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

Creative Commons Attribution 3.0 Licence <creativecommons.org/licenses/byncnd/3.0>

PERU

Rights versus crime: Twenty years of wiretapping and digital surveillance in Peru

Red Científica Peruana and Universidad Peruana de Ciencias Aplicadas
Fabiola Gutiérrez and Jorge Bossio
www.rcp.pe, www.upc.edu.pe

Introduction

The systematic monitoring of citizens by the state in Peru was revealed in 2000, after the collapse of the second administration of ex-president Alberto Fujimori (1995-2000). Fujimori resigned in his last year in office, after a network of government espionage and corruption was revealed. This included video recordings of secret meetings and alleged communications surveillance conducted and managed by presidential advisor Vladimiro Montesinos, working with the National Intelligence Service (SIN). This systematic surveillance by the state resulted in the dissemination of private information, recordings and videos of public officials, journalists and many other influential people.

These events sparked the beginning of the debate around the purpose of surveillance in Peru, and the violation of the right to private communications by state agencies and private entities – and what legislation could be developed to regulate this. This discussion is ongoing, with more cases of communications interception being revealed.

From state surveillance to industrial espionage and hacking

The Constitution of Peru establishes the privacy of communications as an individual right and does not differentiate between digital or non-digital communications. Nevertheless, respect for freedom of expression and association and non-discrimination, which are basic rights, have been violated many times due to the government's interest in tracking opposing opinions, the actions of political opponents, industrial competition or even religious tendencies and sexual preferences.

It is generally recognised that the state has the tools for monitoring, and can do so within a legal framework, with judicial approval, including in cases of suspected terrorism and crime. But, for instance, Peruvian legislation on cyber crime has also included a modification on what is permissible when it comes to tapping telephones, a change that has been met with criticism.

Over the past 15 years there have, as a result, been several cases of communications violations, both by the state and individuals. Among the most notorious cases: the surveillance by the Fujimori government; industrial espionage that revealed the corruption of officials in influence peddling and lobbying; the dissemination of private telephone conversations of electoral candidates; and the publication of the email communications of government ministers by journalists.

The Fujimori government, the intelligence services, and the use of the military for surveillance (2000)

The history of the regime of Alberto Fujimori, president of Peru during two consecutive terms (between 1990 and 2000), is stained by the corruption that led to his resignation. His presidential adviser Vladimiro Montesinos had a starring role in this story full of espionage and extortion, and even kidnapping and murder.

Montesinos effectively became the chief of intelligence services, where he allegedly created a giant spy network using army personnel and monitoring equipment, intercepting communications and recording videos of public officials, journalists, media entrepreneurs and other influential people.

Industrial espionage: The case of Business Track (2008)

Authorities found some 60,000 intercepted emails by journalists and politicians opposed to the government in the computer systems of the general manager of the private security firm Business Track, Manuel Ponce Feijoo, a retired Navy officer. Evidence of the wiretapping of officials and business executives was also discovered. The most relevant case was called *Petroaudios* (the so-called "oil recordings"), in which telephone conversations about illegal negotiations involving state oil concessions that would benefit a foreign company (Norway's Discover Petroleum Company) were recorded and disseminated. Following this discovery, the illegal

practices of a private company engaged in systematic espionage came to light.[1]

Communications violation: Monitoring a candidate for the mayoralty of Lima (2010)

On September 2010, during the election campaign for the mayoralty of Lima, a television programme broadcast an audio clip of a private telephone conversation between Christian People's Party candidate Lourdes Flores Nano and a former congressman from her party, Xavier Barron. In the conversation, Flores said that she no longer cared about the election, after the results of a preliminary voter poll in which her opponent, Susana Villarán, took the lead for the first time. "I am not interested in this election crap," she said in the extracts that were released, prompting her precipitous decline in voter preferences. This audio recording was a determining factor in her loss of the election.

National Security: Violation of a minister's official emails by LulzSec/Anonymous Peru (2013)

The hacker group LulzSec Peru, collaborators of Anonymous, obtained and shared emails from the Ministry of Interior, including the minister, Walter Alban. Digital communications about issues such as the tracking of regional opposition leaders, the security of officials and prosecutors' investigations were intercepted. The hackers said their intention was to prove the vulnerability of state information systems.

The weak line: Private versus public

After the dismantling of the National Intelligence Service (SIN) following numerous cases of secret video recordings being made and communications monitored during the Fujimori regime, a new intelligence agency called the National Intelligence Directorate (DINI) was created. A couple of years ago, it came to light that the budget for the DINI was increased in order to monitor public network repositories like social networks, forums or general topic lists, arguing that the use of these online platforms meant that this was not a violation of private communications.

However, this surveillance is on the borders of what is considered private and public, and raises the problem of the legality of monitoring the public in general without any suspicion of a crime being committed.

The surveillance by the DINI sparked a debate about access to and protection of information, as it cannot be argued that it has been done with a legitimate interest in mind – if this were the case, the law would have been followed and a court order would have been obtained. Although the increase in the budget allocated to the DINI is to monitor public networks, if they already do so illegally, the suspicion that they perform other types of communications surveillance looms with great force.[2]

The legal framework

Legislation relating to cyber crime in Peru is a relatively new category under the Penal Code. In 2000, provisions relating to espionage or computer hacking (Article 207-A) and computer sabotage (Art 207-B), that were within the scope of crimes against private property, were included. However, it became apparent over time that these did not respond to the needs of protection required when it came to information and communications technologies (ICTs).

