CHAPTER FOUR

Public control and digital surveillance: Understanding the role of civil society in the DRC

Trésor Maheshe Musole

Introduction

In the Democratic Republic of Congo (DRC), civil society is one of the major players in the civic and democratic arena. It comprises all the organised forces in society outside the state, the family, political parties and the market. These are forces and structures such as associations, non-governmental organizations (NGOs), the press, trade unions, churches and universities (Abega, 2009). Over time, the goals of civil society have changed, owing to shifts in the country's social and political landscape, following similar patterns across three periods (Bugeme, 2020).

After the weakening of the welfare state in the 1970s and 1980s, as well as the agrarian crisis in 1980, civil society turned its attention to rural issues and community health, to the point of being described as 'local development brokers' (De Sardan, 1997). Around 1990, civil society became involved in human-rights issues as a result of development-aid conditionalities imposed on Southern African countries by donors. During the decade of war (1996–2006), the actions of civil society were characterised by a polarisation of discourse to the point of leading to an identity crisis, due to the personal positioning of certain players. From the second half of the 2000s, CSOs turned their attention to

natural resources and the opening up of civic and democratic spaces. Faced with serious human-rights violations and strong competition for natural resources, civil society structures exerted strong pressure on the political and economic players concerned (Cappelle and Custers, 2009), to the point of changing public policies.

With the advent of new information and communication technologies, civil society players are facing new challenges in terms of civic and democratic space. This space has expanded to include online or web-based activities. Citizens are increasingly expressing themselves and exercising their political freedoms online wherever they happen to be. This exposes the structural limits of our democracies. Intelligence services are using electronic surveillance on an unprecedented scale to restrict civic space. Civil society actors, citizens' movements and political opposition are subject to a system of spying and electronic surveillance organised by state services (Maheshe and Mushagalusa, 2021), which is constantly increasing in societies (Salvas, 2001; Abu-Laban, 2014; Castagnino, 2018; Cornut St-Pierre, 2019; Camilla, 2020; Sfetcu, 2020; Vuilleumier, n.d.; Viana, 2021;).

However, civil society organisations in the DRC exert little or no pressure on these new forms of restrictions on civic space and digital democracy. As was the case in the area of sexual violence or the natural-resources sector, there is almost no public control on the part of civil society challenging unjustified secrecy by publicising abuses and organising awareness-raising campaigns. Official institutions such as the courts and parliament do not control this massive surveillance because they are highly politicised. The population is facing unprecedented restrictions on online civic space by government authorities. They justify these restrictions on the grounds of security on digital networks and claims of digital sovereignty. State services restrict civic space by resorting either to electronic surveillance of citizens or to control of the internet.

Faced with this situation, this chapter answers two questions:

1. What are the factors behind the low level of interest among Congolese civil society in the issue of surveillance?
2. How could civil society actions limit the abuses of surveillance?

To address these questions, the study first presents the organisation of Congolese civil society (IV) with the aim of identifying the factors that explain this low level of mobilisation in the face of electronic surveillance. Next, to explain the low level of interest in electronic surveillance among civil society organisations, the study draws on three case studies (V). Finally, the paper identifies the factors that explain civil society's lack of interest (V). Before addressing these questions, it is necessary to examine the methodology (II) and theoretical basis (III) on which this study is based.

Methodology

Understanding the role of civil society requires an appropriate, rigorous and operational methodological approach. The overall methodological approach is based on the systemic approach (Donnadieu and Karsky, 2002; Cambien, 2008). It is fundamentally qualitative, based essentially on documentary analysis, case studies and empirical data.

The literature review highlights the role of CSOs in electronic surveillance. Their organisation and functioning are studied with the aim of elucidating the role of these organisations and the factors explaining their inertia.

The qualitative survey contributes to the collection of empirical data by means of individual interviews. The interview narratives provide further depth to our analysis by means of a questionnaire survey. This methodological choice is explained by the desire to go beyond the framework of theoretical research and involve those on the ground facing the challenges of electronic surveillance.

The case study evaluates the actions of civil society with the aim of engaging CSOs in actions that limit the abuse of surveillance by establishing public control. The case study is understood as 'empirical research that studies a contemporary phenomenon in a real context, where the boundaries between the phenomena and the context are not clear' (Albarello, 2001). It is 'a particularly fruitful form of combination that brings together, in the field, data that can be distinguished around a social sequence circumscribed in space and time' (De Sardan, 2008). In this paper, the case

studies will help to explain the role of civil society in the face of electronic surveillance.

Geographically, the scope of the presentation covers the DRC, focusing on the province of South Kivu. The province was chosen because of the dynamism and fighting spirit of its CSOs. According to Amuli, 'Local civil society in Kivu has been recognised for its combativeness since well before the period of the Sovereign National Conference, and it is above all the ONDGs that are the bearers of this dynamism' (Amuli et al., 2003).

In this province, six individual interviews were conducted with CSOs, lawyers, parliamentarians and so on. The information gathered was supplemented by two studies that had previously involved CSOs. One study looked at the role of civil society in mining governance. Forty-two individual interviews and 17 discussion groups were organised with FDHM's CSO partners, political and administrative authorities and stakeholders involved in the exploitation of mining resources (mining companies and mining cooperatives). In addition, 237 people were interviewed – 194 men and 43 women (CERDHO, 2022). The other studies the actions of CSOs working on natural resources in the DRC in the era of electronic surveillance: 10 individual interviews and 10 focus-group discussions (FG) were conducted with CSOs and citizens' movements working on mining governance in the DRC, security companies and mining companies operating in the sector and based in South Kivu.

Agency and the decolonial approach: The theoretical basis for understanding the role of CSOs

To understand the role of CSOs, the paper uses agency theory. The agency refers to a subject's ability to act autonomously and reflectively (Rebughini and Colombo, 2023). This refers to the possibility of acting in a dissident and innovative way against the forms of domination and construction observed in a society (Rebughini and Colombo, 2023). Theoretically, the doctrine distinguishes between two ways of understanding the notion of the agency. This paper draws on both approaches.

The first approach comes from Western thought, based on the theory of action. According to this theory, the causes of action lie in the actor's

intention (Davidson, 1980). Intention implies a motivational commitment to action (Lyotard, 1991). This motivation is determined by the interests of the actors. Actors act according to whether or not their interests are affected. To understand the role of CSOs, this paper uses the theory of affected interests, which makes this motivational commitment more explicit. From a historical perspective, Annah Arendt associates intention with freedom, starting with Greek philosophy (Arendt, 1978). In ancient Greek society, absolute intentionality was outlawed (Rebughini and Colombo, 2023). In his work, Platon explains it in these terms: '*l'excès de la liberté amène à la tyrannie, qui est la confiscation de la liberté au profit d'un seul tyran. La vraie liberté est maîtrise des passions et obéissance à la raison*' (Platon, 1834). Ultimately, the agency is the freedom of the social actor in relation to social laws or the idea of the sovereign subject and his fantasy of completeness and autonomy (Rebughini and Colombo, 2023). Faced with the norms governing electronic surveillance in the DRC, CSOs are breaking free in order to regain their freedom to act. Resilience enables them to survive in a repressive environment.

