Electronic surveillance in Mozambique: The risks and suspicions in a context of authoritarianism and military conflict

Ernesto Nhanale

May 2021

Electronic surveillance in Mozambique: The risks and suspicions in a context of authoritarianism and military conflict

Ernesto Nhanale

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

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

May 2021

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

Table of Contents

Summary

The political context, marked by an authoritarian culture of control and restrictions of freedoms as well as recurrent military conflicts, has constituted a fertile environment to substantiate suspicions about electronic surveillance in Mozambique. This report, based on desk research and interviews with several politicians and human rights activists in Mozambique, shows some of the mechanisms under which the State is suspected to perform the electronic surveillance that was established during the post-independence period, where, with the adoption of the party-state model, various surveillance mechanisms were institutionalised in order to control the various risks of contestation and subversion against the "regime", as well as emerging political and military conflicts. The report shows how surveillance emerges from the political culture of the formally authoritarian state (1977-1990) and continues as a practice in the context of multiparty democracy (since the 1990s), using, in the last 20 years, the development and expansion of electronic communication networks – mobile phones and the internet – as mechanisms of social and political control, in contexts where the state continues to face military conflicts. In addition to serving the useful purpose of ensuring security, the culture of repression of civil liberties, the qualification of differentiated opinion as political enmity of the Mozambican Liberation Front (Frelimo) party government, as well as the weaknesses of the laws protecting citizens' data, mean that most of the technological measures and systems introduced are viewed with the suspicion of serving the interests of espionage by the government. The cases of installation of public security cameras, the compulsory registration of SIM cards and a series of other measures introduced by the government, rather than serving the useful purpose of guaranteeing security, fighting crime and insurgency, instead substantiate citizens' perceptions that the state is using them to spy on citizens, thereby violating their fundamental rights such as privacy and freedom of expression.

Introduction

Even with the unimaginable gains that the internet and the digitalisation of the various spheres of life have brought, we live in a world in which the idea that *we are being watched* has become widespread. From the most rudimentary forms, to the current mechanisms of citizens' identity recognition, via digital or even facial recognition, security controls from security cameras, as well as the various forms of digital databases, lead to this belief and stimulate the perception that people are losing their spheres of freedom and are being exposed to more and more control.

Despite the fact that technologies have been developing in an accelerated and exponential way, especially in the early 21st century, the debates and practices of surveillance have developed since antiquity, having been raised with greater vigour in the context of the rationalisation of the modern state. Examples of this are Jeremy Bentham's *The panopticon* (1977) and Michel Foucault's celebrated work, *Discipline and punish* (2014), which discuss systems of control through the constant surveillance of individuals.

Even with the urgency of the state in performing its legitimate power of control for the purposes of security or even recognition of its citizens, the use of the potentialities of the new communication technologies has been the subject of polemics and discussions, in many countries, about the limits

of this power or even its abusive use, invasion of privacy and massive spying (see Morozov, 2013). Even with the idea that the internet has translated into an opportunity for the democratisation of power, Morozov (2010) offers some of the most passionate questions about how authoritarian governments are using the internet to suppress freedom of expression and spread propaganda.

Not wanting to resist the idea that there is massive surveillance performed in current societies by states, this report seeks to question the practices of electronic surveillance in Mozambique. The research starts from the hypothesis that the political context, founded on a culture of control and limitations on freedoms, and marked by recurrent military conflicts, as well as the weaknesses of the legal framework that protects citizens from surveillance practices may be determining factors to explain the risks, as well as the constant suspicion that there is excessive control over citizens' communications, especially their mobile communications.

Even with the limitations of being an exploratory study, the case studies presented here, as well as the general analyses, offer important elements for understanding the context, the meaning and the grounds for suspicions about electronic surveillance in Mozambique, especially in a context in which such practices cannot be seen as provable due to the high level of secrecy under which such practices are carried out.

This report is divided into three key parts:

1). **The roots of surveillance**: A discussion of the effects of the authoritarian state and military conflicts. It is shown how surveillance was applied to serve as a response mechanism in the face of a context of high risks of political contestation of the new party-state regime, as well as against the imminent military conflicts resulting from that contestation;

2). **The legal framework**: A consideration of advances in the protection of personal data. The fact is discussed that, in an antinomic logic, at the same time as a series of advances are sought, especially with the signing of the international pacts on data protection, so too standards that encourage surveillance practices prevail or are introduced;

3). **Three case studies are provided**: More than categorical statements on the existence of digital surveillance in Mozambique, the cases studies elaborate and question the fact that, even though they constitute important measures to ensure State security and fight crime; the context in which they are introduced and the authoritarian practices of the state in its relationship with citizens, make these measures the object of suspicion of espionage.

