Examining Internet Freedom in Latin America (EXLILA)

Country report: Mexico

Luis Fernando García and Vladimir Chorny

R3D: Red en Defensa de los Derechos Digitales

Association for Progressive Communications (APC)
March 2016

This report was produced as part of the APC project Examining Internet Freedom in Latin America (EXLILA). The project is funded by the Open Society Institute (OSI) and APC and coordinated by Derechos Digitales.

Table of contents

1. Executive summary....3
2. Introduction....3
3. General legal framework: Main regulations on the internet....4
4. Problematic cases: Judicial and non-judicial cases....5
4.1. Constitutional appeal against the Telecommunications Law....5
4.2. Hacking Team in Mexico....6
4.3. Censorship of internet links by the National Institute of Transparency, Access to Information and Data Protection....6
4.4. Practices contrary to net neutrality....7
4.5. Cyber crime bill....7
5. Conclusions and recommendations....8

1. Executive summary

Mexico's Constitution recognises the right of access to information and communication technologies (ICTs). However, the population has a low rate of access to the internet.

The law recognises net neutrality, including the principles of non-discrimination and free access. However, there is documentary evidence of practices that run contrary to these principles. The Federal Telecommunications Institute (IFT – Instituto Federal de Telecomunicaciones) should issue guidelines on internet traffic management that enforce the legal obligation to protect net neutrality.

The Mexican authorities have augmented their technical and legal powers of surveillance of communications. The legislation does not clearly and precisely identify which authorities are empowered nor in what circumstances surveillance may take place. In some cases, the legislation does not recognise the requirement for judicial authorisation to carry out surveillance nor does it establish other safeguards against abuse.

There is documentary evidence that several authorities have acquired malicious software for surveillance purposes. Most of these authorities are not legally empowered to conduct surveillance of communications. Some authorities have been found to have used the malicious software against political opponents.

Widespread internet content blocking, filtering or regulation have not been reported in Mexico. However, the right to freedom of expression on the internet is under threat due to the context of violence, which is particularly serious against journalists. Similarly, some interpretations of the right to privacy of personal information have led to censorship of links to information of public interest about cases of corruption, and have proposed wide-ranging responsibilities for intermediaries.

Some legislative initiatives, for example, a bill to create a law on cyber crime, lack technical and legal rigour, and could criminalise legitimate uses of technology, which would affect the exercise of internet rights as well as the overall functioning of the internet.

2. Introduction

Mexico is one of the most populous countries in Latin America and one of the largest economies in the region, yet only 51% of the population has access to the internet,[1] a low penetration rate compared with other countries of the region.

The telecommunications sector is highly concentrated. For instance, one company alone (Telmex) controls 60.2% of the fixed broadband market and 89% of the mobile broadband market.[2]

Meanwhile, international organisations for the defence of human rights recognise that Mexico is experiencing a serious human rights crisis, characterised by extreme insecurity and violence, forced disappearances, extrajudicial killings, torture and high levels of impunity.[3]

[1]Asociación Mexicana de Internet (AMIPCI). (2015). Estudio sobre los hábitos de los usuarios de internet en México. www.amipci.org.mx/images/AMIPCI_HABITOS_DEL_INTERNAUTA_MEXICANO_2015.pdf

[2]Instituto Federal de Telecomunicaciones - IFT. Sistema de Información Estadística de Mercados de Telecomunicaciones (SIEMT). siemt.ift.org.mx

[3]Comisión Interamericana de Derechos Humanos (CIDH). (2015). Observaciones preliminares de la visita in Loco de la CIDH a México. www.oas.org/es/cidh/prensa/comunicados/2015/112A.asp

Journalists and human rights defenders are particularly vulnerable to violence, especially in places where organised crime is active and there is collusion with state agents. To give an example, 67 journalists have been murdered in the last decade.[4]

Due to this situation, self-censorship has reduced the availability of information of public interest in the traditional media, making the internet an essential resource for people to be informed about matters affecting their communities. Internet platforms have also become spaces for political protest and criticism with a large influence on public opinion and on the behaviour of public figures and officials.

Public debate around regulatory policies and strategies affecting the internet has increased, and laws and administrative and judicial decisions have been passed, sometimes threatening the exercise of human rights on the internet.