A second approach to the agency comes from the American sociological tradition influenced by pragmatism. According to this approach, the agency is not based on the subject, but rather on action. This conception rejects the agent/structure dualism (Rebughini and Colombo, 2023). It involves a decentring or deconstruction of the subject. The agency implies a relational process of contextualised interaction and not a permanent struggle between the agent and social structures (Goodman, 1995). As such, action is influenced by the cultural and material characteristics of the environment (Rebughini and Colombo, 2023). In this way, the agency ceases to be an ideal characterised by the agent's intention and becomes the product of human interactions, the flow of adjustments and temporal constraints (Wright Mills, 1966). Without being the fruit of a single actor, the agency is the result or attribute of a network of given actors. It comprises the result of recursive events that interact. It is sometimes influenced by the social environment, coloniality. The coloniality refers to an approach that questions the structures of power and thought inherited from colonialism (Fanon, 1961). Decolonial approaches intervene at this level to understand the subject/structure relationship, which is sometimes explained through colonial thought patterns that characterise the social environment.

In this chapter, the agency measures the influence of norms and structures of thought or power in the role of CSOs in the field of electronic surveillance. It looks at the extent to which CSOs are free to act. For Hobbes, the freedom to act is only realised in situations where there are no obstacles, shackles or imprisonment (Hobbes, 2000). In this sense, anything that is not determined to act by any external cause should be called free (Bugeme, 2020). In the DRC, the public authorities restrict civil society initiatives by adopting restrictive legislation. This contributes to the restriction of civic space.

Faced with such restrictions, CSOs often adopt resilience strategies that run counter to public policy. They develop practices that fall outside the law. They are described as practices that are subversive of social laws. Their actions can be explained in part by the margins of choice and the degree to which their interests or those of the population are affected. In 2020, for example, all the CSOs protested against the public policies introducing the RAM tax, to the point of getting the government to back down. Without being contradictory in itself, this situation can be explained by the agency. In social sciences, the agency is used to explain social construction. As such, it becomes not the fruit of the will of a single actor, but the result of recursive events. The combination of these different events makes it possible to explain the social phenomenon.

Organisation and functioning of civil society: A justifying factor for the lack of interest in public monitoring of surveillance?

According to the civil society coordinator in South Kivu, 'there is no specific CSO activity in the area of electronic surveillance. CSOs only intervene when networks are disrupted or tariffs are overcharged. That's when CSOs get organised to make demands.'[1] This statement raises the question of the reasons for this lack of interest. To answer this question, the paper focuses on the organisation and functioning of civil society. The aim is to ascertain whether the organisation and operation of civil society are a factor in explaining this lack of interest.

1 Source: Interview with NB, 12 July 2024.

Civil society is an umbrella organisation for not-for-profit associations whose legal status is based on Law No. 004–2001 on 20 July 2001, laying down general provisions applicable to not-for-profit associations and public-utility establishments. According to a more traditional definition, it includes all the organised forces in society outside the state, the family, political parties and the market. These are forces and structures such as associations, NGOs, the press, trade unions, churches and academics (Abega, 2009). In South Kivu, for example, the organisation of civil society is based on the South Kivu Civil Society Charter and the internal regulations. According to article 1er of the Charter, civil society is understood to be a grouping of structures and associations coordinated and organised at different levels of service for the vital interests of the people. It does so collectively or through the specialised mechanisms of its components.

In organisational terms, the diversity of associations makes it difficult to clearly identify the components of civil society. This difficulty can be explained by the diversity of the social-mobilisation framework, characterised by the nature of the actors (media, private institutions), the area of intervention (urban or rural) and the mobilising issues (Abega, 2009). Despite this difficulty, the doctrine classifies organisations into several components (Yamba Yamba, 1998). These include cooperative associations, cultural and sports associations, free and independent press associations, student associations, women's associations, humanitarian and philanthropic associations, learned and scientific associations, corporations, professional orders and associations, churches, youth movements, human-rights NGOs, development NGOs, employers' unions and workers' unions (Bugeme, 2020).

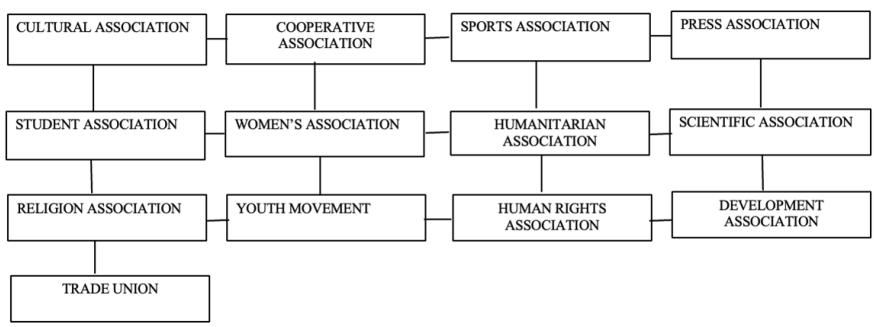

Figure 4.1: Composition of civil society in South Kivu. © Author.

This figure shows the diverse composition of civil society in South Kivu. The CSOs are diverse and varied. They pursue various objectives ranging from the protection of women's rights to religious associations. Given the diversity that makes up civil society, there are some coordination problems.

In terms of how it operates, the components of civil society come together in networks or thematic groups in order to frame their aspirations and strengthen their ambitions. In South Kivu civil society has 26 thematic groups, including Mining, Democracy and Elections, and Human Rights. Alongside the thematic groups, operational networks are emerging. In South Kivu, there are currently two major operational networks that act like NGOs in their own right, because they negotiate and receive funding while carrying out actions (Bugeme, 2020). These are the Conseil Régional Des Organisations Non Gouvernementales de Développement (CRONGD) and the Réseau des Associations des Droits de l'Homme du Sud-Kivu (RHADOSKI).

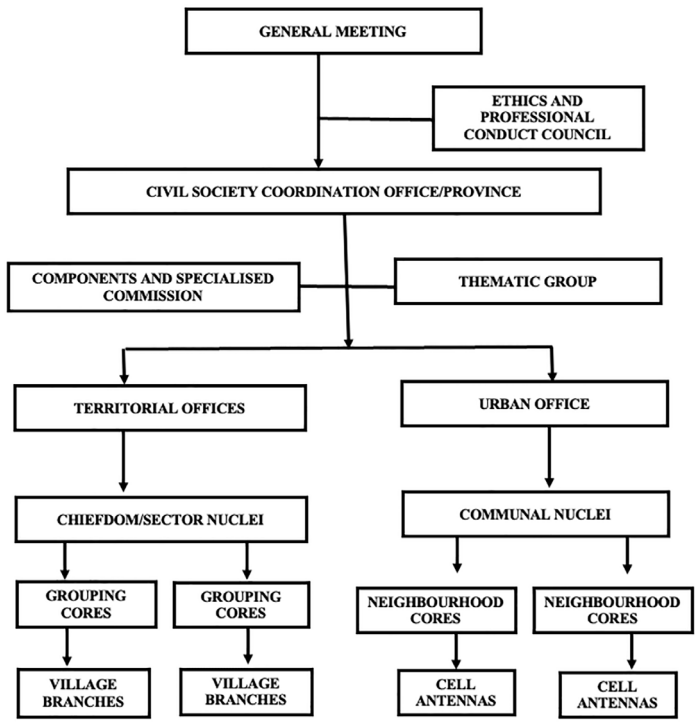

Figure 4.2: The organisation and functioning of civil society in South Kivu. © Author.

