GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

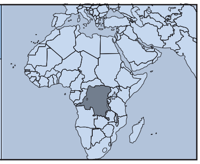
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

CONGO, REPUBLIC OF

Civil society and cyber surveillance in the Republic of Congo



AZUR Développement
Romeo Mbengou
www.azurdev.org

Introduction

Information and communications technologies (ICTs) now hold an important place in our daily lives. They are the source of many benefits, including easy and rapid exchanges and communication, data storage, and the digitisation of administrative procedures. However, technologies must be respectful of the privacy of users. This obligation applies to all, with few exceptions, and both to institutions and to individuals.

Yet, according to the revelations of Edward Snowden on the work of the US National Security Agency (NSA), it has now been established that we are not protected from spying eyes. Everything we do is monitored and followed by others for one reason or another. This is cyber surveillance: that is to say, the technical control of electronic communications. Some use it as a means to spy on what others are doing to prepare for any eventuality; others in order to do harm. Whether for one reason or another, cyber surveillance, except in cases where it is permitted by law, is harmful for users because it is a violation of fundamental human rights, including the right to have your privacy respected.

As a world phenomenon, cyber surveillance is ignored by some, its threat is minimised by others, and it is even non-existent in some countries. So, what is the situation in the Republic of Congo? How does civil society consider cyber surveillance? Several Congolese civil society organisations use ICTs in their everyday work. Do they feel monitored on the web? What about the Congolese legislation?

These are the questions that this report will try to answer. To do this, it is important to provide an overview of the legal framework for ICTs in Congo, before analysing civil society awareness of cyber surveillance in the country. This has been done through interviews with civil society organisations.

Overview of the legal framework for ICTs

The legal framework for ICTs in the Congo currently includes:

- The Congolese Constitution of 20 January 2002, which states in Article 19 that "everyone has the right to freely express and disseminate his opinions in speech, writing, image, or any other means of communication..." Article 20 says that "the secrecy of correspondence, telecommunications or any other form of communication cannot be violated except in the cases provided by law."
- Law No. 8-2001 of 12 November 2001 on the freedom of information and communication. This law guarantees the freedom to access information and communicate, including on the internet.
- Law No. 9-2009 of 25 November 2009 regulating the electronic communications sector. This law describes the conditions for the installation and operation of networks and electronic communications services. In Article 6 it states that "electronic communications activities are practiced freely in accordance with the terms of the legislation and regulations." This law, which also deals with the protection of users' privacy, prohibits cyber surveillance. Article 125 states: "It is unlawful for any person other than the users to listen to, record, or store communications and traffic data related to them, or submit it to any other means of interception or surveillance without the consent of the users concerned, except when legally authorised to do so..."[1]
- Law No. 11-2009 of 25 November 2009 establishing the regulatory agency of postal and electronic communications. In Article 5 it states that the agency promotes and protects the interests of users in the field of postal and electronic communications.

Other laws are being drafted, including a law on the protection of personal data, a law on cyber security, a law on the fight against cyber crime, a framework law on the Congolese information society and

[1] Law No. 9-2009 of 25 November 2009 regulating the electronic communications sector.

digital economy, and a plan for national broadband development in the Congo.

Use of ICTs by civil society

Congolese civil society organisations are working in several areas, including the defence and promotion of human rights in general, the preservation of the environment, the fight against poverty, the fight against corruption, the fight against HIV/AIDS, and the promotion of ICTs.

These organisations, such as the Congolese Observatory of Human Rights (OCDH), have worked and are working on sensitive issues concerning human rights, and, in the course of their work, they use ICTs. Some organisations have computers on which they can store sensitive data resulting from the analysis or investigation of violations of human rights. This data could include email addresses and phone numbers. The phone is the most frequently used way to contact a civil society organisation in the Congo. Very few organisations maintain a website, a blog or a Facebook account.

Analysis of cyber surveillance in the Congo

Interviews with civil society organisations involved in human rights and ICTs conducted for this report suggest that many are unaware of cyber surveillance. They also pointed to the lack of a government policy on cyber surveillance, and the lack of an independent body securing personal data.

Civil society's understanding of cyber surveillance

As suggested, it appears that a number of civil society organisations in the Congo have no clear understanding of cyber surveillance. This is largely due to them not having, for the most part, extensive knowledge of and experience in using computers and the internet. Given that they are seldom presented with circumstances that could draw their attention to cyber surveillance, several organisations do not suspect any surveillance, interception or control over the internet.

Loamba Moke, president of the Association for Human and Prisoners' Rights (ADHUC), commented, "The concept of cyber surveillance is unfamiliar to us. It is unclear whether our email communications are intercepted or stored, and we don't know how to secure our data on the internet." In other words, they do not have the expertise necessary to secure their communications, but are also unable to detect the interception or monitoring of their electronic communications. A similar point of view is held by Wilfrid Ngoyi Nzamba, executive secretary of the Congolese Association of ICT Consumer Products and Services, who argues that there is a clear lack of evidence on the existence of cyber surveillance. He states that "there is no cyber surveillance in Congo" – but for him the reasons include the fact that there are few people qualified to carry out surveillance in a country where there are still a lot of "computer illiterate" citizens among the population.