The following three cases are discussed: a) the registration of SIM cards, initially taken in the context of popular demonstrations and strikes against the low quality of governance; b) the use of centralised surveillance systems, via mobile phones and security cameras, which although installed to serve in the fight against crime, have brought few results in the eyes of citizens; c) finally, the measures taken in the context of the Covid-19 pandemic, which reinforce the idea of state authoritarianism, as well as the use of the context to violate the rights to privacy.

The roots of surveillance: The effects of the authoritarian state and military conflicts

Mozambique has had a democratic rule of law since 1990. However, the country previously went through a period of one-party rule, founded in 1977,[1] two years after the Proclamation of National Independence (Rosário, 2014).

The political and social context of transition from the post-colonial period (1975) and of independence was marked by distrust on the part of Frelimo based on the risks of contestation by the pro-democratic movements at local as well as regional level, which led to an intense control and surveillance of citizens. The definition of a policy of punishment and repression against the regime's detractors was one of the responses of the new Frelimo regime to the risks of various threats from internal enemies. Certainly, to put into practice the policy of repression, through the various forms of punishment of the "enemies"[2] of the revolutionary cause of post-independence Frelimo, it was important to permanently monitor the possibilities and actions considered subversive.

The reactions to the ignorance of the legitimacy of Frelimo, after having adopted a Marxist-Leninist orientation, culminated in internal violence in the capital and suburbs, and on the other hand, in conflict with the Mozambican National Resistance (Renamo), which was supported by the Rhodesian and apartheid regimes in South Africa, This led to the banning of civic movements, the repression of all forms of freedom of expression, and the intensification of mass surveillance activities to identify enemies (Machava, 2011).

Even in the absence of information and communications technologies (ICTs), the recovery of colonial structures in villages, the so-called "communal villages" (Medeiros, 1989; Ginisty & Vivet, 2012), and in the cities, in quarters and neighbourhoods, as well as the use of route plans to control the movements of citizens, through leadership structures loyal to the political power, known as "facilitator groups", constituted an important instrument of surveillance, parallel to all mechanisms of punishment, whether in the form of reprimands or even serious sentences, including the death penalty (Ginisty & Vivet, 2012). This whole organised system facilitated surveillance actions to identify any form of subversion against the principles of the regime (Temudo, 2005).

Another fundamental contextual aspect is related to the militarisation and subsequent wars in Mozambique, which *per se* demanded a high level of control. Since the war of liberation, Mozambique has experienced and continues to experience periods of military conflict, starting from Ian Smith's invasion from Rhodesia, attacks by the apartheid regime, to the long armed conflict that lasted 16 years, later resurfacing between 2013 and 2016 with the origins of electoral discord. This continues currently (2020), from the attacks in the centre of the country by the so-called "military junta" and, more seriously, since 2017, in Cabo Delgado, the fighting against insurgents, designated as armed groups linked to the Islamic State (Ngoenha, 2020).

Thus, even with the democratic transition of 1990, marked by the first elections in 1994, the culture of restrictions on freedoms, as a political method established soon after independence to reduce spaces for criticism, means that those, even if not in political opposition, who make critical comments about the quality of governance are subject to surveillance, and are therefore on the

1 Strictly speaking, it cannot be said that Mozambique has been a one-party state since 1975, but since 1977, when the III Congress of the Frelimo Party officially adopted the Marxist-Leninist and "vanguard" ideological orientation, taking the country to a one-party regime (Rosário, 2014).

2 "Mass detentions and arrests, displacement and imprisonment in camps of re-education and of production in remote areas of the country, corporal punishment and public executions by firing squad were some of the main mechanisms of state violence and punishment against the 'enemies' of the 'popular state' and of the 'revolution'" (Machava, 2011: 595).

map of those who should be watched, using all mechanisms.

With the same party in power – Frelimo – the surveillance practices have been continued. Such surveillance not only of politicians, but also of those who through their critical opinions are catalogued as being opponents of the regime, is being assisted by the ICTs, by tapping phones.

The legal framework: The advances and gaps in personal data protection

The development of the regulatory framework constitutes a crucial element for data protection as well as the defence of citizens' privacy rights. This section seeks to understand how the Mozambican legal framework is laid out, exploring its limits and gaps that may constitute an opportunity for the prevalence of electronic surveillance practices. The fundamental rights framework in Mozambique has been defined since 1990, with the introduction of the new democratic constitution. In the revision made in 2004, Mozambique kept in its constitution a chapter establishing the general framework on "rights, duties and fundamental freedoms" under which is defined, specifically, in Article 41, the protection of personal rights: *"every citizen has the right to honour, to a good name, to reputation, to the defence of his or her public image, and to the reservation of his or her private life"* (Constitution of the Republic of Mozambique, 1990).

Article 41 of the Constitution of Mozambique (1990) thus establishes the right to privacy in a more comprehensive way, and specifically, protection against surveillance of private life using digital or electronic means, even placing this limit to the use of electronic means for the monitoring of citizens in the course of their political or religious activities or in violation of their private life. Article 71 of the Constitution sets out these prohibitions in paragraphs 1,2,3 and 4, as well as expressing the need to protect citizens' data, outside of the exceptions that the law establishes, even if these are problematic.