What follows is a brief summary of legislation, policies and emblematic cases on the state of internet freedom in Mexico.

3. General legal framework: Main regulations on the internet

Article 6 of the Constitution of Mexico recognises the duty of the state to guarantee access to information and communications technologies (ICTs), including the internet. Item B ii of the same article establishes that telecommunications are a public service of general interest, and must be provided under conditions of competition, quality, plurality, universal coverage, interconnection, convergence, continuity, free access and without arbitrary interference.

In spite of this broad constitutional recognition of the internet as a public service of general interest which must be guaranteed by the state under conditions of free and universal access, without arbitrary interference, secondary legislation does not always live up to this principle.

The Federal Telecommunications and Broadcasting Law was enacted to implement the constitutional obligations toward the internet. In Articles 145 and 146 it establishes net neutrality principles for internet access services. Amongst these principles are freedom of choice, non-discrimination, privacy, transparency and quality, and it also limits the possibilities for internet traffic management by service providers.

The Federal Telecommunications Institute (IFT – Instituto Federal de Telecomunicaciones), the autonomous body provided in the constitution to be the regulator of the sector, has yet to implement these principles by issuing guidelines on internet traffic management.

Articles 189 and 190 of the Telecommunications and Broadcasting Law establish various measures allowing surveillance of communications by the authorities. Telecommunications companies are obliged to keep data records on all their users, including the origin and destination of communications, date, time and duration and even the geographical location of devices. The law demands that this "communication metadata" be retained for two years.

The law also stipulates an obligation to cooperate with security and justice agencies for telecommunications companies and those providing internet applications, content or services. Such cooperation includes handing over metadata, tapping private communications, and real-time geographical localisation of communication devices. However, the law does not clearly specify in detail which

[4]Ibid.

authorities may request such cooperation, or under what circumstances. There is no explicit mention of the need for a court order or other transparency and accountability measures to prevent or avoid the abuse of surveillance measures.

Other laws also provide for state surveillance measures. The National Code of Criminal Procedure, for example, empowers the country's district attorneys and prosecuting offices to tap private communications and access metadata after obtaining a court order, as well as to demand real-time geographical localisation of communication devices, although in this case the code does not stipulate the need for a court order. Authorities in charge of criminal investigations are granted similar powers under the General Law to Prevent and Punish Crimes of Kidnapping (Articles 24 and 25) and the Federal Law against Organised Crime (Articles 8 and 16-28).

The National Security Law empowers the Investigations and National Security Centre to tap private communications, although it uses vague language about the circumstances in which "threats to national security" justify these measures. Similarly, the Federal Police Law empowers the federal police to carry out surveillance measures in order to prevent crime.

Another law with implications for the digital environment in Mexico is the Federal Law on the protection of personal data held by private individuals, which recognises the rights of access, correction, cancellation and opposition of personal data that must be complied with by internet companies providing services in the country.

Despite the personal data protection provided for internet users by this law, the National Institute for Access to Information and Data Protection (INAI) has interpreted the law in ways that limit the right to freedom of expression on the internet, by ruling that the right to correction and cancellation of personal data gives people the right to demand that internet intermediaries, as well as search engines, remove links to content they consider detrimental to their reputation, or that constitute unauthorised use of their personal data.

Finally, the Federal Criminal Code defines several crimes directly related to the internet, for instance, the crimes of illegal access to computer systems and equipment mentioned in Article 211 bis 1-7.

4. Problematic cases: Judicial and non-judicial cases

Controversy over internet rights has intensified in Mexico in recent years. Some cases that illustrate this conflict are summarised below.

4.1. Constitutional appeal against the Telecommunications Law

A group of people lodged a constitutional appeal against the provisions of the Federal Telecommunications and Broadcasting Law, which requires the saving of metadata on telecommunications users and other invasions of the privacy of communications.

Since communications surveillance measures are, by nature, carried out in secret, establishing the legitimacy of the appeal was difficult, as normally the person challenging a law must show that the entry into force of the law itself affects him or her, or that the law has been enforced against the person.