The figure above summarises the organisation and functioning of civil society in South Kivu. The organisational structure of civil society is characterised by a certain hierarchy, but CSOs act independently. At the top is the General Assembly, which brings together all the organisations that make up civil society. It is the plenary body responsible for giving broad guidelines and appointing the members of the coordination bureau. The office is responsible for coordinating the activities of all the components, although the CSOs retain their independence. The coordination office is represented in all the administrative subdivisions of South Kivu province. The aim is to ensure that civil society is represented in all parts of the province, including the remotest corners such as villages.

Based on this organisational structure, two observations can be made regarding public control of electronic surveillance in the DRC.

Firstly, there are almost no civil society organisations working in the field of electronic surveillance. In South Kivu there is only one organisation working in this field. This is the Partnership for Integrated Protection (PPI), which works in three areas: (1) documenting and preventing the control of information during the electoral period in the Democratic Republic of Congo; (2) training in digital security; and (3) setting up an online assistance platform on digital security. However, in the DRC, CSOs face restrictions on online civic space by government authorities. These restrictions are based on digital-network security and claims to digital sovereignty. The DRC government wishes to exercise control over digital activities. In the National Digital Plan, the President of the Republic expresses his desire 'to consolidate digital sovereignty' (DRC, 2019, p. 120). State services restrict civic space by resorting either to electronic surveillance of citizens or to internet control. This control is achieved by cutting off the internet, excluding people from the domain and refusing to liberalise the internet.

Secondly, there is no place in the civil society organisation chart for public monitoring of electronic surveillance. There are no components or thematic groups interested in these issues. This lack of interest is partly due to the absence of players in this field. However, public control of electronic surveillance is included in the activities of two thematic groups, namely Democracy and Human

Rights. Electronic surveillance sometimes involves restrictions on civic and democratic space. It also leads to the manipulation of personal data, which constitutes a violation of privacy. As such, CSOs should deal with it within existing thematic groups without having to create new structures. Faced with this situation, and with the advent of decentralisation, Congolese legislators are trying to put civil society back at the heart of security issues and electronic surveillance.

In 2013, the legislature adopted decree no. 13/041 on 16 September 2013 on the creation, organisation and operation of local community safety councils. The law invests these councils with two main missions. On the one hand, it seeks comprehensive and sustainable solutions to problems of public safety, tranquillity and health, within the jurisdiction of the ETDs (art. 3). This involves implementing the local community safety plan. They are also involved in monitoring and evaluating the annual or multiannual community safety plan (art. 4). Given that electronic surveillance is one of the key security issues, there was reason to be hopeful. The Council is made up of a number of leading figures, including public authorities and CSOs. Such a composition brings the security services closer to the local population for whom they have been invested. With the participation of CSOs in such local structures, the protection of the local population should be at the heart of the security services. However, the implementation of this structure is struggling. Local community security councils do not operate throughout the DRC, owing to a lack of political will (Hoebeke et al., 2019). Their establishment is therefore conditional on the adoption of the Prime Minister's decree setting out the terms and conditions of their organisation.

In 2023, the legislature adopted Ordinance-Law No. 23/010 of 13 March 2023 on the Digital Code. Article 262 of the law created a Data Protection Authority (DPA). The legislator assigns it to the main task of monitoring compliance with the protection of personal data (art. 263). The Data Protection Authority is made up of three bodies. These are the Plenary Assembly, the Bureau and the standing committees (art. 264). In the composition of this body, the legislator reserves two places out of nine to two components of civil society,

including the bar and the representative of employers' organisations (art. 266). However, this structure, like the previous one, is still awaiting the Prime Minister's decree setting out the organisation and operation of the DPA. Despite the forthcoming decree, the authority's scope of action remains limited because the future ordinance will not be able to take account of personal data controlled by the security services.

Three case studies: An illustration of civil society's lack of coordination

Most of our respondents said that CSOs undertake very little action in relation to electronic surveillance. According to NB, 'There are no specific activities in this area except when there are network disruptions or overcharging, which is when civil society gets organized to make demands and find out what is going on.'[2] As for NA, 'There are no general joint actions, but there are certain associations that organise in-house training to detect whether we are being monitored and the practices and tricks that we can put in place to escape control.'[3] However, the absence of coordinated action should not detract from the existence of electronic surveillance carried out by state services. According to NA, 'public authorities and socio-political actors are tracked and sometimes geo-located.'[4] Faced with this difficulty, this section examines cases in which the authorities have resorted to electronic surveillance. The aim is to analyse the actions of CSOs against such measures.

To illustrate the role of CSOs in monitoring surveillance, the presentation focuses on three case studies. The aim is to analyse them in order to understand the actions of civil society in the face of the phenomenon of surveillance. This study attempts to understand the low interest of civil society organisations in electronic surveillance through the behaviour of the actors.

2 Source: Interview with NB, 12 July 2024.

3 Source: Interview with NA, 11 July 2024.

4 Source: Interview with NA, 11 July 2024.

RAM case

In 2020, the Autorité de Régulation des Postes et Télécommunications (ARPTC) decided to levy the Mobile Appliance Register (RAM) tax. This government has several objectives. Firstly, it justifies the levying of this tax by its concern to combat the circulation of counterfeit telephones. Secondly, it is intended to combat the theft and counterfeiting of mobile terminals. Finally, through this tax, the government wants to protect the health of users against the toxic effects of devices that do not comply with local and international standards, and to increase the security and quality of service of mobile networks in DR Congo. CSOs have never been convinced by this argument, as one respondent told.[5]

In 2022, the CSOs demanded that the Congolese government abolish the RAM tax and reimburse the deductions made between September 2020 and February 2022. They took several steps.

Firstly, they are taking criminal action against the government's decision. The Comité Laïc de Coordination (CLC), a group with close ties to the Catholic Church, is bringing a civil action against the four telecommunications companies in a criminal trial. It accused them of having taken millions of dollars from their subscribers' mobile phones between September 2020 and February 2022 through a fee of between $1 and $7 per year. According to the NA investigator, this decision constitutes fraudulent misappropriation of sums belonging to others. This is an offence of theft under the Congolese Criminal Code.[6]

Secondly, the CSOs are organising public demonstrations alleging that the RAM tax is illegal. They base their argument on the constitutional principle of the legality of taxes. In the DRC there are no legislative texts instituting this tax. It is a government initiative in violation of the Constitution. In addition, the CSOs note the effects of nonpayment of the RAM tax. In the event of nonpayment, mobile-phone owners run the risk of disconnection or blocking of the network to millions of young people and women whose cost of living

5 Source: Interview with NB, 12 July 2024.

6 Source: Interview with NA, 11 July 2024.

remains low. To force the government to withdraw its decision, 'CSOs are organising sit-ins at all telecom companies to demonstrate their refusal to pay the RAM tax levied by them.'[7] All these actions are supported by the media through reports and radio broadcasts.[8]

Thirdly, the CSOs are carrying out systematic monitoring of the RAM dossier. The coordination office is leading this monitoring through the South Kivu consumers' league (Licoski). They are able to put a figure on the losses incurred by the inhabitants of South Kivu as a result of the RAM tax.[9] According to one respondent, thanks to the work of CSOs in South Kivu, parliamentarians have taken up the issue by questioning the Minister for New Information Technologies. Not only was the tax illegal, but several million dollars had been misappropriated.[10] Failing to pass a motion of no confidence in the minister, the government abolished the RAM tax in March 2022 following strong pressure from CSOs.