However, other organisations are more aware of digital security. This is the case with the Organisation for the Development of Human Rights in Congo (ODDHC), which conducted training on digital security for human rights defenders with the support of the Multi-Actor Joint Programme (PCPA) in March 2013. According to Sylvie Mfoutou Banga, president of the ODDHC, "The risk of the piracy of information from human rights advocates has led us to develop this training on human rights and digital security." Several topics were discussed during the workshop: how to create safe passwords, how to download and install free antivirus protection off the internet, and how to work on the internet without leaving digital traces. Regarding phones, Mfoutou does not know if her phone is tapped.

Another organisation, the Group of Journalists for Peace (GJP), has received training on the secure communications software FrontlineSMS and FrontlineCloud. Tools like these "allow members of an NGO to communicate safely," said Natalie Christine Foundou, the president of GJP. In 2013, AZUR Développement, in collaboration with the Association for Progressive Communications (APC), organised training on the protection of privacy in the management of online data on women and girl victims of violence.[2]

Lack of a common national policy on data protection

In the current institutional set-up, there is no common policy on data management, protection and privacy. Each institution or agency, both private and public, is obliged to manage its data in such a way that no data theft can happen. However, the reason why there is no common policy on data protection is simple: email services and websites are not hosted in Congo, but abroad, particularly in France and the United States. Only over the past three years have there been efforts to set up the Congolese Agency for Internet Naming (ACNIC). This new organisation will now manage the internet country code domain ''.cg".

"If Congolese civil society or any other person is subject to control or cyber surveillance, this would not be on the part of national authorities, but rather

[2] www.violencedomestique-congo.net

foreign institutions; and they will be monitored not as Congolese civil society necessarily, but as Yahoo or Google users," said Davy Silou, a computer engineer and independent consultant. He also mentioned that some computers used by civil society are often not secure, and do not use the original licences.

In addition, training in ICTs must remain a priority for the Ministry of Posts and Telecommunications, responsible for new technologies, and the Ministry of Higher Education, as a national data protection programme will require a high level of skills. There is still no computer course in the one and only public institution for higher education, the Marien Ngouabi University of Brazzaville. Investment in research and development are insufficient to be able to develop skilled human resources in the ICT sector in Congo. Cisco courses are offered at an approximate cost of 40,000 FCFA (USD 80) per module.

ICT incubator projects are insufficient. The company VMK created the Bantu Hub, a technology hub located in Brazzaville, which serves as a shared working space and an incubator for business start-ups. Bantu Hub hosts various activities that help to share knowledge and learning about ICTs.

Lack of an independent body ensuring data protection and civil liberties

The Republic of Congo also lacks an independent body for the protection of personal data and individual freedoms on the internet in Congo.

Article 130 of Law No. 9-2009 of 25 November 2009 regulating the electronic communications sector, appears to offer an opportunity for abuse. According to a provision, "for the purposes of defence and security, the fight against paedophilia and terrorism, network operators open to the public or electronic communications operators are required... to store the data for electronic communications. Individually designated and authorised governmental agents who have a special responsibility for this task may require operators and persons to share the data that has been stored and processed."[3]

The difference is that in other countries, citizen identification files are protected by independent bodies such as the National Commission for Computing and Civil Liberties (CNIL) in France, to ensure that electronic communications and data are at the service of the citizen, and that his or her privacy and personal freedoms are not violated. This is not yet the case for the Republic of Congo. Under these conditions, one may wonder if Congolese citizens and civil society in particular are actually safe from intrusion or control on the part of public and private authorities.

Conclusion

In light of the previous analysis, while the legal framework does not encourage the practice of data protection, it is clear that it is also difficult to identify or document if cyber surveillance is taking place. The skills at the disposal of civil society are very limited to do this. It is therefore important to equip Congolese civil society organisations with knowledge of security tools to prevent intrusion into or control of their communications. Beyond civil society, the government should invest enough in training, research and development in order to develop capacity in the field of ICTs, including ensuring data protection.

Action steps

In order to do the above, the implementation of the following recommendations may be necessary.

The government should:

- Adopt laws on the protection of personal data.
- Establish an independent body for overseeing the management of personal data.
- Create a computer training and internet course in higher education.
- Invest in ICT research and development.

Civil society should:

- Create awareness and train civil society on cyber surveillance.
- Build the capacity of civil society organisations so they can secure their personal data.
- Advocate for the adoption of a more protective legal framework for civil liberties on the internet.

International partners and organisations should:

- Provide financial and technical resources to civil society for awareness-raising programmes and training on internet safety.

[3] Law No. 9-2009 of 25 November 2009 regulating the electronic communications sector.