As a way to respond to the challenges imposed by the development of the technology sector, Mozambique has been approving a set of legal instruments and legislative reforms that, in a direct or indirect way, addresses electronic surveillance issues.

In 2017, the law on electronic transactions was approved (Law no. 3/2017), which regulates e-commerce and e-government issues, as well as the security of ICT providers and users, under which very important discussions on data protection are placed. In the same year, the Criminal Investigation Police was replaced in 2017 by the National Criminal Investigation Service (SERNIC), through Law no. 2/2017[3] which introduces, at the same time, several relevant elements of access to personal data for criminal investigation purposes, specifically in its Article 18.

Still within the scope of this process, in 2019, through Resolution no. 5/2019, Mozambique ratified the African Union Convention on Cybersecurity and the Protection of Personal Data. In addition significant reforms were made in the framework of the criminal code, approved by Law no. 24/2019, with the purpose of covering matters linked to issues on cybercrime, as well as extending the criminal framework criminal practices that may result from the use in new technologies, data forgery, misuse of information devices, as well as very relevant issues on wiretapping.

3 Law number 2/2017, of 9 January created the National Criminal Investigation Service, abbreviated as SERNIC).

A reform process in the telecommunications sector was even carried out in 2016, having, for example, amended Law no. 8/2004 on telecommunications, by-law no. 4/2016. Through this law, in its Article 66, all telecommunications operators are obliged to have an operational and efficient system of interception of communications, for the purpose of criminal investigation, noting that such interceptions must be made, upon the issue of a criminal investigation section judge's authorisation. Two years before the approval of this law, the Government had approved the regulation No. 75/2014 of telecommunications traffic control.

In 2019, the Council of Minister introduced decree no. 44/2019 on "Telecommunications Service Consumer Protection", in which it indicates in Article 10, the consumer's right to privacy and protection against the use against unauthorised use of their personal information, from their communications, personal data and addresses. The same spirit was followed in Article 7, of decree no. 66/2019 of "regulation of the security of telecommunications networks", in which it highlights the issues of data protection and privacy of consumers, as well as the need to obtain data consent for the sharing of their data with other entities.

In the same spirit, Law no. 03/2017, in its Article 14, limits intermediate data transmission service providers to maintain the secrecy and confidentiality of all communications nor disclose them to the detriment of their users, except in situations where there is a judicial or administrative decision, to provide the information.

However, it can be pointed out that these measures are introduced, in material form and in many times, the limits, permissions and excesses of legislation or even state surveillance practices on citizens are made within the principle and interest of States to protect the state assets or even combat criminal practices (Gusmão, 2019). But, materially, on many occasions, it is under the name of "state assets", "defence of security" and/or "fight against crime" or even in excess of the operationalisation of the role of the State that its agents carry out digital surveillance, exceeding the normal measures of control, defining undue targets.

The specific analysis on the limits urges, in some countries, "eavesdropping" measures provided by law may be used for criminal purposes, but for political purposes, in order to define political enemies. Therefore, resulting in an analysis of the gaps and critical spaces under which laws can be used to favour electronic surveillance is relevant. Or in another way, to verify the type of collisions and limits of these laws with the principles of the rights to privacy and intimacy of citizens.

For the case of Mozambique, one of the first risks that arises, right from the start, is founded on the fact of application of the wiretapping law openings for adverse purposes. Law no. 25/2019 approving the new Criminal Procedure Code, in its Article 222 opens space for the carrying out of interceptions and recordings of telephone communications or other electronic means of suspects, as means of evidence. In fact, this is a provision that substantiates the relevant role that is attributed to the use of electronic communications for the criminal investigation process assigned to the National Service of Criminal Investigation (SERNIC), through law no. 02/2017. As the same law states in paragraph a) of Article 21, the interception and recording of communications must be made in the scope of criminal investigation of suspects and must be authorised by a competent judicial body.

As most of the interviewees for this study state, the problematic aspect in these types of measures is the fact that, in Mozambique, wiretaps are carried out outside the scope of SERNIC (the Criminal Investigation Police), either by the State Intelligence and Security Service (SISE), and are based merely on distrust and speculative measures and, in many situations, without any authorisation from a judicial authority.

Moreover, there are disparities and conflicts about the situations in which information should

be made available. For example, even though Law no. 03/2017 on electronic transactions obliges the secrecy of the intermediary providers[4] of data transmission services, it opens space for such information to be offered outside of a judicial warrant, not only for criminal purposes, as referred to in Article 14(4):

> *The intermediary provider may, upon judicial decision or administrative decision, duly founded, provide communications or information that have criminal content or that threaten the security of the State.*

It should be noted that here, as indicated, there is an opening for the concession of information to non-judicial authorities, giving room for information of a personal nature to be provided based on administrative orders under the argument of state security,[5] in a context where the knowledge of state security is itself diffuse. The knowledge on "state security" in Mozambique has been much contested, especially because Law 19/91 that defines it is diffuse, establishing, in its Article 22, that defamation of the PR, ministers, Supreme Court judges and even general secretaries of political parties is considered a crime against state security, punishable by one to two years of imprisonment. This means that, in the name of "state security", normal communications from citizens can be requested, as long as they refer to criticism of the figures that protect them.