The decision to withdraw the RAM tax was based more on relieving the tax burden than on electronic surveillance. In this case, the government demonstrated its ability to access any subscriber's phone and disconnect it at any time, either globally or in a targeted manner. This enables it to manipulate the personal data of millions of subscribers. The technology used to collect tax enabled the government to restrict access to certain mobile-phone functions. According to one interviewee, the government is proving that it can access every subscriber's phone. It can also disconnect them at any time globally or in a targeted manner. Millions of Congolese were surprised to see their access to certain functions of their mobile phones restricted because they had not paid this illegal tax.

In addition to disconnecting SIM cards from the network, the government acknowledged during a parliamentary hearing with the Minister of New Information Technologies that 'RAM offers solutions that, in collaboration with the security services, can combat kidnapping and other crimes through the geolocation of mobile

7 Source: Interview with CM, 17 July 2024.

8 Source: Interview with PM, 19 July 2024.

9 Source: Interview with NA, 11 July 2024.

10 Source: Interview with NB, 12 July 2024.

devices.'[11] Geolocation makes it possible to indicate 'the geographical position of the terminal equipment of a user of an electronic communications service' (Directive 2002/58/EC OF THE EUROPEAN PARLIAMENT). It allows the movements of an individual to be tracked in real time or their presence at a given location to be verified. On phones, geolocation can use three techniques: 'First, a mobile phone can be "pinned", i.e., identified by the nearest base station that identifies its signal. Secondly, the interface may use a satellite geolocation service, such as GPS (Global Positioning System). Thirdly and finally, Wi-Fi technology can also be used to locate an interface' (David Lefranc, Droit des applications connectées – Applications – réseau – interfaces, Larcier, Brussels, 2017, § 994). According to an employee of a telecommunications company, 'the government can use the IMEI number to link communications to a specific device, which will facilitate both the interception of communications and geolocation'.[12]

Faced with this situation, CSOs expressed fears that the government would use this technology to block all critical voices or control citizens' communications.[13] Their actions helped influence the public policies implemented by the government. Indeed, when the Digital Code was adopted in 2023, it limited the use of geolocation and wiretapping. Articles 186 et seq. of Ordinance-Law No. 23/010 on the digital code stipulate that all processing of personal data must be declared to, or authorised by, the Data Protection Authority, failing which it is unlawful. However, intelligence services are not affected by this restriction because the Digital Code does not apply to such structures.

11 Response from His Excellency Augustin KIBASSA MALIBA, Minister of Posts, Telecommunications and New Communication Technologies, to the oral question with debate on the Mobile Device Register (RAM) asked in the National Assembly by the Honourable MISARE MUGOMBERWA Claude, available at https://lesvolcansnews.net/2021/10/14/affaire-ram-integralite-de-la-reponse-du-ministre-des-pt-ntic-aux-deputes-nationaux/.

12 Source: interview with CT, 15 July 2024.

13 Source: interview with NB, 12 July 2024.

Heri Kalemaza case

The tribunal de grande d'instance de Bukavu prosecuted Heri Kalemaza for attempting to undermine the honour and reputation of the provincial governor of South Kivu. The prosecutor accused him of having defamed the governor of South Kivu in the WhatsApp group 'Unis par le droit/ UOB'. He is accused of several acts. Firstly, the defendant accused him of embezzling 3,5000,000 dollars borrowed from the RAWBANK bank. Secondly, the defendant alleged that the governor hacked into the accounts of the province of South Kivu in order to organise an unspeakable tax evasion (Tribunal de paix de Bukavu, 2020).

In judgment RP 3386/ III of 30 September 2020, the Tribunal de Paix sentenced him to a fine of 250,000 Congolese francs for the offence of defamation. The Court based its decision on the act of imputation and the publicity required to commit such an offence. With regard to the act of the imputation, the Court held that the defendant had published these facts 'in the WhatsApp group "Unis par le droit/ UOB", on 26/12/2019, 27/01/2020 and January 2020 respectively' (Bukavu Peace Court, 2020). With regard to the act of publicity, the Court based its reasoning on the defendant's writing broadcast in public in the same WhatsApp group 'Unis par le droit/ UOB'. According to the Court, 'although it is a virtual environment, the WhatsApp group is accessible to 70 interactive people. It is certain that more than one of them read these messages. These kinds of digital platforms are eminently public, which is why they are called social networks' (Tribunal de paix de Bukavu, 2020).

Ultimately, the Court convicted the defendant without demonstrating how he accessed the content of the WhatsApp messaging service. Given that this messaging system is protected by encryption, access to the content can be explained in several ways. First, access to the content may be justified by the composition of his group. Heri Kalemaza was part of a WhatsApp group composed of several people. Some of them allegedly collected the data and passed it on to the provincial authorities. Secondly, access to the content was the result of surveillance carried out by the intelligence services. According to the person concerned, 'there is nothing to rule out the

possibility that ANR agents joined the WhatsApp group using false identities to intercept communications'. The context at the time was conducive to this, as the case comes at a time when 'dozens of people who have criticised government policies, particularly on social media, have been subjected to intimidation and threats, beatings, arrests and, in some cases, prosecution' (Human Rights Watch DR Congo, 2020). There is strong pressure on opponents through the strengthening of surveillance and surveillance capabilities at the level of state structures. According to the CIPESA NGO report, 'Congolese government bodies have, in the past, made requests to telecommunications companies to intercept communications or disclose customer data (...). Sometimes, political authorities do not need to go through official channels for personal interests. For example, it has been reported that President Kabila hired an Israeli company, Black Cube, in June 2019 because he wanted to know everything about his political opponents, but also about his own troops, where traitors might be hiding. Israeli intelligence agents are said to have taken up residence at the Grand Hotel in Kinshasa to carry out, among other things, telephone tapping – an allegation they have denied' (CIPESA, State of Internet Freedoms in the DRC 2019 – Mapping trends in government control of the internet, 1999–2019, January 2020, p. 12).

Through such acts, the government is restricting digital civic space by affecting online democracy. This limits freedom of expression, leading CSOs to censor themselves. The government controls digital space without the need for electronic surveillance.

Unlike the RAM case, the case of Heri Kalemaza did not provoke a strong mobilisation of CSOs. In an interview, a respondent criticised the variable geometry of CSO involvement in Bukavu.[14] There are several explanations for this situation.

