PRIVACY INTERNATIONAL

Stakeholder report
Universal Periodic Review
31st session period – Mexico

The Right to Privacy in the United Mexican States

Presented by Red en Defensa de los Derechos Digitales (R3D) and Privacy International

March 2018

The Right to Privacy in the United Mexican States

March 2018

PRIVACY INTERNATIONAL

www.privacyinternational.org

R3D
Red en Defensa
de los Derechos Digitales

INTRODUCTION

1. This report is presented by Red en Defensa de los Derechos Digitales (R3D) and Privacy International (PI). La Red en Defensa de los Derechos Digitales (R3D) is a non-governmental, non-profit organisation located in Mexico, dedicated to the defence of human rights in the digital environment. Privacy International (PI) is a non-governmental, non-profit organisation located in London, focused on the defence, promotion and protection of the right to privacy around the world.

2. PI and R3D wish to raise concerns regarding the situation of the violation of the right to privacy in Mexico, for consideration in the next review of Mexico as part of the 31st session of the Universal Periodic Review (UPR) Working Group.

Right to Privacy

3. Privacy is a fundamental right recognised in numerous international human rights instruments.[1] The right to privacy enables the exercise of other rights such as the right to freedom of expression, free association, and access to information, and it is essential for the dignity of people and the viability of democratic systems.

4. Infringements of the right to privacy can only be justified when they are established by law, necessary to achieve a legitimate goal, and proportional to the objective pursued.

5. Based on the development of information technologies that have enabled the mass collection, retention and processing of data, protection of the right to privacy has expanded to the processing of personal data. Several international instruments include personal data protection principles,[2] and such principles have been incorporated into many national laws, such as Mexico's[3].

[1] Declaración Universal de Derechos Humanos Article 12, Convención de las Naciones Unidas sobre Trabajadores Migrantes Article 14, Convención de Naciones Unidas sobre los Derechos del Niño Article 16, Pacto Internacional sobre Derechos Civiles y Políticos Article 17; convenciones regionales including Article 10 of Carta Africana sobre los Derechos y el Bienestar del Niño, Article 11 of Convención Americana sobre Derechos Humanos, Article 4 of Principios de la Unión Africana sobre Libertad de Expresión, Article of Declaración Americana de los Derechos y Deberes del Hombre, Article 21 of Carta Árabe sobre Derechos Humanos and Article 8 of Convención Europea para la Protección de los Derechos Humanos y las Libertades Fundamentales; Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y Acceso a la Información, Principios de Camden sobre Libertad de Expresión e igualdad.

[2] See: Consejo de la Convención Europea para la Protección de Individuos con respecto al Procesamiento Automático de Datos Personales (Nº 108), 1981; Guía sobre protección de la privacidad y flujo transfronterizo de datos personales de la Organización para la Cooperación y el Desarrollo Económico (1980) and Guía para la regulación de bases de datos personalizadas (Resolución 45/95 de la Asamblea General y E/CN.4/1990/72).

[3] As of January 25, 2018, more than 100 countries around the world have adopted comprehensive personal data protection laws and approximately forty countries have pending approval of laws or initiatives dedicated to the protection of personal data. Banisar, David, National Comprehensive Data Protection / Privacy Laws and Bills 2018. January 25, 2018. Available at: https://ssrn.com/abstract=1951416

The Right to Privacy in Mexico

6. The Political Constitution of the United Mexican States recognises the right to privacy in Article 16, which upholds:

   'No one shall be disturbed in his person, family, domicile, papers, or possessions, except by virtue of a written order of the competent authority establishing and substantiating the legal cause for the proceeding.[4]'

7. Regarding the right to privacy of private communications, Article 16 of the Constitution also states that:

   'Private communications are inviolable. The law will criminally sanction any act that impinges on the freedom and privacy of the same, except when they are supplied voluntarily by any of the individuals participating in them. The judge will assess the scope of these, provided that they contain information related to the commission of a crime. Under no circumstances will communications that violate the duty of confidentiality established by law be admitted.

   The federal judicial authority exclusively, at the request of the federal authority that authorises the law or the holder of the Public Ministry of the corresponding federal entity, may authorise the tapping of any private communication. To do this, the competent authority must establish and substantiate the legal causes of the request, as well as state the type of tapping, the subjects of the same and its duration. The federal judicial authority may not grant these authorisations when dealing with matters of an electoral, fiscal, mercantile, civil, labour or administrative nature, nor in the case of the detainee's communications with his counsel.'

8. The Federal Law for the Protection of Personal Data in Possession of Bound Entities[5] and the Federal Law for the Protection of Personal Data in Possession of Individuals[6] regulate the processing of personal data in Mexico.

9. The Mexican Constitution deems all human rights standards listed in international treaties to be at the same hierarchical level as the Constitution. Mexico is part of all the major human rights treaties of the universal system and of the Inter-American human rights system.

Monitoring the Previous UPR

10. The report presented by Mexico during the 17th session of the Universal Periodic Review, which took place in October 2013, does not mention the right to privacy. In the reviews conducted on Mexico in past sessions, there have been no recommendations from other member states on the right to privacy, although

[4] Constitución Política de los Estados Unidos Mexicanos Article 16. Available at: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf

[5] Available at http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[6] http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

there were several recommendations on the need to adopt appropriate measures to protect journalists and human rights defenders.