Also, as previously mentioned, is up to the Communications Regulatory Authority (ARECOM), within the framework of its scope, to apply administrative measures to oblige the operators under its jurisdiction to provide information, as per paragraph d) of Article 15 of the Law that created it (no. 4/2021):

> *… to issue administrative instructions to operators, service providers and other users of radio frequency and telecommunications numbering resources, provided that they do not interfere with private management and the rights and freedoms defined by law, except where there is justifiable fear of crime or danger to state security*

It should be clearly noted that this attribution, while ostensibly prohibiting it, in fact freely allows interference in the privacy and surveillance of persons and institutes. It is not necessary that there are indications justifying it, as long as ARECOM understands that there are "fears", even without a mandate from the judge/court, it can apply an administrative measure for the access to private data.

In conclusion, the indicated gaps show that the judicial authorisation in the Act 2016 is a mere decoration, and that private data can be accessed by SISE using various mechanisms whenever the argument is that of state security.

Case Study 1: The registration of SIM cards: A case of control of freedoms?

The registration of SIM cards (subscriber identity module) for mobile phones in Mozambique was introduced and carried out under the suspicion of public opinion that, rather than serving national security and counter-crisis interests, there were motivations for political control, collective surveillance and undue individual eavesdropping.

After the introduction of the mobile phone system in 1997, it was only in 2015, when it supported 13 585 907 users, distributed over three operators (Moçambique Cellular, Vodacom and Movitel), that the compulsory registration of SIM cards was introduced, having as one of the fundamental arguments by the government the

4 Under Law 02/2017, the intermediary service provider is defined as "any person who, on behalf of another person, sends, receives or stores data messages. They are those who provide access service to the network or provide services from it (access providers, content providers, application providers and hosting providers).

5 Law number 19/91, 18 August 1991 (Law of Crimes against State Security). Maputo: National Press.

need to fight crime, fraud and to protect the citizens themselves (INCM, 2017).

The political context under which the decision was taken, after so many years in which the system had operated without registration, left one with suspicions that it was to allow greater political control and limit actions by civic movements contesting governance.[6]

These suspicions are based on the fact that the first order of registration was taken soon after violent protests in Maputo against the rise in the cost of living and corruption and replicated in other cities of the country, in February 2008 and September 2010, followed by further demonstrations in Maputo in November 2012 (De Brito et al., 2017).

The first large demonstration on 5 February 2008 was preceded by a wide circulation of messages by SMS and on the internet social networks, especially Facebook, calling for the strike, which, after having taken place and for the impact it had, remained without any "face" from the point of view of its promoters. As recorded in several reports, the demonstrations did not have an identified or organised leadership, precisely because electronic means were used for their convocation and dissemination (Tsanzana, 2018). When the government announced an increase in the prices of bread, domestic gas and electricity, on 1 and 2 September 2010, the country faced a new wave of popular demonstrations which were once again based on SMS (*Observer*, 2016).

On 15 and 16 November 2016, the capital city once again had a half-day stoppage, much on account of supposed demonstrations, after transport fares had been increased. Once again, this information of the demonstrations would have been circulated by SMS. One of the mechanisms the government used to reduce the impact of this was the blocking of communication services, especially SMS, as a way to make it difficult to spread information about the demonstrations (De Brito et al., 2017).

Besides having restricted text messages, via mobile operators, on the days of the strike of 1 September 2010, the government instituted, through ministerial decree 153/2010[7], the mandatory registration of the carriers of each of the numbers, and that unregistered numbers should be blocked. According to the government, the introduction of this measure aimed to "promote the responsible use of the SIM card, contributing to the maintenance of public order and peace".

This measure, even if it was not with the intention of maintaining public safety, was widely criticised, mainly because it was viewed as a means of repressing the freedoms of expression and demonstration, and freedom from interception of citizens' communications (Observatório de Direito no. 1, CIP, 2010). In its publication, the CIP (2010) shows that the introduction of this measure was unconstitutional in nature, since it is up to the Assembly of the Republic to introduce measures that restrict freedoms and fundamental rights, in addition to understanding that there can be no obligation to register a SIM, since the use of this means it is not mandatory. After this announcement the Council of Ministers introduced decree 18/2015, which regulates the registration and activation of SIM cards.

With the authoritarian tradition of the government and the context of popular movements to contest the governance measures, the acts of blocking mobile communications were seen as anti-democratic surveillance measures, generally, applied by authoritarian countries, as response measures and for popular control (DW, 2013).