The first explanation lies in the political nature of the dispute. One respondent explained the situation as follows:

> There was no strong mobilisation around the Heri Kalemaza case. This is one of the weaknesses of the CSOs in Bukavu.

14 Source: Interview with HK, 15 July 2024.

> The reason is as follows. Heri Kalemaza wore a political hat. He was a member of the Congolese Party for Progress (PCP). As such, he could not benefit from CSO support because he did not fall within the code of human rights defenders who must be accompanied in such cases. I did not agree with this approach (...).[15]

It is clear that both the victim and the accused are members of political parties. The second explanation lies in the issue of human rights. According to one interviewee, 'human rights is an issue reserved for the elite of society. The rest of the population is not concerned'.[16] As long as the arrest of an individual in violation of his or her rights does not affect the interests of the entire population, CSOs are not prepared to take up the cause. It is an isolated case with no impact on the household basket, as was the case in the RAM affair.

Despite this low level of support, the Court upheld the minimum sentence following pressure from some sections of society. He regained his freedom after conviction because the length of the sentence was equivalent to the number of days spent in detention. This logic was also followed in the Stanislas Bujakera case.

Stanislas Bujakera case

In the case of Stanislas Bujakera, the Kinshasa/Gombe High Court sentenced the correspondent of the magazine *Jeune Afrique* on 18 March 2024 to six months' imprisonment and a fine of 1 million Congolese francs. The court accused him of having committed 'forgery', 'forgery of documents', 'use of forgeries', 'propagation of false rumours' and 'transmission of an erroneous message'. He is charged with having shared a false document from the Internal Security Department of the National Intelligence Agency (ANR) in a WhatsApp group on 3 September 2023. The charge was based

15 Source: Interview with NA, 11 July 2024.

16 Source: Interview with HK, 15 July 2024.

on a digital analysis of the metadata. He was accused of transmitting false messages via a computer system. The Congolese state was prosecuting him for sending the false message about the investigation into the death of Mr Cherubin Okende via a fabricated ANR report to the WhatsApp accounts of individuals clearly identified in the judgment (10th page). The Congolese state used surveillance software to detect these transmissions.

The court based its conviction on several reports demonstrating that 'thanks to the MD-NEXT used via Kali Linux 22; 01.lts, the number +243823327460 used by the defendant BUJAKERA was identified through the Internet Protocol address (public IP address): 192.162.12.04, as being the first distributor of this fabricated report on WhatsApp, and that the experts traced the numbers attached to clearly identified recipients' (26th page). Consequently, the Court found 'this charge established in fact and in law and sentences him to six months (6 months) of principal penal servitude' (26th page).

For its part, the journalist's defence team demonstrated that such an analysis was unfounded for technical reasons. Indeed, there was no evidence that this address was used by the journalist's phone. The IP address in question was assigned to a web server located in Spain. The Telegram and WhatsApp platforms from which the message was allegedly sent did not allow messages to be traced or metadata to be stored that would enable them to be identified (Kinshasa/Gombe High Court, 2024).

In the DRC, as in many countries, states use technological and digital advances to carry out preventive surveillance in the name of national security in general and, in particular, in the name of the fight against terrorism (https://www.radiookapi.net/2024/02/24/actualite/justice/felixtshisekedi-jai-decide-de-me-meler-du-dossier-de-larrestation-du).

In countries with 'authoritarian' governance such as the DRC, digital surveillance serves as both a repressive and a destructive lever for those in power. With the advent of the Digital Code, the legislature established the National Cybersecurity Agency, entrusting it with several missions (Digital Code, Articles 275 to 280). From now on, this agency will intercept not only personal data but also, and above all, citizens' conversations (AE, A. E., TP, T. l., & Ritimo

(2020) DRC Protection Programme: Country Profile on Digital Security). In most cases, these practices are justified on grounds of national security.

In this case, journalist Stanislas Bujakera was subject to double surveillance of his telephone conversations. Prior to this, the defendant was subject to electronic surveillance of his conversations by the ANR. When he was arrested at Ndjili airport by the ANR, the authorities accused him of transmitting false messages and spreading false rumours (p. 12). Such accusations can only be based on increased surveillance by the authorities. Subsequently, the court ordered that his various conversations be examined by independent experts in order to establish the truth. However, these government interferences are contrary to freedom of expression (Const. Art. 23) and privacy (Const. Art. 31). As the guarantor of freedoms, the judge should have examined the proportionality of such surveillance measures. Instead, he convicted the defendant on grounds that raise a number of questions.

In his reasoning, the judge referred to the IP address to attribute the transmission of the message to the defendant's telephone. According to the court, 'the number used by the defendant BUJAKERA was identified through the Internet Protocol address' (p. 26). This reasoning raises the question of the role of the IP (Internet Protocol) address in electronic surveillance. The IP address is a unique identifier for any device connected to the internet (a computer, smartphone, tablet or any other connected device). Each device is assigned an IP address that uniquely identifies it and allows it to communicate with other devices on the internet. IP addresses play several roles, including user identification, online activity tracking, access blocking, criminal investigations, government surveillance and so on.

However, when it comes to electronic surveillance, it does not apply to applications that use end-to-end encryption. Several messaging applications have integrated this technology to ensure a level of confidentiality. This is the case with Signal, WhatsApp and Telegram. Through the end-to-end encryption used by these devices, data is exchanged directly between end users without passing through a centralised server. In this case, the IP addresses

of the devices involved in the communication were used to route the data directly between them, without passing through an intermediate server. The purpose of encryption is precisely to solve the problem at its root by not allowing the server to read everything between senders and recipients. The message remains encrypted from one end (the sender) to the other (the recipient), without ever being decrypted between the two points, hence its name. This technique offers users several advantages, including increased confidentiality, protection against data leaks, reduced risk of espionage, data integrity, protection against government requests, increased user confidence, privacy protection and so on.

Given this end-to-end encryption, in this particular case, the government could not identify Stanislas Bujakera as the author of the message. Technically, this was therefore impossible. This case highlights the difficulty for judges to protect fundamental rights in the face of security imperatives. In such a context, the government carries out electronic surveillance of citizens without the judge being able to stop or control it. Once such intrusions are provided for by law and justified on security grounds, the judge should examine them in the light of the principle of proportionality. Otherwise, he sacrifices fundamental rights on the altar of security imperatives.

Although most of the people we interviewed in South Kivu were not familiar with this case, it had been the subject of strong mobilisation by CSOs in the DRC, particularly the 'Press and Media' component.

Initially, the international press were very active. All the organisations that defend journalists were mobilised around this issue. Reporters Without Borders (RSF) devoted an investigation to the case.[17] According to an interview with a journalist, 'this strong mobilization can be explained by the fact that the journalist worked for an international media, namely Jeune Afrique. The response would

17 RSF investigation. Stanis Bujakera case in the DRC: the journalist is not the author of the note for which he is facing 10 years in prison, available at https://rsf.org/fr/enquête-rsf-affaire-stanis-bujakera-en-rdc-le-journaliste-n-est-pas-l-auteur-de-la-note-pour

not have been the same if it had been a journalist working locally.'[18] At every press conference abroad, the Head of State had to answer a question about this affair. In an interview with RFI and France 24 on 16 November 2023, the President of the Republic said the following: 'I am neither behind his arrest nor pulling the strings so that he can be brought to justice. I cannot intervene,' Félix Tshisekedi replied to journalists Marc Perelman and Christophe Boisbouvier. 'I will only intervene later, perhaps, if he is convicted, for an amnesty, a pardon or whatever. But at this stage, I have nothing to say.'

