014 du Conseil d'Etat "Le numérique et les droits fondamentaux", La Documentation Française*, (pp. 423-434). Etudes et documents, Conseil d'Etat. halshs-01055503.

Castagnino, F. (2018). Critique des surveillances studies. Éléments pour une sociologie de la surveillance. *Déviance et Société*, 2018/1 (Vol. 42) (https://doi.org/10.3917/ds.421.0009), 9-40.

Cipesa, C. O. (2016). *État des lieux des libertés sur Internet en République Démocratique du Congo 2016: Les stratégies des gouvernements africains pour étouffer les droits numériques des citoyens*.

Corentin, D., Tellier, S., De Cooman, J., Petit, N., Duquenne, E., Lombardo, A., . . . P. (2018). *La vie privée à l'ère des big data dangers & opportunités de la révolution numérique*. Bruxelles.

Cornut St-Pierre, P. (2019). Usages et finalités des registres d'entreprises à l'ère numérique: de l'efficience économique à la surveillance citoyenne des entreprises. *Les Cahiers de Droit,, vol. 60 no 3*, 589-622.

Dcaf, L. C. (2019). *Guide pour la bonne gouvernance de la cybersecurité*. Dakar / Paris / Genève.

De Terwangne, C. (2019). Internet et lA Protection de la vie privée et des données à caractère personneL. In C. De Terwangne, *L'Europe des droits de l'homme à l'heure d'internet*, 325-368.

Donnadieur, G., & Karask, M. (2002). *La systémique, penser et agir dans la complexité*. Éditions Liaisons.

FIACAT; ACAT. (2016). *Rapport alternatif de la FIACAT et de l'ACAT RDC pour l'adoption d'une liste de points à traiter à l'occasion de l'examen du quatrième rapport périodique de la République démocratique du Congo sur la mise en œuvre du Pacte international relatif aux*. Comité des droits de l'homme des Nations Unies 119ème session – mars 2017.

FIDH. (2016). *Il faut mettre un terme à la répression et garantir les libertés d'expression et de manifestation*. Retrieved from https://www.fidh.org/fr/regions/afrique/rdc/il-faut-mettre-un-terme-a-la-repression-et-garantir-les-libertes-d

Forget, C. (2016). Surveillance et vie privée: à la recherche de l'ennemi intérieur. *Dssier*, 15-16.

GEC. (2018). *RDC : les élections de tous les dangers*. Note 3 : La crédibilité des élections en question.

Harivel, J. (2018). *Libertés publiques, libertés individuelles, risques et enjeux de la société numérique* (Vols. NNT : 2018PA01D024 . tel-01889924). Paris,, Thèse, Droit. Université Panthéon-Sorbonne-Paris.

Hcnudh, C. D. (2018). *Le droit à la vie privée à l'ère du numérique*. Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme, Nations Unies .

Henno, J. (2016). La figure de l'oracle dans le discours sur la surveillance numérique. *Revue Française des Sciences de l'Information et de Communication*.

Henri, I., & Kalika, M. (2001). Organisation, technologies de l'information et vie privée. *RePEc*.

Kapinga, S., Kadda, C. et al, (Juin 2021). *Étude sur l'Agence Nationale de Renseignements en République Démocratique du Congo et quelques orientations stratégiques de réforme*. African Security Sector Network (ASSN).

Larsen, M., & Piché, J. (2009). Public vigilance campaigns and participatory surveillance after 11 September 2001, . In S. Hier, & J. Greenberg, *Surveillance: Power, Problems, Politics*, (pp. 187-202). Vancouver,: UBC Press.

Maignien, Y. (2012). Source et fuites : du sens des flux de données numériques. *Revue internationale International Web Journal* (https://doi.org/10.7202/1043664ar), 1-15.

Mayamba, T. (2012). *Mapping Police Services in the Democratic Republic of Congo: Institutional Interactions at Central, Provincial and Local Levels* . Institute of Development Studies (IDS),.

Mayamba, T. (2013). *Building a Police Force 'for the good' in DR Congo Questions that still haunt reformers and reform beneficiaries*. The Nordic Africa Institute.

Murray, H., & Admire, M. (2020). *A Patchwork for Privacy Mapping communications surveillance laws in southern Afric a*. A report for the Media Policy and Democracy Project .

Navarrete, I. (2015). L'espionnage en temps de paix en droit international public. *The Canadian Yearbook of International Law*, 531-565 (doi:10.1017/cyl.2016.16).