6 The interest in massification of mobile phones use, before the service was introduced in 1997, may have contributed to the free registration policy by the Government. But the public manifestations, organized from mobile phones, aroused the need for greater control by users.

7 Diploma Ministerial no 153/2010, Boletim da República, I Série, no 37, 15/09/2010

Case Study 2: Telecommunications systems and electronic surveillance in Mozambique

According to the latest official data published by the Communications Regulatory Entity (ARECOM), in 2019 in Mozambique, three mobile phone companies – Moçambique Cellular (Mcel), Vodacom and Movitel – operated, with a total of 14 074 248 subscriptions (INCM, 2019). According to data from INE (2017), about 26,4% of the population owned a mobile phone, and only 6,6 % had access to the internet. It is estimated that by 2021, the growth rate of internet users could have increased to around 20%, from around 33 internet access operators (ISPs), including mobile phones.

In 2018, Mcel merged with Empresa Publica de Telecomunicações (the sole operator of the landline telephone system and owner of the fibre optic network), forming a giant publicly owned company called TMcel (Mozambique Telecom), a decision taken by the government in 2016. With the power of TMcel controlling the fibre optic system, a key data transport infrastructure, the state is in the privileged condition of direct control of the sector. As well as relying on the fact that Movitel, the third mobile operator entering the market in 2011, is a joint venture between Viettel and SPI (Management and Investment), a holding company of the Frelimo party,[8] it has a key role in expanding the mobile signal to rural areas from the fibre optic system (Gilward et al, 2019).

While the market and the use of ICTs are growing, several reports show that the government is intensifying its monitoring of electronic communications, both in terms of wiretaps and surveillance through public security cameras.

In 2016, the *A Verdade* newspaper reported the fact that the government, through a system designed by ZTE Corporation (a Chinese telecommunications company), the authorities were intercepting and monitoring citizens' communications through constant reading of messages (SMS, emails, Whatsapp and Viber), phone tapping and monitoring of social networks, as well as websites (Tsandana, 2016). According to the report quoted by *Jornal A Verdade*:

> *The information captured by the system in real time, listed in the project we are discussing, goes from the simplest telephone call or text message (SMS) of all the millions of users of mobile telephone networks, to the messages of all types of electronic mail (whether POP3, SMTP or IMAP4), and even the emails exchanged by various online providers (Gmail, Yahoo, live). The system also captures the data exchanged over chat applications, from the most popular to the least known, accesses voice communications over internet protocol (VOIP), accesses data exchanged on FTP or TELNET, and permits the tracking of communications exchanged via social networks (Facebook, Twitter, Google Plus and YouTube).*

One of the major problems that arises over the use of these systems in Mozambique is the fact that there is total secrecy about who manages the installed systems (the military, the criminal investigation services, or the intelligence and state security services). This secrecy, in addition to raising concerns about the use of the system for espionage, does not give space to understand the scope and objectives of the interventions.

The use of high-definition digital cameras associated with high-speed internet, by public and private entities, for the surveillance of public space has been a phenomenon occurring in several cities worldwide. Most of these CCTV cameras have smart capabilities to recognise small details, even such as car number plates or facial recognition. The amount of individual data collected from these

8 https://www.rtp.pt/noticias/economia/movitel-ganha-concurso-para-terceira-operadora-movel_n389962.

surveillance systems has opened several debates on the issues of the privacy of data that ends up being held by these entities (Kwet, 2020).

In Mozambique, there has been an exponential growth in the installation of high-definition surveillance camera systems in homes, private and public institutions and even on public roads, in an environment where there is no specific regulation of such devices.

Since 2014, a process of installing 450 high definition and real-time data transmission cameras for public surveillance purposes was initiated on the main public roads of the cities of Maputo and Matola, with an extension to part of national road number 1 (Caldeira, 2018). This equipment includes HD IR Network Box cameras, HD IR Network high-speed PTZ dome cameras, with capacity to capture voice and images in high definition, with wireless transmission in real time. These cameras are associated, within the same project, to data interception equipment, in real time, through VOIP or TELENET, as well as the decryption of data in equipment considered secure.

Although there was no official information from the authorities regarding this monitoring of public movements, it was argued that, besides crime control, the project was designed to support traffic control and traffic accident investigation (Gonçalves, 2020). However, in a context where the capital city has been the scene of violent crimes, including kidnappings of citizens, there is little evidence that the police have used the equipment in solving such crime.

These cameras are part of a project valued at around US$140 million funded by China and awarded to a consortium made up of a local company, Msumbiji Investments Ltd and China's Zhong Xing Telecommunications Equipment Company Ltd (ZTE), in a public contract signed by the Military House, an institution dedicated to the security of the Head of State.