11. The summary of reports submitted by stakeholders during the previous review of Mexico includes a recommendation presented by Privacy International (PI) about the need for strict regulation and oversight by judicial authorities and other independent authorities on the use of digital surveillance programmes.[7]

ISSUES OF CONCERN

A. Inadequate regulation of communications surveillance in Mexico

12. In recent years, the Mexican State has increased its legal powers and technical capacity to implement surveillance measures. For example, laws such as the Federal Telecommunications and Broadcasting Law, the National Code of Criminal Proceedings and other laws have been issued and reformed to establish surveillance measures such as the following:

1. Massive and indiscriminate retention of communications data

13. Article 190, Section II, of the Federal Telecommunications and Broadcasting Law (LFTR) mandates telecommunications companies indiscriminately keep, for two years, communications record for all their users. This record includes a set of data known as 'communication metadata' which include: the origin and destination of communications; their date, time and duration; identification data of communicators and devices; and even the geographic location of users.

14. The disclosure or analysis of this data may compromise the privacy of all users. The generation of this massive and indiscriminate record severely compromises privacy, especially in the event of unlawful access to this data as a result of cyber attacks or acts of corruption.

15. That is why, for example, the European Court of Justice has invalidated legal requirements that provided for massive and indiscriminate retention obligations, insofar as they do not provide necessary or proportionate restrictions to the right to privacy.[8] The Human Rights Council of the United Nations has recognised that "metadata, when aggregated, can reveal personal information that is as sensitive as the content of communications"[9],

[7] Summary prepared by the Oficina del Alto Comisionado para los Derechos Humanos in accordance with paragraph 15 (b) of the annex to Consejo de Derechos Humanos resolution 5/1 and paragraph 5 of the annex to Council resolution 16/21. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/160/17/PDF/G1316017.pdf?OpenElement

[8] CJEU Digital Rights Ireland vs. Minister of Communications, Marine and Natural Resources et al. Casos Conjuntos, C-293/12 y C-594/12, April 8, 2014. Available at: http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=es&type=TXT&ancre=. See also CJEU. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson et al. Casos conjuntos C-203/15 y C-698/15, December 21, 2016. Available at: http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203&lang1=en&type=TXT&ancre=

[9] Resolución del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital, UN doc. A/HRC/RES/34/7.

and the Human Rights Committee has stated in the same vein that data retention policies constitute an interference with the right to privacy and that as a general rule, States must "refrain from imposing third party data retention schemes".[10]

2. Access to communications data and geolocation in real time

16. Access to the data kept by telecommunications companies and the real-time monitoring of the location of users are both poorly regulated in Mexico. For example, the LFTR does not clearly, accurately or thoroughly establish which authorities can carry out said surveillance measures or establish the circumstances and proceedings.

17. Nor is the need for judicial authorisation to carry out these privacy invasion measures explicitly established. Taking into account the context of human rights violations in Mexico where organised crime operates with tolerance, acquiescence, management or guidance on the part of public officials, the risk to privacy, security, physical integrity and life is seriously compromised by surveillance measures without safeguards against abuse.

3. Absence of adequate safeguards against abusive surveillance

18. Mexican legislation does not provide adequate and sufficient safeguards against the abuse of secret surveillance measures. In addition to not clearly and explicitly establishing the need for prior judicial regulation for all surveillance measures, the legislation does not take into account measures such as independent oversight or the right to notification of parties concerned. This prevents the detection, investigation and sanctioning of abusive surveillance operations.

19. Furthermore, although legislation provides some requirements for proactive transparency regarding surveillance measures such as publishing statistics on the use of surveillance, in practice these have not been implemented and the authorities and judiciary routinely deny access to these statistics, even in redacted versions, which prevents public scrutiny of these activities.

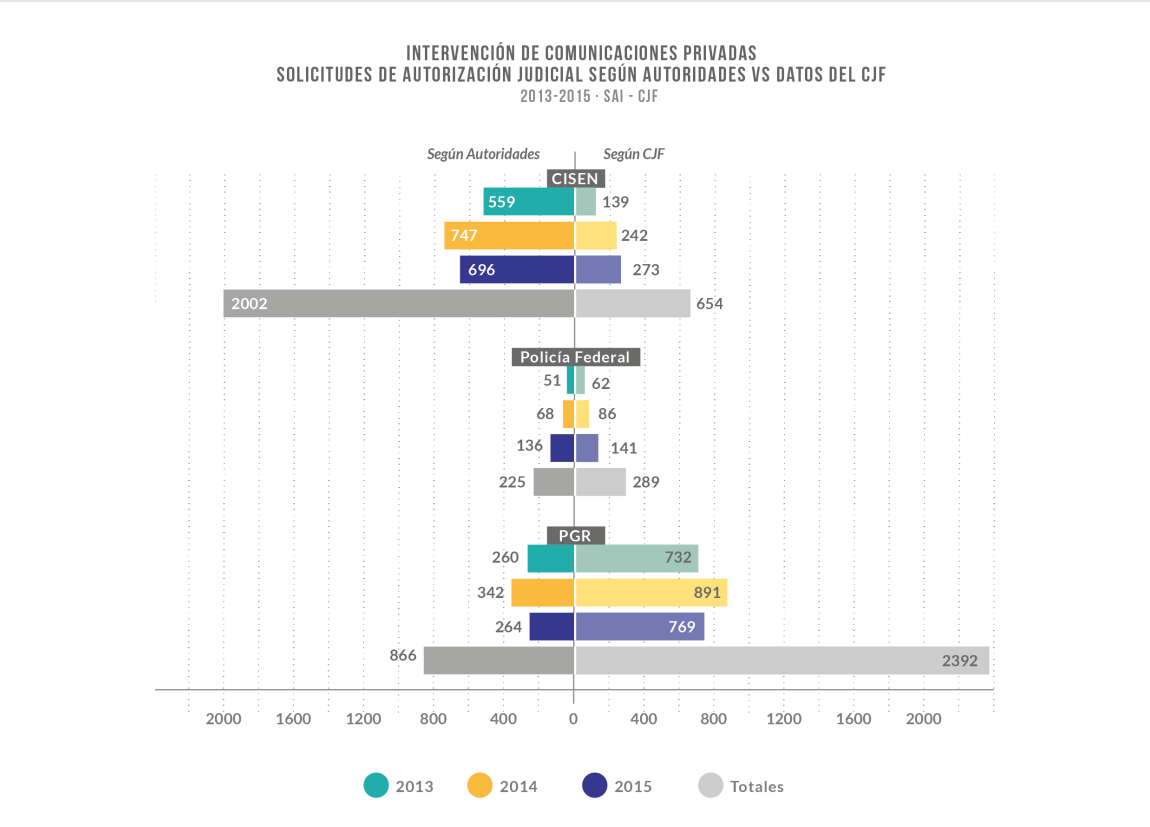
B. Unlawful and unchecked surveillance in Mexico