Ndiaga, G. (2020 , juin 24). *Surveillance numérique pour combattre la COVID-19 : Le droit à la vie privée et le droit à l'information en péril au Sénégal*. Retrieved from https://www.apc.org/fr/pubs/surveillance-numerique-pour-combattre-la-covid-19-le-droit-la-vie-privee-et-le-droit

Nicolas, H., Miguel, N., Romain, R., Marc-Olivier, K., & Roy, M. (2012). Campagne de collecte de données et vie privée. *Manuscrit auteur, publié dans* "GDR GPL" 12 (https://www.researchgate.net/publication/266502240), 253-254".

Owenga, E. L. (2001). Le respect de la vie privée et les inforoutes en République Démocratique du Congo. *Lex Electronica*, 6(2), Hiver / Winter 2001.

Plan National du Numérique. (2019). *Planation du numérique à l'horizon 2025. Pour une RD Congo connectée et performante*. Kinshasa: Présidence de la République.

Salvas, B. (2001). *La protection de la vie privée sur le Web avec P3P : l'arrimage incertain du technique et du juridique*. Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade Maîtrise en droit (L.L.M.), Univesité de Montréal.

Sanija, A. (2021). La Cour européenne des droits de l'homme et la protection de la vie privée contre la surveillance . *Archives*.

Sfetcu, N. (2020). Contre-espionnage – Communautés épistémiques en UE. *SetThings (18 janvier 2020)* (https://www.setthings.com/fr/contre- espionnage-communautes-epistemiques-en-ue/).

Viana, A. (2021). La surveillance numérique en temps de pandémie – Cité Unie. In Soistier, & J., *Repenser les relations post-coloniales : débattre et restituer ?*

Vuilleumier, C. (n.d.). Espionnage, police et secrets d'État. *La Cité*.

Yende, G., Madawa, Z., Mbakwiravyo, O., Kasimwande, W., Kakule, T., & Mahasano, E. (2020). De la protection des donnees a caractere personnel des internautes en RDC. *Global scientific Journals*, 8(5), 1870-1892.

Annex I. Guides for individual interviews and focus groups

Interview guide for individual interviews and focus groups

Topic: Digital surveillance and privacy: towards a balance between national security and personal data protection

Identification of respondents

1. State services working on security: ANR, DGM
2. Telecommunications companies: Airtel, Vodacom and Orange
3. Political parties (6 parties: 3 from the opposition and 3 from the presidential majority) / Focus Group
4. Citizens' movements: Lucha, Filimbi and the indigen movement / Focus Group
5. Media (RTNC, OKAPI, MAENDELEO, MARIA, RTNK, ISDR) / Focus Group

1. Questions addressed to State services working on security: ANR, DGM

1. What do you understand by the following concepts?
   a. Digital surveillance
   b. Privacy
   c. Personal data.
2. Do you think that digital technology has had an impact on the performance of daily activities in your department? If so, how? If not, why not?
3. Do you think that digital surveillance and other modern means of communication can be useful in the fight against insecurity/crime in the DRC? How and why?
4. And within your service, do you use digital surveillance to fight insecurity and/or for another reason?
5. How would you assess the use of digital surveillance to reduce insecurity, violence and injustice in the DRC?
6. Do you think that digital surveillance is compatible with human rights instruments?
7. And in using digital surveillance, how do you ensure the balance between national security and personal data protection?
8. And looking to the future, what should be done to make digital surveillance effective in the DRC?

2. Questions addressed to the telecommunications companies: Airtel, Vodacom and Orange

1. What do you mean by the following concepts?
   a. Digital surveillance
   b. Privacy
   c. Personal data.
2. What are the most common forms of digital surveillance in the DRC?
3. Tell us briefly about how digital technology has revolutionised the way you deal with your clients.

4. Do you think that digital developments have enabled you to manage, track and monitor your clients? If yes, how? If not, why not?
5. In the course of your daily activities, do you collect data relating to privacy (identities, conversations, etc.)? What measures do you implement to ensure their protection?
6. Are you ever contacted by the State (its services) for investigative or other reasons, in order to provide information about a client's conversations and/or personal data? If so, how do you react? Is the client informed of this procedure?
7. Do you think that such a procedure is in line with the human rights instruments ratified by the DRC?
8. What are the contributions and roles played by communications companies in the fight against insecurity and/or violence in the DRC?
9. What are the main constraints that handicap your activities?
10. What are the strategies to be implemented to ensure digital surveillance compatible with human rights instruments?