One of the arguments that has been put forward to suspect the use of this equipment for electronic surveillance of citizens has to do with the fact that, even with its operationalisation, from 2017 to 2020, there have been violent crimes that include kidnappings and murders of citizens in places near where these cameras were installed, however, the authorities have not been able to clarify or identify their authors. Secondly, this project is being developed in a context of a legal vacuum regulating digital data privacy issues. And thirdly, the fact that the contracting entity, the Casa Militar (Military House), is an institution of personal security of the Head of State and his family, not an institution linked to public or state security – such as the Police of the Republic, through the Criminal Investigation Services, the Attorney General's Office or even the Information and State Security Services (Gonçalves, 2020). These all gaps serve as support for the suspicions that the cameras are in the surveillance service, more than the purposes of guaranteeing public security.

On the other hand, there is a mistrust of the risks of global espionage in businesses set up with the support or use of Chinese funds and technologies. As in several countries in the SADC region, and in Africa in general, a large part of investments in security systems, especially in public surveillance cameras, have been made with Chinese investments (Swart, 2020).

It should be noted that, apart from the contract for the television digitalisation sector which was awarded to Startimes International by the Mozambique government, it is mainly Chinese companies in the telecommunications sector that have been growing, with ZTE and Huawei playing a fundamental role. Huawei, for example, has gained a strong predominance, especially in offering technological solutions, whether in terms of equipment and software, especially in 4G and 5G services. In 2019, Tmcel invested about $23 million in a partnership with Huawei for the provision of technologies for the mobile telephony sector.[9] These

9 https://www.noticiasaominuto.com/economia/1241626/tmcel-vai-investir-20-milhoes-em-equipamento-de-telecomunicacoes

business partnerships came to be substantiated and sponsored by the government, through a macro agreement signed with Chinese company for a more strategic performance in the areas of infrastructure, training and technologies.[10]

One of the major arguments for the role and use of Chinese ICTs for public surveillance systems in Mozambique has to do with the fact that China is offering credit facilities for the development of various types of infrastructure in the area of telecommunications; as well as lower prices compared to European and American providers (Swart, 2020).

Case Study 3: Authorised surveillance due to Covid-19? A question for debate

The measures to prevent the Covid-19 pandemic that forced several states around the world to declare a "state of public calamity" or "state of emergency" placed tension between security measures and the rights to liberty, individual protection and the right to privacy (Silveira, 2020). In the need to ensure compliance with mandatory quarantine rules, many states, including Mozambique, have introduced from the Presidential Decrees of State of Emergency the use of electronic monitoring from mobile phones as a way to control the movement of people based on data provided by national telecommunications operators (Tsandzana, 2021).

In the case of Mozambique, the introduction of these measures, by Presidential Decree number 11/2020, raised several debates that they clash with the constitutional rights of data protection. The questioning of these measures arose specifically because they are considered contrary to the principles of safeguarding personal data that the Constitution of Mozambique itself establishes in its Article 71.

Even though the Constitution itself establishes restricted situations under which the State may have access to personal data, in cases of judicial orders, the same Constitution establishes, in Article 56(2), that limitations on freedoms may safeguard other rights or interests protected by the Constitution. And, on the other hand, in its paragraph 3, the Constitution clarifies that any law can only exercise these limitations to the freedoms of guarantees in cases expressly provided for in the Constitution.

Now, the point for debate and the critical nature of the measure in Mozambique is based on the fact that the Constitution itself defines, in Article 72, the declaration of the State of Emergency at at a time when individual rights and freedoms may be temporarily suspended. As Chamuço (2020) discusses, even if this is established by the Constitution, there is a legitimate question that has been raised for the use of these mechanisms in the name of safeguarding public health.

In this sense, the problematisation of the measures adopted under the State of Emergency in Mozambique does not lie in the issues of access to data, but in the introduction of geolocation measures, as established in paragraph e) of Article 3 of Decree 12/2020, which regulates Presidential Decree number 11/2020, establishing the "requirement of real-time knowledge of people through the use of geolocation".

It was as a result of the Presidential Decree no. 11/2020 National Institute of Communications in Mozambique (INCM) issued the resolution no. 02/CA/INCM/2020 of April 16, under which to establish measures in the telecommunications sector. In paragraph c) of Article 2 of the resolution, INCM establishes as the competence of telecommunications operators, "ensure the tracking of people in quarantine and in isolation, when requested by health units".

These measures open a space for the use of electronic applications or systems to control the movements of citizens forced into isolation, for various reasons related to the risk of contamination

10 https://www.ecofinagency.com/telecom/1311-42053-mozambique-partners-with-huawei-to-boost-ict-industry, accessed 15 January 2021.

of Covid 19, by being able to give information about the possibilities of infected people as well as facilitate the tracking of contacts (Tsandzana, 2021).

Both from the point of view of advantages and relevance to public security, these measures have been seen as problematic, especially because these platforms do not allow the protection and confidentiality of data (Chamuço, 2020). Furthermore, these measures appear to be purely administrative and not judicial in nature, nor within the scope of criminal investigation.