20. In addition to deficiencies in surveillance regulation in Mexico, unlawful and unchecked surveillance has been documented in Mexico. In the report *'The State of Surveillance: Out of Control,'*[11] Red en Defensa de los Derechos Digitales (R3D) documents various inconsistencies and illegalities.

[10] Observaciones finales del cuarto reporte periódico de los Estados Unidos de América. Comité de Derechos Humanos de la ONU, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (April 23, 2014).

[11] Available at: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

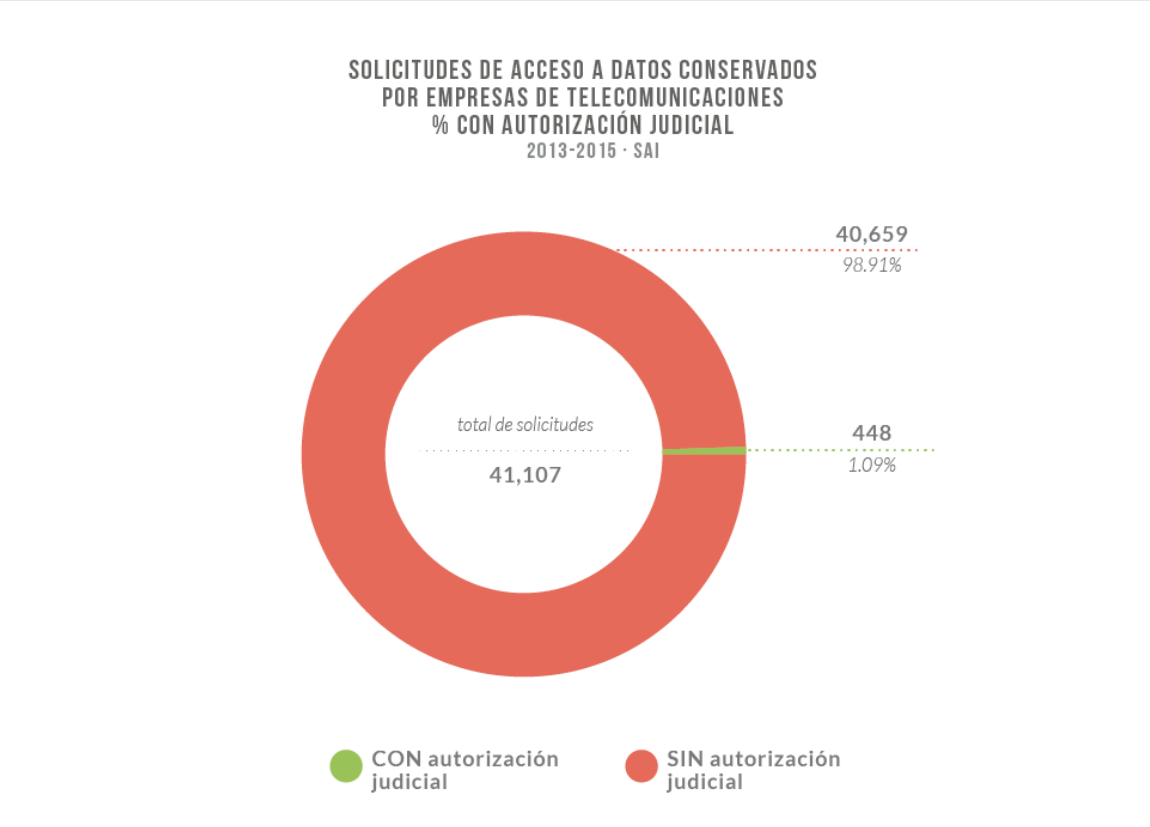
21. In the first place, there are serious inconsistencies between the data reported by the authorities that undertake surveillance of private communications, and the data provided by the judicial authorities of the Federation *(Poder Judicial de la Federación).* For example, between 2013 and 2015, the prosecutors' and attorneys' offices of the states of Colima, Zacatecas, Jalisco, Tabasco, Guerrero, Puebla, Querétaro and Quintana Roo reported having requested judicial authorisation to carry out surveillance of private communications. However, the Federal Judicial Branch does not report any request.



