GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

Global Information Society Watch

2014

APC Hivos

Financial support provided by
Humanist Institute for Cooperation with Developing Countries (Hivos)

Global Information Society Watch
Published by APC and Hivos
2014

ISSN: 2225-4625
ISBN: 978-92-95102-16-3
APC-201408-CIPP-R-EN-DIGITAL-207

APC and Hivos would like to thank the Swedish International Cooperation Agency (Sida) for its support for Global Information Society Watch 2014.

SENEGAL

Communications surveillance in the Senegalese digital society

JONCTION
Ababacar Diop
www.jonctions.org

Introduction

Senegal, located in West Africa, is a country formerly colonised by France which gained its independence in 1960. It currently has a population of roughly 13 million people.

The advent of the Senegalese digital society in the late 1990s and its exponential development since the 2000s has led policy makers to set up an institutional and legal framework for digital activity with the adoption in 2008 of a series of laws governing the internet in the country.[1] Policy makers found this necessary for reasons of national security, and to establish a legal and institutional framework to protect citizens against crimes related to online activity.

ICTs have brought real changes in the forms of communication and exchange, not only at the corporate level, but also in the relationships between citizens. However, even if it is proven that ICTs are great tools at the service of freedom of speech, they also constitute a real danger when it comes to the privacy of correspondence.

The Senegalese media continue to reveal scandals about citizens' communications being monitored either by the government or by private companies.[2] This will be the subject of our discussion, which attempts to analyse the institutional and legal architecture of communications surveillance in Senegal.

Political context

Senegal has signed and acceded to several international and regional human rights instruments, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the African Charter on Human and Peoples' Rights.

The Universal Declaration of Human Rights states in Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The same UN text provides in Article 19: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[3]

In addition, Article 17 of the International Covenant on Civil and Political Rights states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[4]

In compliance with Senegal's international commitments, its constitution states in Article 13: "The secrecy of correspondence and of postal, telegraphic, telephonic and electronic communications shall be inviolable. This inviolability shall be subject only to such restrictions as are made applicable by law."[5]

"Noticing echoes..."

Senegal, like many countries in the world – as demonstrated by the revelations of Edward Snowden – is threatened by the practice of illegal surveillance of communications. This practice, which does not meet international standards prescribed by the relevant United Nations texts, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, is a real threat to privacy, freedom of expression and the right to confidentiality of communications.

Revelations made by the Senegalese press about the tapping of citizens' telephone conversations, but also the monitoring of communications of employees in a telecommunication company, illustrate this.

1 www.jonctions.org/index.php?option=com_content&view=article&id=16&Itemid=62

2 Enquête+. (2013, July 29). Les enregistrements téléphonique comme moyens de preuves : "Illégaux" et "irrecevables", selon des juristes. Enquête+. www.enqueteplus.com/content/les-enregistrements-t%C3%A9l%C3%A9phoniques-comme-moyens-de-preuves-ill%C3%A9gaux-et-irrecevables-selon-des

3 www.un.org/en/documents/udhr/index.shtml#a12

4 www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

5 www.wipo.int/wipolex/en/details.jsp?id=6223

According to an article in the newspaper Le Pays, published on 5 September 2011 and posted on the OSIRIS website: "It is common: we often notice echoes in the middle of a call, unusual noise, interrupted conversations without apparent reason and even noise ... of mechanical tools. This implies that wiretaps are being made. To pierce the mystery surrounding the ongoing wiretapping that Senegalese are subject to, there could be no more appropriate source than a mobile phone company."[6] Moreover, the same newspaper reports in its edition on 30 November 2011: "Wiretaps were organised internally by the top management and have practically turned the lives of the workers upside down, reveal anonymous Tigo agents. Senior employees were unpleasantly surprised to receive sanctions and other requests for explanations, based on the content of messages sent by email."[7]

If these claims are true, they show infringements on the communications of Senegalese citizens by both the government and private companies. This constitutes a real threat to the enjoyment of fundamental human rights which our country has committed to respect.

According to Article 13 of the Senegalese constitution, as noted above, the secrecy of correspondence and communications is inviolable, and this inviolability is "subject only to such restrictions as are made applicable by law."

Even if there is no specific legislation on phone tapping, there are several laws and regulations protecting the confidentiality of correspondence and other communications. These include Law 2008-12 on the Protection of Personal Data, Law 2011-01 of 24 February 2011 on the Telecommunications Code, and the decree on electronic communications made for the purposes of Law 2008-08 of 25 January 2008 on Electronic Transactions.[8]

According to Article 7 of the Telecommunications Code: "The operators of telecommunications networks open to the public and suppliers of public telecommunications services, as well as their staff members, are sworn to secrecy of correspondence and continuity of the service under penalty of prosecution pursuant to Article 167 of the Penal Code. They must also ensure that consumers and users have optimal network conditions that guarantee confidentiality and neutrality of the service with respect to transmitted messages and the protection of privacy and personal data... There can be no exception to this rule unless under the conditions prescribed by law."[9]

Article 12 of the Telecommunications Code provides that "[a] judge or police officer, for the needs of the prosecution or an investigation, or the enforcement of a judicial ruling, may require that telecommunications operators and service providers or telecommunications networks make available useful information stored in the computer systems they administer. Telecommunications operators and service providers of telecommunications networks are required to submit the required information to the authorities."[10] In other words, only a judge or police officer is authorised by law to order a restriction on the inviolability of private communications. This seems to be, for us, consistent with the principle of legality as well as that of the competent judicial authority provided by the 13 International Principles on the Application of Human Rights to Communications Surveillance.[11] According to the principle of legality, "Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act."