As Silveira (2020) argues, this administrative measure of electronic monitoring of data, without consent and lacking a judicial decision, means that much that is done in the systems used in the context of Covid-19, even if it is provided with some arguments that are based on the constitution, "completely removes the right to privacy and its essential core".

In this sense, the process of electronic monitoring cannot suffice as a simple administrative measure of prevention of Covid-19, but must rather be linked only to processes of criminal investigation and with judicial warrants produced for this purpose. The tracking of citizens to be done outside these mechanisms, as defined by the regulation of the state of emergency in Mozambique, opens potential space for the exercise of massive surveillance on behalf of Covid-19.

Conclusions

The contextual elements surrounding surveillance in Mozambique are marked by an authoritarian political culture based on a strong interest in establishing political control, and placing limitations on freedom of expression in order to reduce the levels of contestation and repress political enemies. On the other hand, we see the political, economic and technological links between Mozambique and countries that have been catalogued on surveillance maps worldwide, such as China.

The context of the militarisation of the State and the almost permanent environment of military conflicts of various kinds; as well as the fragility of the institutions and the laws in establishing limits on the protection of personal data are relevant to understanding the enormous scale and scope of public surveillance, and why it raises suspicions and the general public perception that there is massive surveillance of communications, both interpersonal and electronic.

In the cases that have been presented, besides the general context linked to control, one can notice the existence of elements that may substantiate these suspicions, indications of a propitious environment for mass surveillance. The investments made by the state for the installation of security cameras, in a context where crime is rising brutally in the form of kidnappings and murders, sometimes in places where these cameras are located, but which the police entities are unable to clarify, are fundamental to the perceptions and the risks of associating these installed technological apparatuses with the purpose of watching, controlling and violating the rights to privacy.

The cases of registration of SIM cards and the environment of distrust created in the context of Covid-19 show how certain measures, even if relevant for urgent objectives of protection and defence of the public interest, when taken in authoritarian contexts of excessive control, can be viewed with suspicion, as substantiating the perception that the government is watching the citizens.

This report has been a relevant tool for the debate on surveillance practices, especially by describing context and bringing forward several cases that, even in the form of "suspicions", illustrate the risks of surveillance for democracy.

The escalation of the violence that Mozambique is suffering in Cabo Delgado has been a reason for strengthening mechanisms of control and surveillance to ensure greater security. The actions of terrorist groups increased in frequency and severity, which reveals the inefficiency of the surveillance systems used by government. On the other hand, the surveillance measures have a negative impact, insofar as they have contributed to the illegal arrests of innocent citizens. For example, the illegal detention of two journalists in Cabo Delgado, under the pretext of liaison with extremist movements, appears to have been based on incorrect suspicions aroused by electronic espionage of their communications.

References

Bentham, J. (1977). *Le panoptique.* Paris: Belfond.

Caldeira, A. (2018). Camaras de vídeo vigilância em Maputo e Matola são para distrair do comando de interceção de informação de Moçambique. *Verdade*, 4 April 2018. Available at: http://www.verdade.co.mz/tema-de-fundo/35-themadefundo/65381-camaras-de-video-vigilancia- em-maputo-e-matola-sao-para-distrair-do-comando-de-intercepcao-d

Chamuço, T. (2020). Direito digital: o direito 'preferencial' dos tempos de quarentena forçada pelo covid-19. Available at: http://opais.sapo.mz/direito-digital-o-direito-preferencial-dos-tempos-de-quarentena-forcada-pelo-covid19-

CIP (2010). *Sobre o Registo de Cartões SIM*. Diploma Ministerial incoerente, ilegal e anticonstitucional. Observatório de Direito nº 1, CIP, 2010. Available at: https://macua.blogs.com/files/observatório-de-direito-nº-1.-registo-de-cartões-sim-é-ilegal-e-anti-constitucional.-documento-do-cip-2010.pdf

De Brito, L., Chaimite, E., Pereira, C., Posse, L., Sambo, M., & Shaankland, A. (2017). Revoltas da fome: Protestos populares em Mocambique (2008-2012)" in De Brito, L. (ed.) *Agora eles têm medo de nós! Uma coletancia de textos sobre as revolstas populares em Mocambique (2008-2012)*, 1-45. Maputo: IESE.

DW (2013). Greves em Mocambique: Um sinal de mudança? Available at: https://www.dw.com/pt-002/greves-em-moçambique-um-sinal-de-mudança/a-16651640

Foucault, M. (2014). *Vigiar e punir: O nascimento da prisão*, 42 ed. Petropolis: Vozes.

Ginisty, K. & Vivet, J. (2012). Frelimo territoriality in town: The exemple of Maputo. *L'Espace Politique*, 18(3). Available at: http://journals.openedition.org/espacepolitique/3164; https://doi.org/10.4000/espacepolitique.3164

Gonçalves, F. (2020). Camaras de vigilância: como o governo usa as tecnologias para controlar os cidadãos, *Jornal Savana*, Ano XXVIII, numero 1379, Maputo, 12 de Junho.