22. Similarly, as shown in the figure below, while the Centre for Research and National Security (CISEN) reports having made 2,002 requests for the surveillance of private communications between 2013 and 2015, the judiciary only acknowledges having received 654. By contrast, while the Office of the General Prosecutor (PGR) reports having requested judicial authorisation in 866 instances, the Judicial Branch reports 2,392 requests.[13]

23. Conversely, as apparent in the following figure, it has been documented that in 98.91% of instances where an authority has accessed data of telecommunications users retained by service providers, the authority has done so without judicial authorisation. The same has happened in cases of real-time geolocation.[14]

12 R3D. Estado de la Vigilancia: Fuera de Control. 2016. Pg. 45.
13 Idem.
14 Ibidem. Page 56.



24. Instances have even been documented in which authorities have accessed user communications data without even possessing legal powers, such as the Superior Court of Justice of Mexico City, the Government of the States of Mexico and Colima or the Secretariat of Finance and Public Credit.

25. Illegal access to user data has been facilitated by some telecommunications companies. While AT&T rejected about 46% of requests it received from authorities for not complying with the legal requirements, the largest operator, Telcel, did not reject any of the 87,650 requests for access to user data received in 2016 and the first half of 2017.[15]

26. In addition, the inefficiency of surveillance measures for the purpose of criminal investigation has been documented. Only 8% of the preliminary investigations in which a surveillance measure was carried out have culminated in criminal proceedings.[16] This suggests that more than 90% of people monitored in the context of a criminal investigation did not end up being accused of any crime.

15 Data obtained from the reports issued by Concesionarios y Autorizados en la prestación del servicio de telecomunicaciones to the Instituto Federal de Telecomunicaciones pertaining to the year 2016 and the first half of 2017, available at: https://drive.google.com/drive/folders/1DPMpb8LJtF3foQBZaiVd3WwqKOoyfi5R?usp=sharing

16 R3D. Estado de la Vigilancia: Fuera de Control. 2016. Pages 71-74.

C. Irregular acquisition and operation of surveillance malware in Mexico

27. In recent years it has been revealed that Mexican authorities have acquired highly sophisticated surveillance capacities. In particular, there is evidence that different authorities, both federal and state, have acquired the capacity to infect computers and mobile phones with different types of malicious programmes, which allow authorities to extract information from devices and even take control of them to turn them into a permanent surveillance mechanisms.

28. This has been enhanced by the absence of a legal framework to regulate and oversee the acquisition and use of these malicious programmes, and the lack of regulation regarding hacking activities by the State.

29. On 5 July 2015, a large number of the Italian firm Hacking Team's emails and internal documents were leaked to the public, exposing their customers and business practices.[17]

30. Out of a total of 35 countries, including Brazil, Chile, Colombia, Ecuador, Honduras and Panama, Mexico proved to be the firm's main client,[18] with transactions made by different local governments, units and federal agencies via various intermediary companies.

31. Among the authorities indicated to having commercial relations with Hacking Team are the Governments of Baja California, Campeche, Chihuahua, Durango, Guerrero, Jalisco, Nayarit, Puebla, Querétaro and Yucatán; the Attorney General of the State of Mexico; the Ministry of Public Security of Tamaulipas; and federal agencies such as the Ministry of National Defense, the Centre for Investigation and National Security, the Federal Police, the Office of the General Prosecutor, and even Petróleos Mexicanos (PEMEX). The vast majority of listed authorities do not even have legal powers to conduct surveillance of private communications, so both the acquisition and use of such technologies are clearly unlawful.

32. In August 2016, Citizen Lab,[19] an interdisciplinary laboratory of the Munk School of Global Affairs at the University of Toronto, Canada, revealed information about a sophisticated surveillance software named *Pegasus* marketed to governments by the company NSO Group.

33. According to the Citizen Lab research, most of the NSO infrastructure domains are linked to Mexico, which indicates that Mexican authorities are NSO clients and that people in Mexico could have been targets of this form of surveillance.

34. There is evidence that Mexican authorities such as the Secretariat of National Defense (SEDENA), the Office of the General Prosecutor (PGR) and the Centre

17 Privacy International (6 de julio de 2015) Surveillance company Hacking Team exposed. Available at: https://www.privacyinternational.org/node/618

18 Angel, A. (7 de julio de 2015) México, el principal cliente de una empresa que vende software para espiar. Animal Político. Available at: http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

19 Citizen Lab (2016) About Citizen Lab. Available at: https://citizenlab.org/about/

for Research and National Security (CISEN) bought the NSO software, *Pegasus*. Serious irregularities have been revealed about the Office of the General Prosecutor's process of contracting the Pegasus software along with its use against human rights defenders and journalists, as is explained in the following section.[20]

D. Espionage against journalists and human rights defenders in Mexico

35. Several instances have been documented in which surveillance, and in particular surveillance malware tools, has been used against dissidents, journalists and human rights defenders.