3. Questions addressed to political parties (6 parties: 3 from the opposition and 3 from the presidential majority)

1. What do you understand by the following concepts?
   a. Digital surveillance
   b. Privacy
   c. Personal data.
2. What are the most common forms of digital surveillance in the DRC?
3. Tell us briefly about how digital technology has revolutionised your political activities?
4. Do you think that digital developments have enabled you to manage, track and monitor your activities? If so, how?
5. Have you been the victim of digital surveillance by state services in the course of your activities? If so, from which service and what was the motive?
6. Do you think that this surveillance targets political parties differently depending on whether they belong to the opposition or the presidential majority? If so, what are the reasons?
7. Have any members of your party (leaders and activists) been arrested because of publications or messages sent via the NICTs and intercepted by the security services?
8. Some media have revealed that some politicians and citizen movements have been wiretapped especially before the last elections. Do you think these claims are correct? If so, were your party or its members personally targeted?
9. Have you changed your usual means of communication to avoid these practices?
10. Do you think that this practice (digital surveillance) is compatible with the human rights instruments binding the DRC?
11. What strategies should be implemented to ensure digital surveillance is compatible with human rights instruments?

4. Questions addressed to citizen movements: Lucha, Filimbi and the indigen movement

1. What do you understand by the following concepts?
   a. Digital surveillance
   b. Privacy
   c. Personal data.
2. Tell us briefly about how digital has revolutionised your business?
3. What are the most common forms of digital surveillance in the DRC?
4. In the course of your activities, have you been a victim of digital surveillance by state security services?
5. Do you think that this surveillance targets citizen movements, political parties and civil society in general differently? If so, what are the reasons?
6. Have any members of your movement (leaders and activists) been arrested because of publications or messages passed via NICTs and intercepted by security services?
7. Some media revealed that some politicians and citizens' movements were wiretapped especially before the last elections. Do you think these claims are correct? If so, were your movement or its members personally targeted?
8. Have you changed your usual means of communication to avoid these practices?
9. Do you think that this practice (digital surveillance) is compatible with the human rights instruments binding the DRC?
10. What strategies should be implemented to ensure digital surveillance is compatible with human rights instruments?

5. Questions addressed Media (RTNC, OKAPI, MAENDELEO, MARIA, RTNK, ISDR)

1. What do you mean by the following concepts?
   a. Digital monitoring
   b. Privacy
   c. Personal data.
2. Tell us briefly about how digital has revolutionised your business?
3. What are the most common forms of digital surveillance in the DRC?
4. Do you use digital surveillance in your activities (information retrieval and others)?
5. Has your media been a victim of digital surveillance? If so, by whom and for what reasons?
6. Do you think that this surveillance targets the media differently according to their "political affiliation" (opposition and majority)?
7. Have any journalists from your media been arrested because of their information or messages? If yes, who was the author of these arrests?
8. Some media outlets have revealed that some politicians and citizen movements were wiretapped especially before the last elections. Do you think these claims are correct? If so, have you as a media documented these revelations?
9. Have you modified your usual means of communication to avoid these practices?
10. Do you think that this practice (digital surveillance) is compatible with the human rights instruments binding the DRC?
11. What are the strategies to be implemented to ensure digital surveillance compatible with human rights instruments?

Annex II. Qualitative data compilation sheet

1. **Targets:** State services (ANR, DGM); Telecommunications companies (Airtel, Vodacom and Orange), Political parties (6 parties: 3 from the opposition and 3 from the presidential majority), Citizen movements: Lucha, Filimbi and the movement of the indigens and Media (RTNC, OKAPI, MAENDELEO, MARIA, RTNK, ISDR)
2. Target activities related to surveillance

Main theme	Sub-theme	Answers given	Highlights of the interviews	Sources/ quality of respondent	Possible theoretical references (see literature review)
Your understanding of digital surveillance					
Digital surveillance practises	Recurring				
	Characteristics				
	Procedure				
	History of the practices				
Reasons for digital surveillance	Legal basis				
	Reason of security and safety of the State				
Actors	The main actors	State, private and foreign actors			
Surveillance tools					
Reconciliation of digital surveillance practises	Positive	Negative			
Recommendation for the humanisation of digital surveillance					

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.