Secondly, the local media mobilised alongside their international partners through the #FreeStanis campaign and the organisation of public events. At a special press briefing in Kinshasa with the Minister of Communication on 22 February 2024, the President decided to get involved in the case, saying: 'Journalist Stanis Bujakera may be a victim of the dysfunction of the Congolese justice system,' and promising that on Saturday, 22 February he would inquire about his case with the justice system, which he described as 'sick'.[19]

Thanks to this strong mobilisation, the authorities had to change their perception of Stanislas's case to the point of influencing the Court's decision in such a way that he was released despite the conviction. Instead of releasing him, the authorities sentenced him to six months' imprisonment. However, he had already served his sentence. The sentence was therefore equivalent to an acquittal. It is not clear what impact this case will have on electronic surveillance.[20] Although the CSOs obtained the release of their colleague, they never asked for the law authorising the ANR to carry out electronic surveillance to be amended.

Beyond the strong mobilisation of CSOs, this case raises the question of the role of the IP (Internet Protocol) address in electronic surveillance. According to one interviewee, the IP address is a unique

18 Source: Interview with PM, 19 July 2024

19 Radio Okapi, 23/2/2024 https://www.radiookapi.net/2024/02/24/actualite/justice/felixtshisekedi-jai-decide-de-me-meler-du-dossier-de-larrestation-du).

20 Source: interview with P.M., 19 July 2024

identification tool for any device connected to the internet (a computer, smartphone, tablet or any other connected object). Each device is assigned an IP address that uniquely identifies it and enables it to communicate with other devices on the internet. The IP address plays a number of roles, including identifying users, monitoring online activities, blocking access, criminal investigations and government surveillance.[21]

However, electronic surveillance does not apply to applications using end-to-end encryption. Several messaging applications have integrated this technology to ensure a level of confidentiality. These include Signal, WhatsApp and Telegram. Through the end-to-end encryption used by these devices, data is exchanged directly between end users without passing through a centralised server. In this case, the IP addresses of the devices taking part in the communication are used to route the data directly between them, without going through an intermediary server. The aim of encryption is precisely to solve the root of the problem by not allowing the server to read everything between sender and recipient. The message remains encrypted from one end (the sender) to the other (the recipient), without ever being decrypted between the two points, hence its name. This technique offers users a number of advantages, including increased confidentiality, protection against data leaks, reduced risk of espionage, data integrity, protection against government requests, increased user confidence and protection of privacy.[22]

Given this end-to-end encryption, the government could not identify Stanislas Bujakera as the author of the offending message. Technically, this was impossible unless the sender used a VPM that dynamically assigned IP addresses. The court did not demonstrate this.

In view of the above, the mobilisation of CSOs is mixed and varies from one case to another. The presentation will now focus on the factors that explain such actions. The aim is to understand the reasons for this variable-geometry mobilisation of CSOs in the face of cases of electronic surveillance.

21 Source: Interview with C.M., 17 July 2024.

22 Source: Interview with C. M., 17 July 2024.

Factors explaining the low mobilisation of CSOs

In the DRC, the future of digital freedoms is at the heart of the news. Citizens are faced with contradictory situations. The exercise of their digital freedoms contrasts with policies aimed at narrowing the space for online freedoms. Over the past few years in several Central African countries, and particularly in the DRC, the future of digital freedoms has been at the heart of the news, especially where liberal democracies are concerned (information sharing, free expression, calls for uprisings and so on). On the one hand, internet users are faced with situations that at first sight seem contradictory, characterised by the availability of online solutions and, on the other, the strengthening of a balance of power that is increasingly unfavourable to public freedoms. On the one hand, there are emerging aspirations to benefit from certain digital freedoms. On the other, there are government strategies to regulate online activities.

However, CSOs exert little or no pressure on these new forms of restriction of civic space and digital democracy. The case studies demonstrate this. There is little or variable mobilisation on the part of CSOs. During the interviews, the interviewees identified the strengths and weaknesses of CSO mobilisation. These are endogenous and exogenous causes. The aim of the presentation is to elucidate their scope.

Endogenous factors

There are a number of reasons for the low level of CSO involvement in the government's electronic surveillance.

Firstly, the lack of motivational commitment on the part of the population justifies the low level of mobilisation of CSOs. According to one interviewee, 'human rights violations and electronic surveillance only concern the elite of the Congolese population. As long as the population as a whole is not affected by public policies, the mobilization of CSOs will remain lacklustre'.[23] In the RAM case, CSOs mobilised because all telephone holders were subject to the RAM

23 Source: Interview with HK, 15 July 2024.

tax without discrimination. Unlike the RAM case, CSOs did not take up the cause of the Heri Kalemaza case, which was considered to be an isolated conflict between political players. This situation can be explained by the agency theory. According to this theory, the causes of action lie in the actor's intention (Davidson, 1980). Intention implies the actor's motivation, which must be proportional to the interests involved. The theory of affected interests, a variant of the agency, provides a better explanation for this low level of mobilisation. According to this theory, membership of a state political community presupposes the existence of common interests that may be affected by a national decision (Beckman, 2006). Used to exclude foreigners from exercising their political rights, this theory explains the low level of mobilisation of CSOs. CSOs can only be mobilised if the interests of the population are affected by public policy. La Fontaine's famous maxim is eloquent: *'ILS NE MOURAIENT PAS TOUS, MAIS TOUS ÉTAIENT FRAPPÉS'* (La Fontaine, 1678–79). If they are not all struck down, public control of surveillance will remain a pious hope.

Secondly, the organisational structure of CSOs in South Kivu also explains this low level of mobilisation. According to one interviewee, 'there is no thematic group within civil society devoted to electronic surveillance. Although this issue could be included in existing themes such as democracy or human rights, CSOs are not equipped.'[24] However, their membership of this thematic group contributes to CSO capacity building. The latter is defined as a deliberate process that increases the capacity of an individual, group, organisation, network or system to improve or develop new knowledge, skills, attitudes (KSAs), systems and structures needed to function effectively, work towards sustainable development and achieve goals (CRS, 2017). CSOs understand capacity building as 'a training package' or 'upgrading actors'. However, there is no such training for CSOs. Another interviewee said that 'these days there are one or two organisations that train CSOs to protect themselves against electronic surveillance techniques'. CSOs do not have a holistic approach to this problem. This is a weakness on their part. Thus, in

24 Source: Interview with NB, 12 July 2024.

the RAM case, although the mobilisation was a success, the CSOs reduced their actions to withdrawing the tax without demanding an end to the monitoring of telephones by state services. This situation can be explained in terms of agency. An individual's actions are influenced by the environment. Faced with a social environment characterised by a lack of capacity building, there is no reason to expect mobilisation in the future.