36. In February 2017, it was announced that the Mexican State used surveillance malware developed by the Israeli company NSO Group with the intent of spying on human rights defenders whose campaign focused on combatting obesity by increasing taxes on sugary drinks, including the director of El Poder del Consumidor, a Mexican consumer rights organisation. The attacks perpetrated against the activists took place while a campaign in favour of the tax on sugary drinks was being planned.[21]

37. In June 2017, Citizen Lab, as well as ARTICLE 19, the Red en Defensa de los Derechos Digitales (R3D) and SocialTIC published the report 'Spy Government: Systematic surveillance of journalists and human rights defenders in Mexico'[22], which accounts for multiple cases of *Pegasus* malware infection attempts.[23]

38. In total, more than 100 text messages with links that lead to Internet domains identified as part of the NSO structure have been documented. This implies that the messages analysed correspond to *Pegasus* malware infection attempts.

39. Human rights defenders, journalists, anti-corruption activists and even minors are included among the more than 20 people and organisations documented as having received messages with the aim of infecting their devices with *Pegasus* malware:

    - **Miguel Agustín Pro Juárez Human Rights centre (Centro Prodh):** Between the months of April and June 2016, three people within the organisation received messages that have been confirmed as *Pegasus* spyware infection

20 MCCI. PGR compró Pegasus a prestanombres. Julio de 2017. https://contralacorrupcion.mx/web/pgrcompropegasus/index.html

21 Perlroth, Nicole (11 de febrero de 2017) Spyware's Odd Targets: Backers of Mexico's Soda Tax. The New York Times. Available at: https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?smid=fb-share&_r=0 ; Scott-Railton, John. Marczak, Bill. Guarnieri, Claudio. Crete-Nishihata, Masashi. Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links. The Citizen Lab. Available at: https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/ ; R3D. Destapa la Vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. Available at: https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/

22 Available at: https://r3d.mx/gobiernoespia/

23 See also: Ahmed, Azam. Perlroth, Nicole. (June 19, 2017) Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families. The New York Times. Available at: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

attempts. The messages were received on key dates within the work of defending human rights that the Centre Prodh carried out around high-impact cases such as the forced disappearance of 43 students from Ayotzinapa, the Tlatlaya massacre and sexual torture cases in Atenco.

- **Aristegui News (Carmen Aristegui, Emilio Aristegui, Rafael Cabrera and Sebastián Barragán):** Messages received in 2015 and 2016 by Carmen Aristegui, by her son Emilio and by members of her research team such as Sebastián Barragán and Rafael Cabrera were documented. In recent years, the journalistic activity of Aristegui Noticias has revealed cases of corruption such as 'White House'[24] and exposed a prostitution ring[25] that operated from the offices of the Institutional Revolutionary Party (PRI) in Mexico City. It has also reported on cases of serious human rights violations in Mexico such as the forced disappearance of the 43 university students of Ayotzinapa.[26]
- It is important to point out that, at the time of receiving the messages, Emilio was a minor. This represents the first documented attack against a direct relative of a target with this malware, and more than 40 attempts against the journalist's son were recorded in total.
- **Carlos Loret de Mola (journalist):** Radio and television journalist and print columnist. His television programme 'Despierta con Loret' (formerly 'Primero Noticias') is the newscast with the largest audience in the country. It was documented that between August 2015 and April 2016, he received at least eight messages intended to infect his device with *Pegasus* malware. The first of the messages was received on the same day he published a report on extrajudicial executions in Tanhuato, Michoacán.[27]
- **Mexican Institute for Competitiveness (IMCO):** It has been documented that the director of the organisation, Juan Pardinas, and another member of the organisation, Alexandra Zapata, received messages trying to infect their devices. IMCO is one of the organisations leading advocacy efforts for anti-corruption legal reform, notably promoting the '3 of 3 Law',[28] which generated great resistance and attacks by political forces associated with the federal government.
- **Mexicans Against Corruption and Impunity (MCCI):** It has been documented that journalists Salvador Camarena and Daniel Lizárraga,

[24] Cabrera, R., D. Lizárraga, I. Huerta y S. Barragán (November 9, 2014) "La casa blanca de Enrique Peña Nieto (investigación especial)". Aristegui Noticias. Available at: http://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/

[25] "Video: Opera #RedProstitución en PRI-DF (investigación)" (April 2, 2014) Aristegui Noticias. Available at: http://aristeguinoticias.com/0204/mexico/opera-redprostitucion-en-pri-df-investigacion-mvs/

[26] "Caso Iguala: 1 mes y no aparecen los 43 estudiantes" (October 24, 2014) Aristegui Noticias. Available at: http://aristeguinoticias.com/2410/mexico/caso-iguala-1-mes-y-no-aparecen-los-43-estudiantes/

[27] Loret de Mola, C. (August 5, 2015) "Nueva ejecución extrajudicial". El Universal. Available at: http://www.eluniversal.com.mx/entrada-de-opinion/columna/carlos-loret-de-mola/nacion/2015/08/5/nueva-ejecucion-extrajudicial; (September 1, 2015) "Tanhuato: las pruebas que hacen tropezar al gobierno (I)". El Universal. Available at: http://www.eluniversal.com.mx/entrada-de-opinion/columna/carlos-loret-de-mola/nacion/2015/09/1/tanhuato-las-pruebas-que-hacen

[28] Cortés, J., Kaiser, M., Roldán, J. et al. (February 2016) Iniciativa ciudadana de Ley general de responsabilidades administrativas. Available at: http://ley3de3.mx/wp-content/uploads/2016/02/Ley3de3_LEY_IniciativaCiudadanaDeLeyGeneralDeResponsabilidadesAdministrativas_Documento.pdf