The court of first instance recognised the procedural legitimacy of a challenge by any person against covert surveillance measures such as those contested. However, on further analysis it ruled the measures

in the law were constitutional because they were for the legitimate purpose of protecting security. This decision has been challenged and the final ruling will be made by the second chamber of Mexico's Supreme Court.

4.2. Hacking Team in Mexico

In 2015, internal documents of the Italian firm Hacking Team were leaked, revealing that many Mexican authorities had purchased malicious spyware, most of them without even having constitutional or legal powers to tap private communications.[5]

It was also discovered that Mexico is Hacking Team's best client, because it is the country with the most current or potential clients and the source of the Italian company's greatest profits.[6]

Hacking Team's clients include the Baja California Secretariat for Planning and Finances, the Jalisco Government Secretariat and the offices of the governors of Querétaro and Puebla, as well as state companies like PEMEX.[7] These authorities are not constitutionally or legally empowered to tap private communications, and so obtaining and using software and equipment sold by Hacking Team through intermediary companies in Mexico is clearly illegal. It has also been shown that authorities like the Puebla state government have used software purchased from Hacking Team to spy on political opponents.[8]

It was also revealed that the Secretariat of National Defence was holding conversations for the acquisition of Hacking Team software called "Pegasus". According to the leaked documents, the Mexican army was seeking the capacity to infect and spy on 600 targets simultaneously,[9] in spite of the fact that it has no legal powers whatsoever to tap private communications of the civilian population.

4.3. Censorship of internet links by the National Institute of Transparency, Access to Information and Data Protection

INAI recently decided to order Google to remove three links to internet pages that mention the name of a member of the business community.[10] The INAI decision was based on a broad interpretation of the rights of cancellation and opposition of personal data, applying the European doctrine developed by the European Union's Court of Justice popularly known as the "right to be forgotten".[11]

One of the links ordered removed was to a report in the magazine *Revista Fortuna* documenting alleged acts of corruption involving a transport company and public officials, including the family of a former

[5]Ángel, A. (2015, 7 July). México, el principal cliente de una empresa que vende software para espiar. *Animal Político.* www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente; Ángel, A. (2015, 21 July). Sedena negoció compra de software de Hacking Team en 2015 para espiar a 600 personas. *Animal Político.* www.animalpolitico.com/2015/07/sedena-negocio-compra-de-software-a-hacking-team-en-2015-para-espiar-a-600-personas

[6]Ángel, A. (2015, 7 July). Op. cit.

[7]Ibid.

[8]Aroche, E. (2015, 22 July). El Gobierno de Puebla utilizó el software de Hacking Team para espionaje político. *Animal Político.* www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico

[9]Ángel, A. (2015, 21 July). Op. cit.

[10]Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2015). Procedimiento de Protección de Datos Personales. Expediente PPD.0094/14. inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf

[11]Red en Defensa de los Derechos Digitales – R3D. (2015). Decisión del IFAI compromete libertad de expresión. r3d.mx/wp-content/uploads/2015/01/posicionamiento_IFAIGOOGLE.pdf

Mexican president.[12] INAI's censorship order is a highly threatening precedent for the right to freedom of expression.

Legal action has been taken by Google and *Revista Fortuna* to oppose the INAI decision, which is currently suspended. However, reputation management companies have been emboldened to demand that digital media remove information on the internet related to public figures on the basis of their clients' rights to cancellation and opposition of personal data.

4.4. Practices contrary to net neutrality

Although, as has been pointed out, the Constitution and the Federal Telecommunications and Broadcasting Law recognise and protect net neutrality, the IFT has not begun the process of issuing guidelines on net neutrality in spite of this having been scheduled for August 2015.[13]

There is evidence of a series of practices contrary to net neutrality that have been actively promoted by internet access providers and providers of applications and services, even with the cooperation of the federal government, as in the case of zero-rating offers and Facebook's programmes Internet.org and Free Basics.[14]

In spite of documentary evidence of practices contrary to net neutrality, such as zero-rating, the IFT has been remiss in taking action against these violations, which opens the door to normalisation of these practices, to the detriment of the right to freedom of expression on the internet.