Exogenous factors

Based on the interviews, the study identified several factors that are not directly related to CSOs. One interviewee revealed that 'the relationship between CSOs and donors is marked by colonialism. According to him, although CSOs are described as partners by donors, they remain in a completely unequal relationship. Their relationship is tinged with coloniality. This concept[25] 'reflects the material and symbolic relationship of domination of Europe over the rest of the world' (Le Petitcorps and Desille, 2020). The aim is to see to what extent and how colonial conceptual and ideological thought patterns are reflected in a country's public policies (Spijkerboer, 2023) or in social relations. In South Kivu, coloniality is reflected both horizontally and vertically.

On a vertical level (state–individual relationship), coloniality is measured through the public policies adopted by the state. Such policies can justify the weak mobilisation of CSOs. To reduce this mobilisation, the state restricts civic space and freedoms through repressive legal texts.

In the DRC, repressive legal texts are tinged with coloniality. For example, offences against the state were imported from the colonial era and contain patterns of colonial thinking. The prohibition of subversive activities is a constituent element of several offences. It appears in Article 52 of our Constitution. According to this provision, 'All Congolese have the right to peace and security, both nationally

25 This concept was the work of Anibal Quijano. On this subject, 1. Quijano, A. 2000. Coloniality of power and eurocentrism in Latin America. *International Sociology* 15(2), pp. 215–32.

and internationally. No individual or group of individuals may use any part of the national territory as a base for subversive or terrorist activities against the Congolese State or any other State.' Subversion, according to the common meaning of the term, is defined as 'illegal action, often covert, aimed at undermining established values and institutions' (Rey-Debove and Rey, 2015). Such vague incriminations restrict civic space and contribute to limiting the actions of CSOs.

In 2023, the government adopted the Digital Code, which made it a criminal offence to spread false rumours on the internet. The people interviewed welcomed the initiative of this law. One civil society player 'welcomes the adoption of the Digital Code. This law has not been sufficiently publicised. As a result, many people don't know about it'. However, the process that led to the adoption of this law deserves to be criticised in terms of both form and content.

In terms of form, the power to adopt the Digital Code falls within the remit of the law under Article 122 of the Constitution.[26] The legislator has exclusive powers in this area, which is not a concurrent matter. The government cannot intervene in the area of the law without the authorisation of Parliament. With regard to the Digital Code, the President of the Republic relies on Article 129 of the Constitution.[27] This provision authorises the National Assembly to grant the government the power to legislate, during the parliamentary recess, in place of the National Assembly. On the basis of this authorisation, the government adopted the Digital Code. Ultimately, this code was adopted in the DRC without being examined by the people's representatives. It is a law that has no legitimacy. On a

26 Article 122 of the Constitution: 'Without prejudice to the other provisions of this Constitution, the law shall lay down rules concerning: (...) 6. the determination of offences and the penalties applicable thereto, criminal procedure, the organisation and functioning of the judiciary, the creation of new orders of courts, the status of magistrates, the legal regime of the Supreme Council of the Judiciary; (...).'

27 Art. 129 of the Constitution: 'The Government may, for the urgent execution of its programme of action, ask the National Assembly or the Senate for authorisation to take, by ordinance-laws, for a limited period and on specified matters, measures which normally fall within the domain of the law.'7

substantive level, the digital code excludes the security services from its scope. The latter carry out electronic surveillance without their actions being monitored.

During the colonial era, the administration controlled the indigenous population in order to protect colonial power by adopting repressive legislation. Today, public policy reflects the same pattern. The administration is restricting space by using the same methods as the coloniser. The DRC should follow the example of Kenya, where the judge in the Joshua Ayika case challenged this way of thinking.

The courts are prosecuting a civil society activist for publishing on X (formerly Twitter) the possibility of the army taking control of the government for 90 days. The post was made during a period of public protests against the high cost of living. As a result, he was prosecuted in Kenya's High Court. The person concerned, Joshua Ayika, posted on X (formerly Twitter) that the army could take control of the government for 90 days. Joshua made the post during protests against the high cost of living led by opposition parties. After acquitting him, the court annulled article 77 (1)(a) of the Penal Code, which provides for the offence of subversive activities. The judge's objective was to eradicate the colonial legacy in Kenya's legal system. According to the Court:

> 105. It is not far from our lips and eyes that independent Kenya inherited from the colonial state a repressive system . . . 135. It therefore goes without saying that, Section 77(1) and (3) of the penal code is a colonial legacy which limits freedom of expression through the vaguely worded offence of subversion (Malidzo Nyawa, 2024, § 105).

By striking down this subversion provision of the Kenyan Penal Code, the Court took an important step towards eliminating the colonial legacy from the Kenyan legal system. The ruling illustrates how judges in postcolonial contexts interpret the law in light of the country's history (Malidzo Nyawa, 2024). This case reveals the colonial patterns that characterise African legislation. Like Kenya, the DRC is no exception. Such public policies influence the behaviour of actors and their agency.

Horizontally, coloniality manifests itself in the relationship between CSOs and donors. Although they are considered partners, CSOs do not receive equal treatment from donors. According to one interviewee, 'Funding is decided in the North, as is the direction it takes. Their mobilisation in the electronic surveillance sector remains limited due to a lack of funding. Nor can they redirect the funds allocated to this sector, where the stakes are so high.'[28] For this reason, another interviewee argues in favour of 'decolonizing official development assistance and access to funding'.[29] The aim is neither to revisit the colonial period nor to oppose one vision to another, but rather to study the challenges of the contemporary world by widening the prism of analysis and agreeing to shift it. There are various approaches to decentring. It involves distancing oneself from the object of funding in order to consider it from other angles. It also means integrating into the analysis an awareness of the relationships of domination that may have defined a framework. And, of course, it means accepting that other realities, other than 'our own', deserve to be studied.

Conclusion

Towards public monitoring of electronic surveillance: a matter of time

This chapter examined the role of civil society in public scrutiny of state electronic surveillance. The results have been mixed, as the case studies have shown. This paper proposes two prerequisites for establishing public oversight of surveillance.

On the one hand, the success of public monitoring requires the establishment of an 'electronic surveillance' thematic group within civil society in the DRC. The nonexistence of such a group is a weakness linked to the organisational structure of civil society. However, such groups enable CSOs to develop networks with the

28 Source: Interview with H.K., 15 July 2024.

29 Source: Interview with H.K., 15 July 2024.

aim of emerging and strengthening each other (Bugeme, 2020). Following the example of the 'natural resources' thematic groups that exists in all civil societies and whose work made a major contribution to the reform of the mining code in 2018,[30] this thematic group should serve as a starting point for discussions on electronic surveillance in the DRC.

On the other hand, the future of public control of electronic surveillance depends on whether or not CSOs take ownership of certain security services. Since the start of decentralisation in 2006, public policies have included CSOs in certain security and public-protection services. In 2013, through decree no. 13/041 on 16 September 2013, the legislator created local councils for local security, with the possibility of CSOs to join as members. In 2023, the legislator set up the Data Protection Authority (DPA) in which CSOs sit as members.