General Manager of Journalistic Research and Chief Information Officer of the organisation respectively, received at least three messages with NSO malware in 2016. Salvador Camarena and Daniel Lizárraga were also part of Aristegui Noticias in the past and participated in investigations such as the revelation of the Panama Papers. Likewise, on 30 August 2017, *Pegasus* malware attacks against the director of the organisation, Claudio X. González[29] were revealed, and other forms of intimidation by the federal government were revealed in *The New York Times*.[30]

40. In addition, Citizen Lab at the University of Toronto confirmed in a new report,[31] also published by The New York Times,[32] that on 10 July 2017, a telephone belonging to the Interdisciplinary Group of International Experts (GIEI) received text messages linked to *Pegasus* malware infrastructure; the delivery of the text messages with malicious links took place during one of the most sensitive cases for the federal government: the investigation into the enforced disappearance of 43 students (the Ayotzinapa case), confirming the federal government's constant obstruction against the group of experts that called into question the Office of the General Prosecutor's so-called 'historical truth' in the Ayotzinapa case, in addition to having been the target of a constant smear campaign to suppress their work.

41. It is important to highlight that on the dates journalists, scientists, activists and human rights defenders received the messages, they were at critical junctures of journalistic work and human rights defence in which they were confronted with a common actor: the federal government.

42. On 19 June 2017, accompanied by civil society organisations, nine of the persons targeted filed a criminal complaint regarding the facts revealed in the 'Spy Government' reports, demanding transparency about the *Pegasus* contracting processes and an independent investigation.

43. In one of the first official reactions, President Peña Nieto downplayed the violation of privacy and threatened the complainants. After admitting that the federal government had acquired the *Pegasus* malware, the president noted that 'none of the people who feel aggrieved can affirm or show or even demonstrate that their lives have been affected by this alleged tapping and by any such alleged espionage'.[33]

29 Scott-Railton, John. Marczak, Bill. Razzak, Bahr Abdul. Crete-Nishihata, Masashi. Deibert, Ron. RECKLESS V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware. The Citizen Lab. Available at: https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/

30 Ahmed, Azam. (August 30, 2017) Un empresario activista lucha contra la corrupción en México y se convierte en un blanco del Estado. The New York Times. Available at: https://www.nytimes.com/es/2017/08/30/mexico-pegasus-claudio-x-gonzalez-laporte-enrique-pena-nieto-corrupcion/

31 Scott-Railton, John. Marczak, Bill. Razzak, Bahr Abdul. Crete-Nishihata, Masashi. Deibert, Ron. RECKLESS III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware. The Citizen Lab. Available at: https://citizenlab.ca/2017/07/mexico-disappearances-nso/

32 Ahmed, Azam. (July 10, 2017) Spyware in Mexico Targeted Investigators Seeking Students. The New York Times. Available at: https://www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-pegasus-spyware.html

33 President Enrique Peña Nieto. Inauguration of the Industrial Park at Lagos de Moreno, Jalisco. Mexico. June 22, 2017; R3D. Con sus declaraciones, EPN condena al fracaso la investigación por #GobiernoEspía y amenaza a quienes han denunciado. June 22, 2017. Available at:: https://r3d.mx/2017/06/22/con-sus-declaraciones-epn-condena-al-fracaso-la-investigacion-por-gobiernoespia-y-amenaza-a-quienes-han-denunciado

44. Subsequently, President Peña Nieto concluded by issuing a threat against the complainants, stating, 'I hope that the Office of the General Prosecutor can promptly determine who is accountable, and I hope that the protection of the law can be applied against those who have raised these false accusations.'[34]

45. And yet, weeks after the publication of the 'Spy Government' report, several media outlets published contracts, technical appendices and other information related to the acquisition of usage licences for *Pegasus* by the Criminal Investigation Agency of the Office of the General Prosecutor.[35] Within the official investigation, it has been confirmed that the Office of the General Prosecutor is a user of the *Pegasus* system. However, the prosecutor in charge of the case has refused to request the contracts and technical appendices, or to undertake any investigation into the Criminal Investigation Agency.

46. In view of the President's statements and the fact that the Office of the General Prosecutor, which is in charge of the official investigation, is the main suspect, the complainants and organisations requested that a mechanism for international oversight of the investigation be accepted, so that society can have minimum guarantees of the investigation's independence, comprehensiveness and technical rigour.[36]

47. The seriousness of the alleged acts has also motivated pronouncement by international bodies. For example, four experts from the United Nations issued a statement[37] in which they emphasised the duty of the Mexican authorities to guarantee the necessary conditions for a transparent, independent and impartial investigation into the allegations of the use of the malware with the intention of spying on human rights defenders, activists and journalists.

48. Moreover, on 17 July 2017 the Nobel Prize Women's Initiative[38] called on the government of Mexico to end cyber surveillance and other systematic surveillance against journalists and activists, and to put an end to the criminalisation of activists and journalists who investigate or address human rights abuses.

49. At the end of their joint visit to Mexico, the UN and Inter-American Court of Human Rights (IACHR) Rapporteurs for Freedom of Expression conveyed their concern about the case and recommended ensuring the independence of the

[34] Idem.