However, the law should be more precise to comply with the principle of adequacy, by specifying the extent and limits of an order by a judge or police officer under Article 12 of the Telecommunications Code. According to the principle of adequacy as established in the abovementioned 13 International Principles, "Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified." For us, it seems to be necessary that the judge or police officer declare the legitimate aim pursued by the order, which has the advantage of avoiding any abuse by the authorities.

In light of this, there is no doubt that the incidents reported above are unfairly and severely violating the integrity of the communications of citizens, because they do not have any legal grounds. Beyond that, they are a breach of citizens' rights to privacy and freedom of expression as enshrined in the Senegalese legal system.

It is undisputed that, for security requirements, the state may conduct surveillance of communications. But monitoring the communications or correspondence of citizens outside of legal channels is an intrusive act against privacy and personal data protection, and stands against human dignity.

6 Diagne, E. (2011, September 5). Surveillance des communications téléphoniques : Pourquoi et comment l'État écoute les citoyens. Osiris. osiris.sn/Surveillance-des-communications.html

7 Seck, A. A. (2011, November 30). Tigo et le scandale des écoute téléphoniques. Senenews.com. www.senenews.com/2011/11/30/tigo-et-le-scandale-des-ecoutes-telephoniques_17135.html

8 www.jonctions.org/index.php?option=com_content&view=article&id=16&Itemid=62

9 www.gouv.sn/IMG/pdf/code_des_Telecom_2011_senegal.pdf

10 Ibid.

11 https://en.necessaryandproportionate.org/text

It is even more serious if illegal surveillance of employee communications is the work of private companies. The case of the telecommunications company cited earlier, illegally "spying" on its employees by monitoring their electronic correspondence and telephone communications, reveals serious issues when it comes to human rights and fundamental freedoms within the company. These rights are at the heart of corporate social responsibility.

In addition to the monitoring by the state and companies, citizens monitor each other. Often scandals involve people illegally recording the private conversations of others using mobile phones. These recordings not only infringe on privacy, but are sometimes used to attack the dignity of others.[12]

This is why the government – but also citizens – should proactively protect the right to privacy of correspondence, not only to be compliant with international standards of human rights, but also to ensure the safety and the social and democratic stability of our country.

Conclusion

The rapid growth of ICT use raises the issue of the security of communications and electronic exchanges. This is not only a technical issue but also a societal one. What are actually being threatened are the foundations of the rule of law and a democratic society, which are the aspiration of African countries, including our country, Senegal.

However, given the recent situation prevailing in Nigeria, with attacks and kidnappings carried out by Boko Haram, one can legitimately ask whether it is not useful to better monitor communications to effectively fight against terrorism. Our answer is no, because the fight against terrorism should not justify the restriction of fundamental freedoms and widespread infringement on the privacy of citizens. The phenomenon of mass surveillance is a serious danger which civil society organisations and human rights activists have to face.

In this regard, in order to counter the threats to privacy, security and civil liberties, African states face challenges in putting in place appropriate institutional and legal mechanisms to enforce the right to privacy of correspondence. Fraudulent and illegal surveillance of communications in Senegal is a reality and the government, as guarantor of civil liberties, should find solutions. It is an absolute imperative of social and democratic stability, as well as of institutional and citizen security.

Although efforts are being made at the legislative and institutional level to respect the privacy of correspondence, the government must make an effort to protect citizens' internet rights from the threat of evolving surveillance technologies. With the rapid development of sophisticated technology, it becomes possible for private entities or individuals to violate the privacy of communications with the simple aim of harming others. When a telecommunications company is authorised to spy on the correspondence and communications of its own employees, this deserves special attention. It is the same when a citizen is equipped with sophisticated technological means to intercept or record callers without their knowledge, and for a non-lawful use.

While the dynamism of the ICT sector is progressing at an accelerated pace in our country, tools for recording and monitoring communications are becoming increasingly sophisticated and are often out of the government's control. Therefore it is necessary to implement appropriate legislation. The current legislation protecting the confidentiality of correspondence, freedom of expression and privacy does not, as we have seen, take care of all the issues and challenges of mass surveillance of communications.

Action steps

To better ensure the integrity of the digital space, privacy rights, and secrecy of correspondence, we recommend some actions that are absolutely necessary:

- Citizens should be constantly aware of surveillance practices in order to ensure respect of the right to privacy and protection of personal data and to defend against all unjustified and unlawful acts of communications monitoring.
- We recommend that the government further strengthen the legal and institutional framework for communications monitoring from the standpoint of respect for human rights. Also, the government should develop technical and human resources in order to have the ability to exercise appropriate controls on unauthorised wiretapping and communications surveillance technologies installed in Senegal, to ensure security and the public's civil liberties.
- The government must ensure that any regulations on communications surveillance conform to the 13 International Principles on the Application of Human Rights to Communications Surveillance.

12 Nettali.net. (2010, November 23). Affaire Diombasse Diaw : Khadija Mbaye et ses complices prennent 6 mois, Abdou Aziz Diop relaxé. Xalimasn. xalimasn.com/affaire-diombasse-diaw-khadija-mbaye-et-ses-complices-prennent-6-mois-abdou-aziz-diop-relaxe (In this case, the defendants were charged with, among others, acts of cyber crime. The victim was filmed without his knowledge by a supposed friend while he was naked and the footage was then found on the internet.)