Civil society should take ownership of a campaign for the establishment of such structures. Only then will public control of electronic surveillance emerge in the DRC.

References

Abega, S.C. 2009. *La société civile camerounaise et la malédiction de la Belle au bois dormant*. In: Mbonda, E-M. ed. *Annales du CERJUS P*, n°001, *La refondation de l'État en Afrique. Justice, efficacité et convivialité*. Yaoundé: Terroirs.

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

Albarello, L. 2001. *Choisir une étude de cas comme méthodes de recherche*. Brussels: De Boeck.

Amuli, K., Mushi, M. and Yamba Yamba, S.N. 2003. *La société civile congolaise: État de lieux et perspectives*. Brussels: Colophon.

Arendt, H. 1978. *The Life of the Mind, vol. 2*. New York: Harcourt Brace.

Beckman, L. 2006. Enfranchising Citizenship and Voting Rights: Should Resident Aliens Vote? *Citizenship Studies* 10, 152.

30 Source: Interview with NB, 12 July 2024.

Bugeme, Z.Z. 2019–20. *Subjectivité des acteurs et conflictualité au sein des OSC en RDC: entre influence des normes et agencéité.* PhD thesis, Catholic University of Central Africa, unpublished.

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).

Camila P., 2020. Rendre visibles les conséquences de la surveillance numérique Le cas du scandale Cambridge Analytica, Open Edition Journals vol. 37/2 | 2020 (https://journals.openedition.org/communication/13252).

Cappelle, J. and Custers, R. 2009. *Rechercher la problématique des ressources naturelles dans la République Démocratique du Congo.* Antwerp: IPIS vzw.

Castagnino, F. 2018. Critique des surveillance studies. Éléments pour une sociologie de la surveillance *Déviance et Société.* 42(1), pp. 9–40. [Online]. Available from: https://doi.org/10.3917/ds.421.0009.

CERDHO. 2022. *Bonne gouvernance des Ressources naturelles, Droits de la personne et Développement communautaire en République démocratique du Congo: Analyse diagnostique de base contextuelle et organisationnelle.* Report, July 2022.

CORNUT ST-PIERRE, 2019. « Utilisations et finalités des registres du commerce à l'ère numérique : de l'efficacité économique à la surveillance citoyenne des entreprises. » Les Cahiers de Droit, vol. 60, n° 3 : 589-622.

Davidson, D. 1980. *Essays on Action and Events.* Oxford: Oxford University Press.

De Sardan, O. 1995. Anthropologie et développement : Essai en socio-anthropologie du changement social, Paris, APAD-Karthala, coll Hommes et sociétés

De Sardan, O. 2008. *La rigueur du qualitatif – les contraintes empiriques de l'interprétation socioanthropologique.* Louvain-la-Neuve: Academia Brylant.

Donnadieu, G. and Karsky, M. 2002. *La systémique, penser et agir dans la complexité.* Paris: Éditions Liaisons.

DRC. 2019. *Plan national du numérique – horizon 2025.* Kinshasa: Democratic Republic of Congo. Accessed September 2019. 120. https://presidence.cd/uploads/files/Presentation%20PNN_03_final.pdf

Fanon, F. 1961. *Les damnés de la terre.* Éditions Maspero

Goodman, R., ed. 1995. *Pragmatism.* London: Routledge.

Hobbes, T. 2000. *Le léviathan.* Paris: Gallimard.

Hoebeke, H., Van Der Lijn, J., Glawion, T. and De Zwaan, N. 2019. *Garantir la stabilité légitime en RDC: hypothèses extérieures et perspectives locales*. Étude de politique, Stockholm International Peace Research Institute (SIPRI) and Cordaid.

Human Rights Watch. 2020. RD Congo: Restriction croissante des droits – La répression touche les médias, les détracteurs et les manifestants. *Human Rights Watch*. [Online]. Available from: https://www.hrw.org/fr/news/2020/07/22/rd-congo-restriction-croissante-des-droits.

La Fontaine, Jean de. 1678–9. *Les animaux malades de la peste, Fables*.

Le Petitcorps, C., Desille À., 2020. « La colonialité du pouvoir aujourd'hui: approches par l'étude des migrations », Migrations Société, vol. 2020/4, n°182.

Lyotard, J.F. 1991. *Phenomenology*. New York: SUNY Press.

Maheshe, T. and Mushagalusa, J.P. 2021. *Digital Surveillance and Privacy in DRC: Balancing National Security and Personal Data Protection*. Media Policy and Democracy Project.

Nyawa, M.J. 2024. Colonialisme, droit pénal et poubelle de l'histoire: On Kenya's Subversion Judgment. *VerfBlog*. [Online]. Available from: https://verfassungsblog.de/colonialism-criminal-law-and-the-dustbin-of-history/. DOI: 10.59704/916e460f0c11655b.

Plato. 1834. *La République, Livre X*, traduit par Victor Cousin. *Œuvres de Platon*. Paris: Rey et Gravier.

Quijano, A. 2000. 'Coloniality of Power and Eurocentrism in Latin America'. *International Sociology*. 15(2), 215–32.

Rebughini, P., and Colombo, E., eds. 2023. *Framing Social Theory Reassembling the Lexicon of Contemporary Social Sciences*. New York: Routledge.

Rey-Debove, J., et Rey, A. (dir.), 2015. Le Petit Robert 2014, nouvelle édition du Petit Robert, texte remanié et amplifié, Paris, Dictionnaire Le Robert, Sejer.

Salvas, B. 2001. *La protection de la vie privée sur le Web avec P3P: l'arrimage incertain du technique et du juridique*. Master's thesis in law (L.L.M.), Université de Montréal.

SetThings. [Online]. Available from: https://www.setthings.com/fr/contre-espionnage-communautes-epistemiques-en-ue/.

Sfetcu, N. 2020. Contre-espionnage – Communautés épistémiques en UE. *SetThings*. [Online]. Available from: https://www.setthings.com/fr/contre-espionnage-communautes-epistemiques-en-ue/.

Spijkerboer, T. 2023. Coloniality and Case Law on the Australian Asylum

Offshoring Scheme. *International Journal of Migration and Border Studies.* 7(2).
Tribunal de grande instance de Kinshasa/Gombe. 2024. *Judgment no. RP 29. 823, 18 March 2024, Public Prosecutor and Civil Party Théo Ngwabije Kasi against the defendant Stanislas Bujakera Tshiamala.* Unpublished.
Tribunal de paix. 2020. *Judgement No RP 3386/III, 30 September 2020, Public Prosecutor and Civil Party Théo Ngwabije Kasi against the defendant Heri Kalemaza Nicodeme.* Unpublished.
Viana, A. 2021. La surveillance numérique en temps de pandémie. *Revue internationale dedroit des donnéeset du numérique.* 7, pp. 165-78.
Vuilleumier, C. n.d. *Espionnage, police et secrets d'État.* La Cité.
Wright Mills, C. 1966. *Sociology and Pragmatism.* New York: Oxford University Press.

Interview

1. Interview with NB, 12 July 2024.