[35] Aristegui Noticias. El expediente Pegasus en PGR: radiografía de un sistema de espionaje. Available at: http://aristeguinoticias.com/1207/mexico/el-expediente-pegasus-en-pgr-radiografia-de-un-sistema-de-espionaje/

[36] More specifically, the authors of this report sent a letter and a report to the Mexican government, formally supporting the adoption of the indicated mechanism. Available at: https://www.privacyinternational.org/advocacy-briefing/994/letter-and-briefing-human-rights-implications-reported-mexican-government

[37] UN. México: expertos de la ONU piden investigación independiente e imparcial sobre el uso de spyware contra defensores de DD HH y periodistas. Geneva. July 19, 2017. Available at: http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=S

[38] Menchú, Rigoberta. Williams, Betty. Ebadi, Shirin; R3D. Ganadoras del Premio Nobel piden investigación independiente e imparcial sobre el caso #GobiernoEspía. July 24, 2017. Available at: https://r3d.mx/2017/07/24/ganadoras-del-premio-nobel-piden-investigacion-independiente-e-imparcial-sobre-el-caso-gobiernoespia/

investigation into the purchase and use of malware (including *'Pegasus'*) to monitor journalists, activists and human rights defenders, as well as adopting adequate legislative measures and judicial controls so that surveillance measures are carried out in accordance with human rights, and even recommended that Mexico should consider creating an independent body to effectively oversee the State's surveillance tasks.[39]

50. In a similar vein, Michel Frost, the UN Special Rapporteur for the Protection of Human Right Defenders, issued a report after his visit to the country in 2017 in which he notes that the secret surveillance of human rights defenders is a new and worrisome challenge, especially as it lacks adequate control measures. Regarding the Mexican authorities' acquisition of *Pegasus* and its apparent use to monitor journalists and defenders, he reiterated his call, and that of other UN experts, to conduct an independent and impartial investigation into the alleged unlawful surveillance, as it constitutes a serious violation of the rights to privacy and to freedom of expression and association.[40]

E. Lack of careful investigation in the face of cases of unlawful surveillance of journalists and human rights defenders

51. Despite the seriousness of the facts, Mexico has not accepted the establishment of an international monitoring mechanism and documents related to the contracting and use of *Pegasus* malware have not even been made public by Mexican State authorities.

52. More than nine months after the announcement of the launch of the investigation by the Special Prosecutor's Office for Crimes Against Freedom of Expression (FEADLE) of the Office of the General Prosecutor, which is in charge of the investigation, no progress has been made. On the contrary, although the victims' collective representation has offered or requested at least 70 pieces of evidence, the Prosecutor's Office has refused to assent and to carry out the investigation requested by the complainants.

53. The Office of the Prosecutor has also denied a copy of the investigation file to the victims and has refused to carry out indispensable investigations, such as identifying General Prosecutor officials trained and authorised to use the *Pegasus* system; or undertaking forensic tests on equipment, servers and materials used by General Prosecutor officials who operate the *Pegasus* system; nor has it even asked the Office of the General Prosecutor for technical annexes and other information on its process for using *Pegasus*.

[39] Observaciones preliminares del Relator Especial de la ONU sobre la libertad de expresión y el Relator Especial sobre libertad de expresión de la CIDH después de su visita conjunta en México, 27 de noviembre – 4 de diciembre 2017. Available at: http://hchr.org.mx/images/doc_pub/ES-final-version-preliminary-observations.pdf

[40] Report of the Special Rapporteur on the situation of human rights defenders on his mission to Mexico, 12 February 2018, A/HRC/37/51/Add.2. Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Pages/ListReports.aspx

54. It is important to highlight that, in the file, the Criminal Investigation Agency (AIC) of the Office of the General Prosecutor has admitted that it acquired *Pegasus* usage licences and that the equipment from which the software is operated is located in its offices in Mexico City. Furthermore, in their response to the FEADLE (Special Prosecutor's Office for Crimes Against Freedom of Expression), the National Centre for Planning, Analysis and Information for Combatting Crime (CENAPI) as well as the AIC, noted that for the software's correct operation, internal security measures are listed that cover periodic and rigorous evaluation of personnel of the Office of the General Prosecutor by the Centre for Evaluation and Trust Control, as well as encryption and encoding measures. However, they immediately note that "it was not possible to identify a database or formal documentation of the record of numbers that could have been tapped".[41]

55. The alleged absence of records on the use of *Pegasus* reveals what was initially stated about the absence of controls and safeguards under which surveillance operates in Mexico; without adequate controls on use, it is practically impossible to subject such surveillance to a subsequent review to identify its correct use or, when applicable, to sanction arbitrary or unlawful use.

56. On the other hand, the Prosecutor's Office's reluctance to carry out investigative procedures concerning the Office of the General Prosecutor's AIC demonstrates the lack of autonomy, impartiality and professionalism in the investigation, especially given that both the authority conducting the investigation, the FEADLE, and the only authority that has admitted to use of the *Pegasus* malware, the AIC, are part of the same Office of the General Prosecutor.

57. As forensic experts[42] and the NSO Group, the malware manufacturer itself, have pointed out to The New York Times, a forensic analysis of the servers and equipment from which the *Pegasus* system operates should be able to find a record of the infections carried out by the system. The Office of the Prosecutor has refused to undertake any investigation into this matter.

58. In a similar vein, the investigations announced by the National Institute of Access to Information and Protection of Personal Data (INAI) and by the National Commission of Human Rights (CNDH) have not brought significant advances, in part, as has been revealed by these institutions, due to the obstruction of their proceedings by the Office of the General Prosecutor.