In 2011, when the bill for the Cybercrime Law was presented to Congress, its original version meant that the police could access digital communications, and legislators felt that it did not respond properly to the right to privacy of communications. They argued that this right extends to all types of communication, and the bill had to be corrected.

The state filed a new version of the draft law, which was finally approved. However, the approved law was also questioned, because it prohibits, on the one hand, the creation of databases using any public information (which contradicts the law on access to information), and, on the other hand, leaves legislative gaps regarding telephone interceptions.

Cybercrime Law

On 22 October 2013 the new Cybercrime Law[3] was approved. This law was inspired by the Budapest Convention on Cybercrime[4] – although Peru is not a signatory to this international convention.

The new law punishes those who, using ICTs, "introduce, delete, copy, spoil, alter or suppress data, or render data inaccessible" for criminal purposes; those who engage in digital espionage, including telephone interceptions; engage in sexual harassment; and distribute child pornography.

Regarding telephone interceptions, the penalty for this offence has been increased to a maximum of eight years when it comes to classified or "secret and confidential" information. It also includes aggravating circumstances when the offence compromises national security, or when it is performed by public officials or those linked to these officials.

1 Romero, C., & Véliz, A. (2010, April 26). Tenía 53 mil emails hackeados. *La República*. www.larepublica.pe/26-04-2010/tenia-53-mil-emails-hackeados-0

2 Interview with Erick Iriarte A., lawyer and founding partner of Iriarte & Asociados (www.iriartelaw.com), 24 May 2014.

3 Law No. 30096 of 2013.

4 conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

But the Cybercrime Law violates at least two other rights:

Access to information

The law establishes a sentence of three to six years for persons found guilty of capturing digital information from a public institution, such as what is spent on social programmes, and complements this with new data to analyse the information (such as when a journalist analyses public data from different sources, creating a new data set). Critics of this legislation understand that at this point it contradicts the Law on Transparency and Access to Public Information.[5]

Article 6 of the law on access to information makes it a criminal offence to use data without permission, which means that anyone who accesses public information without authorisation and creates a database where this information could be disseminated would be guilty of a crime. In this way, access to public information and the right to freedom of information are limited.[6]

This observation sparked the debate among politicians, civil society and experts and prompted a review. Article 6 was repealed in March 2014.

Information freedom

The amended article regarding telephone interceptions included in the Cybercrime Law goes as far as to punish any kind of monitoring, regardless of the purpose. This makes the privacy of communications so strict that the monitoring of public officials in order to secure transparency is also prohibited, affecting citizens' freedom of information and their ability to conduct research in the public interest. The exemption that applies to the media, and which refers to an exemption of the penalty when investigating or monitoring issues of public interest, was not included in the amendments of the law passed.

Conclusions

Mass surveillance by the Peruvian state has not been proven in recent years; however, it is known that the national intelligence services are treading a thin line of legality through their use of surveillance tools to monitor citizens' publicly shared information, which according to the norm is a crime too. The increase in the budget for the DINI suggests that they could be doing more than that. Ideally, these resources should be directed to using surveillance as a tool for protection and security – but we do not know yet know if that is the case.

Regarding the legal framework for surveillance, the biggest problem is not the law itself, but its interpretation and application. This creates the need for specialised training for legal practitioners, prosecutors and law enforcement authorities in technical terms and standards and technological methods related to the violation of communications in all aspects.

The Cybercrime Law appears to affect freedom of information legislation, which guarantees transparency in the public sector. The Cybercrime Law also impacts negatively on other genuine rights that allow society and individuals to exercise democratic control and play an oversight role. The fact is that what one law defends, the other blocks.

Undeniably, the many cases of interception pushed the approval of the Cybercrime Law, in the pursuit of legal mechanisms to curb such crimes. However, the result reflects little analysis on the topic, poor legal specifications, little precision in the application of the law, and the lack of a conscious review of comparative international laws that could have contributed to making it more efficient and appropriate.

Action steps

The debate on how to improve the Cybercrime Law should continue. Specifically, it should include the clause on media exemption in order to keep track of what is considered in the public interest. In this sense, it is also crucial to protect the right to freedom of information and investigation, which serves as a mechanism for citizen control in governmental affairs.

Given the uniqueness of the environment in which it must be applied, the Cybercrime Law could be reviewed by legal practitioners and compared to similar laws in other countries. It would also be advisable to add some kind of standard glossary of terms as an interpretive guide.

Civil society organisations that are frequently monitored should place more importance on the need to encrypt information and have reliable security mechanisms for their communications. Security protocols and devices can be used to prevent communications being violated. Internet service providers (ISPs) must guarantee their users reliable and safe communications, since it is very likely that intermediaries are used in surveillance.

Finally it is clear that the opposition, civil society and the media cannot give up fighting for their rights to privacy and to exercise their oversight of public affairs. The state will always try to find ways to control its citizens, and Peruvians already know that surveillance is just one of these ways.

5 Law No. 27806 of 2002.

6 Interview with Roberto Pereira C., lawyer and legal consultant at the Press and Society Institute (IPYS) (www.ipys.org), 14 May 2014.