Gusmão, T.H.C. (2019). A vigilância eletrônica e a atuação do Estado sob perspectiva dos direitos do cidadão. Available at: https://jus.com.br/artigos/75880/a-vigilancia-eletronica-e-a-atuacao-do-estado-sob-perspectiva-dos-direitos-do-cidadao

INCM (2017). Registo de cartões "SIM" garante ao publico segurança e serviços de valor acrescentado.. In *25 anos do INCM: Instituto Nacional das Comunicações de Moçambique*, 7-10. Available at: https://www.arecom.gov.mz/index.php/sala-de-imprensa/telecomunicar/154-suplemento-25-anos-do-incm-edicao-especial-1/file

INCM (2019). Relatório de Regulação das Comunicações. Maputo: INCM. Available at: https://www.arecom.gov.mz/index.php/sala-de-imprensa/noticias/413-publicado-relatorio-de-regulacao-das-comunicacoes-do-ano-2019

INE (2019). CENSO 2017: Resultados definitivos. Available at: http://www.ine.gov.mz/iv-rgph-2017/mocambique/apresentacao-resultados-do-censo-2017-1; https://www.rtp.pt/noticias/economia/movitel-ganha-concurso-para-terceira-operadora-movel_n389962

Kwet, M. (2020, 27 January). The rise of smart camera networks, and why we should ban them. *The Intercept,* 27 January 2020. Available at: https://theintercept.com/2020/01/27/surveillance- cctv-smart-camera-networks/

Machava, B.L (2011). State discourse on internal security and the politics of punishment in post-independence Mozambique (1975-1983), *Journal of Southern African Studies,* 37(3): 593-609.

Medeiros, C.A. (1989). Aldeias comunais em Moçambique. *Finisterra*, 24(48): 336-340.

Morozov, E. (2010). *The net delusion: The dark side of internet freedom*. New York: Public Affairs.

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. New York: Public Affairs.

Ngoenha, S., Do Amaral, G. & Nhumaio, A. (2020). Cabo Delgado e o risco sistémico da guerra em Moçambique. In Forquilha, S. (ed.) *Desafios para Mocambique 2020*, 35-46. Maputo: IESE.

Observador (2016, 22 April). Greves e protestos em Moçambique coincidem com visita de Marcelo". Available at: https://observador.pt/2016/04/22/greves-protestos-mocambique-coincidem-visita-marcelo/

Rosário, D.M. (2014). Eleições e corrupção em Moçambique. In Cunha, I. & Serrano, E. (esa.) *Cobertura jornalística da corrupção política. Sistemas políticos, sistemas mediáticos, enquadramentos legais,* 124-148. Lisboa: Aletheia Editores.

Silveira, F.C. (2020). Corona vírus, monitoramento eletrônico e prova criminal. *Consultório Jurídico*. Available at: https://www.conjur.com.br/2020-abr-24/filipe-silveira-monitoramento-eletronico-prova-criminal

Swart, H. (2020). Video surveillance in Southern Africa: Case studies of internet-based security camera systems in the region. A report for the Media Policy and Democracy Project. Johannesburg: MPDP Available at: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf

Temudo, M.P. (2005). Campos de batalha da cidadania no Norte de Moçambique. *Cadernos de Estudos Africanos*, 7(8): 31-51.

Tsandzana, D. (2016, 16 May). Mozambican government is spying on its citizens according to @Verdade. *Global Voices.* Available at: https://advox.globalvoices.org/2016/05/16/ the-government-of-mozambique-is-spying-on-its-citizens-according-to-verdade

Tsandzana, D. (2018). Juventude urbana e redes sociais em Moçambique: A participação politica dos conectados desamparados. *Comunicação e Sociedade*, 34: 235-250. DOI:10.17231/comsoc.34.2947. Available at: https://www.academia.edu/38028668/Juventude_urbana_e_redes_sociais_em_Moçambique_a_participação_pol%C3%ADtica_dos_conectados_desamparados

Tsandzana, D. (2021). In Mozambique, a tug of war between public health and digital rights during the pandemic. Available at: https://globalvoices.org/2021/01/19/in-mozambique-a-tug-of-war-between-public-health-and-digital-rights-during-the-pandemic/

Legislation

Constitution of the Republic of Mozambique (1990). Maputo: National Press.

Diploma Ministerial n° 153/2010, Boletim da República, I Série, no 37, 15/09/2010

Law number 19/91, 18 August 1991 (Law of Crimes against State Security). Maputo: National Press.

Law number 2/2017, of 9 January (Creates the National Criminal Investigation Service, abbreviated as SERNIC). Maputo: National Press.

Law number 3/2017, of 9 January (Law of Electronic Transactions). Maputo: National Press.

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.