41 CARPETA DE INVESTIGACIÓN FED/SDHPDSC/UNAI-CDMX/0000430/2017, Oficio de respuesta de la AIC August 14, 2017 - PGR/AIC/0430/2017, Oficio de respuesta de la CENAPI August 14, 2017, PGR/AIC/CENAPI/OT/DGAAJ/10077/2017

42 Ahmed, Azam, EE. UU. y las víctimas de Pegasus desestiman la investigación de espionaje, New York Times, 20 de febrero de 2018. Disponible en: https://www.nytimes.com/es/2018/02/20/mexico-fbi-investigacion-pegasus-espionaje/?action=click&clickSource=inicio&contentPlacement=1&module=toppers&region=rank&pgtype=Homepage

RECOMMENDATIONS

59. We recommend that the Mexican State:

60. Establish an international group of experts to autonomously and independently investigate cases of unlawful surveillance of journalists and human right defenders.

61. Dutifully investigate and sanction those intellectually and materially responsible for the unlawful surveillance of journalists and human rights defenders with *Pegasus* malware.

a. The Office of the Prosecutor in charge of the official investigation must carry out all the necessary investigative procedures, such as the identification and investigation of all the Office of the General Prosecutor's Criminal Investigation Agency officers who were trained to operate the *Pegasus* system or who participated in any way in the process of selecting objectives, in the operation and in the processing of the intelligence obtained through said system. It is also essential that forensics be performed on the Criminal Investigation Agency's equipment and facilities which were used for operation of the *Pegasus* system.

b. Establish a policy of all state bodies' unrestricted cooperation with the investigations carried out by autonomous bodies such as the INAI and CNDH, as well as with the international group of experts to be established.

c. Proactively make transparent all information related to contracting processes executed between federal and state agencies and any company in order to acquire equipment or usage licences for monitoring tools and surveillance of private communications, including technical information about the acquired surveillance capacities, and withholding only specific information that could demonstrably endanger an investigation, or threaten the life or physical integrity of an individual.

d. Notify all persons who have been the target of intrusive attacks to date, including the legal basis and relevant regulation, if any, that govern such activities, or destroy all material obtained through these intrusive attacks, offering an effective means of redress to all people who have been the target of such attacks.

3. Legislate and implement the reforms necessary to ensure that the acquisition and operation of surveillance tools is carried out in a manner that is legal, necessary, proportionate and respectful of human rights.

a. The National Code of Criminal Procedures, the Federal Telecommunications Law, the Federal Police Law, the National Security Law, the Federal Law to Prevent and Sanction Abduction Crimes, the Law against Organised Crime and the Military Code of Criminal Procedures must be reformed in order to:

   - Clearly and precisely establish the vested authorities, the circumstances and the procedures for undertaking communications surveillance and accessing communication data (metadata), as well as carrying out real-time geolocation of communication equipment.
   - Explicitly establish the need to have prior and duly founded judicial authorisation to carry out surveillance, except in emergency cases in which judicial review should be immediate.
   - Grant effective powers of scrutiny and oversight of surveillance systems to an independent authority, such as the National Institute for Access to Information and Protection of Personal Data or the National Commission for Human Rights.
   - Recognise the right of every person to be notified of state interferences in their private life. Such notification may only be deferred when the notification would demonstrably and seriously hinder an investigation or endanger the life or physical integrity of a person.

b. Regulate the acquisition and operation of intrusive surveillance tools, implementing the following safeguards to guarantee that the practice of these activities is commensurate with a focus on human rights:

   - **Legality:** the powers of surveillance must be authorised by a law with clear and precise limits.
   - **Security and integrity of systems:** an evaluation of the risks and damages to the security and integrity of communications must be made before carrying out these measures.
   - **Necessity and proportionality:** factors should be established to measure the probability of occurrence of a threat against a protected public good, information about the method, the scope and duration of the proposed measure, and a safety assessment.
   - **Judicial authorisation:** an impartial and independent authority must decide whether or not to approve the measure and be empowered to oversee its application, including the possibility of consulting technical experts and experts in other areas.
   - **Integrity of information:** government authorities may not add, alter or delete data collected through tapping measures.
   - **Notification:** government authorities must notify the persons subject to surveillance of the circumstances related to the measure.

- **Destruction and return of data:** government authorities must establish a procedure to destroy data that is irrelevant to the investigation, in addition to establishing a record of this procedure.
- **Oversight and transparency:** authorities must submit their capacities and activities to an oversight body that is independent of intelligence services and the government, and must publish information related to requests.
- **Extraterritoriality:** authorities must comply with their legal obligations and refrain from using international cooperation measures to circumvent legal mechanisms.
- **Redress:** people subject to unlawful state communication surveillance must have access to an effective remedy.

4. **Repeal or refrain from passing legislation that contains provisions regarding surveillance and interference of private communications that:**

   a. Fail to precisely indicate the authorities vested with the power to carry out surveillance measures, authorities not authorised by the Constitution, or authorities vested with powers other than civil authorities.

   b. Establish mass surveillance measures.

   c. Fail to precisely and clearly establish the circumstances and procedures that must be followed to carry out surveillance.

   d. Do not contain democratic controls and accountability measures such as prior or immediate judicial review, independent oversight, transparency and the right to notification.

5. **Eliminate requirements for massive and indiscriminate retention of communications metadata provided for in Article 190, Section II of the Federal Telecommunications and Broadcasting Law.**