4.5. Cyber crime bill

In October 2015, Senator Omar Fayad presented a bill for a Federal Law to Prevent and Punish Cyber Crime.[15] The proposed law would have established a series of severe punishments for a wide range of actions.[16]

For example, a proposed article on "offences against computer systems" was so poorly drafted that it would have imposed a penalty of up to 15 years in prison for "wilfully carrying out any act resulting in a change in the functioning of a computer system," which would have effectively criminalised an enormous number of legitimate and everyday uses of technology.

Similarly, a series of offences "against improper disclosure of personal information" would have criminalised any non-consensual use of personal information, even when such use caused no harm or the information disclosed was of public interest. Concepts such as "cyber weapons" or "cyber terrorism" were also couched in vague and imprecise language that could have had serious consequences for the journalistic profession and the exercise of other rights to freedom of expression.

[12]Pérez, A.L. (2007). Fraude en Estrella Blanca alcanza a Vamos México. *Revista Fortuna*, VI(49). revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm

[13]IFT. (2015). Programa Anual de Trabajo. portalanterior.ift.org.mx/iftweb/wp-content/uploads/2015/01/PAT-2015-vF.pdf

[14]R3D. (2015). *Neutralidad de la Red en México: Del dicho al hecho. Informe sobre prácticas contrarias a la neutralidad de la red ejercidas por proveedores de servicio de internet en México, 2015*. s3.amazonaws.com/f.cl.ly/items/3K2T3v0b452g0a1C0d2E/R3D%20-%20Neutralidad%20de%20la%20red%20en%20Mexico%202015.pdf

[15]Iniciativa con proyecto de decreto por el que se expide la Ley Federal para Prevenir y Sancionar los Delitos Informáticos (2015). www.senado.gob.mx/sgsp/gaceta/63/1/2015-10-27-1/assets/documentos/Inic_PRI_Ley_Delitos_Informaticos.pdf

[16]R3D. (2015). 10 puntos clave sobre la Ley Fayad, la peor iniciativa de ley sobre internet en la historia. r3d.mx/2015/10/28/10-puntos-clave-sobre-la-leyfayad-la-peor-iniciativa-de-ley-sobre-internet-en-la-historia

The bill also included measures that would have affected the privacy of internet users, for example, requiring all telecommunications and internet companies to maintain records on internet use by all their users and to hand over this information to the authorities, without any safeguards against the abuse of these measures being included in the bill.

The controversy raised by the bill led to its being withdrawn only a week after its presentation in the Mexican Senate. However, it has been announced that a process is under way to create a new bill to establish new cyber crimes.

5. Conclusions and recommendations

- Although the Constitution recognises access to ICTs, including the internet, as a right, a low proportion of Mexico's population has access to the internet. The Mexican state should implement policies to achieve universal coverage.
- While the Federal Telecommunications and Broadcasting Law recognises net neutrality and, in particular, the principles of non-discrimination and free access, practices contrary to these principles have been identified. It is essential for the IFT to issue guidelines on traffic management and net neutrality, so that the institute may verify compliance by internet access providers with their legal obligations, and where necessary enforce the relevant penalties.
- The legislation and practice of communications surveillance lack clarity, precision and the necessary safeguards against abuse. The law must define precisely which authorities are empowered to carry out surveillance and the circumstances in which they may use such measures. It is essential to have safeguards against abuse, such as supervision by the courts, the right of the affected person to be notified, and independent measures of transparency and supervision.
- Cases have been detected of purchase and illegal use of malicious spyware but no administrative or criminal responsibility has been incurred. Illegal surveillance, especially when committed by state agents, must not remain unpunished as this only encourages further cases.
- While widespread information regulation, filtering or blocking of content on the internet do not occur, the right to freedom of expression on the internet in Mexico is threatened by the high levels of violence, especially against journalists. In addition, some administrative decisions like that adopted by INAI ordering the removal of links to information of public interest compromise the free flow of information on the internet.
- It is important that any restrictions on freedom of expression on the internet comply strictly with international standards, and in particular, take into account the impact such decisions may have on the functioning of the internet.
- There are plans to reform or create new legislation to regulate actions taken through computer systems. Some attempts, like the Fayad Bill, have lacked precision and would have severely restricted the right to freedom of expression on the internet. Any cyber crime legislation should be drafted carefully so as not to criminalise legitimate uses of technology. The impact of poorly defined cyber crimes on human rights and internet functioning should be taken into account.