**Alternative report**

**Human Rights Committee**

**127th Session - Mexico**

**The right to privacy in Mexico**

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

**September 2019**

**INTRODUCTION**

1. This report is presented by Red en Defensa de los Derechos Digitales (R3D) and Privacy International (PI). 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 (article 17 of ICCPR) in Mexico, for consideration in the next review of Mexico as part of the 127th session of the Human Rights Committee (HRC).

**Right to Privacy**

1. Privacy is a fundamental right recognised in numerous international human rights instruments, including in article 17 of the International Covenant on Civil and Political Rights. The right to privacy enables the exercise of other rights such as the right to freedom of expression, freedom of association, and access to information, and it is essential for the dignity of people and the viability of democratic systems.
2. Interferences with 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.
3. 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,[[1]](#footnote-1) and such principles have been developed further by international instruments such as the European Council Convention 108, of which Mexico is a party to since October 1st, 2018[[2]](#footnote-2).

**The Right to Privacy in Mexico**

1. 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, address, papers, or possessions, except by virtue of a written order of the competent authority establishing and substantiating the legal cause for the proceeding.*

*Every person has the right to the protection of their personal data, to the access, rectification and cancellation thereof, as well as to express their opposition in the terms the law sets, which will establish circumstances of exception to the principles that rule data processing, for reasons of national security, public order, public health and safety or to protect the rights of others.‘[[3]](#footnote-3)*

1. 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.’*

1. The Federal Law for the Protection of Personal Data in Possession of Bound Entities[[4]](#footnote-4) and the Federal Law for the Protection of Personal Data in Possession of Individuals[[5]](#footnote-5) regulate the processing of personal data in Mexico.
2. 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.

**ISSUES OF CONCERN**

**A. Inadequate regulation of communications surveillance in Mexico:**

1. 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, amended in 2014, the National Code of Criminal Proceedings, adopted in 2014 and amended in 2016, as well as other laws that have been issued and reformed to establish surveillance measures such as the following:

***1. Massive and indiscriminate retention of communications data***

1. 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.
2. 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.
3. 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.[[6]](#footnote-6) 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”[[7]](#footnote-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”.[[8]](#footnote-8)
4. Notwithstanding, after a challenge of the constitutionality of the data retention mandate brought by R3D, the Supreme Court decided to validate the provision without even considering it as an interference with the right to privacy[[9]](#footnote-9). However, data retention is currently being challenged before the Inter-American Commission on Human Rights[[10]](#footnote-10).

***2. Access to communications data and geolocation in real time***

1. 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, which has created legal uncertainty and, in practice, has been taken advantage by authorities without legal standing that have claimed to be a “competent authority”..
2. Nor is the need for judicial authorisation to carry out these privacy invasion measures explicitly established in some provisions. 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[[11]](#footnote-11), 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***

1. Mexican legislation does not provide adequate and sufficient safeguards against the abuse of secret communication 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.

1. Furthermore, although legislation provides some requirements for proactive transparency regarding surveillance[[12]](#footnote-12) measures such as publishing statistics on the use of surveillance, in practice these have not been implemented fully by any federal or local agency and the authorities and judiciary routinely deny access to these statistics, even in redacted versions, which prevents public scrutiny of these activities[[13]](#footnote-13).

**B. Unlawful and unchecked surveillance in Mexico**

1. 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,’[[14]](#footnote-14) Red en Defensa de los Derechos Digitales (R3D) documents various inconsistencies and illegalities.
2. 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, even though article 16 of the Constitution requires it.



1. Similarly, as shown in the figure above, 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.[[15]](#footnote-15)
2. Conversely, as apparent in the following figure, it has been documented that in 98.91% of instances where an authority accessed data of telecommunications users retained by service providers, between 2013 and 2015, the authority has done so without judicial authorisation, even though, as the Supreme Court of Mexico clarified, it is required[[16]](#footnote-16). The same has happened in cases of real-time geolocation.[[17]](#footnote-17)



1. 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.
2. 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.[[18]](#footnote-18)
3. 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.[[19]](#footnote-19) 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.

**C. Irregular acquisition and operation of surveillance malware in Mexico**

1. 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.
2. 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 government hacking.
3. 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.[[20]](#footnote-20)
4. Out of a total of 35 countries, including Brazil, Chile, Colombia, Ecuador, Honduras and Panama, Mexico proved to be the firm’s main client[[21]](#footnote-21), with transactions made by different local governments, units and federal agencies via various intermediary companies.
5. Among the Mexican 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.
6. In August 2016, Citizen Lab[[22]](#footnote-22), 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.
7. 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.
8. There is evidence that Mexican authorities such as the Secretariat of National Defense (SEDENA), the Office of the General Prosecutor (PGR) and the Centre 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.[[23]](#footnote-23)
9. There is also evidence that in 2018, the General Prosecutor’s Office acquired a surveillance malware from the company Neolinx, for the amount of USD $ 4,564,252, that allowed it to, amongst others, intervene and gain access to the geographical location of the devices it was deployed on. It was documented that the Office (illegally) used this powerful tool to spy on political adversaries and candidates.[[24]](#footnote-24)

**D. Surveillance against journalists and human rights defenders in Mexico**

1. Several cases have been documented in which surveillance, and in particular surveillance malware tools, has been used against activists, journalists and human rights defenders.
2. In February 2017, it was reported 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 combating 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.[[25]](#footnote-25)
3. 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’[[26]](#footnote-26), which accounts for multiple cases of Pegasus malware infection attempts.[[27]](#footnote-27)
4. 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.
5. Human rights defenders, journalists, anti-corruption activists and even children 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, including:
* **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 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’[[28]](#footnote-28) and exposed a prostitution ring[[29]](#footnote-29) 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[[30]](#footnote-30). 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[[31]](#footnote-31).
* **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’[[32]](#footnote-32), 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, 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[[33]](#footnote-33) were revealed, and other forms of intimidation by the federal government were revealed in The New York Times.[[34]](#footnote-34)
* ***Ríodoce* weekly:** Javier Valdez Cárdenas, the founder of *Ríodoce*, a Mexican newspaper known for investigating cartels was murdered near his office in May 2017. It has been documented that two days after the killing, *Ríodoce’*s director, Ismael Bojórquez, and a close colleague to Javier, Andrés Villarreal, began receiving infection attempts with NSO Group’s Pegasus spyware, which purported to provide information about Valdez killing. According to them, immediately prior to the initial targeting on May 17th, representatives from the Criminal Investigation Agency (Agencia de Investigación Criminal), which is part of the Mexican Office of the Attorney General (Procurador General de la República (PGR)), were assigned to the investigation of the killing of Javier Valdéz[[35]](#footnote-35).
* **Griselda Triana:** it has been documented that Griselda, also a journalist and partner of murdered journalist Javier Valdez, was likewise targeted with NSO Group’s Pegasus spyware following his assassination as well as the infection attempts against Andrés Villarreal and Ismael Bojórquez[[36]](#footnote-36). It is important to mention that the infection attempts against Riodoce’s journalist and Ms. Triana happened months after the first reports of malware attacks against civil society in Mexico were already been published and were even featured in the New York Times.
1. In addition, Citizen Lab at the University of Toronto confirmed in a new report,[[37]](#footnote-37) also published by The New York Times,[[38]](#footnote-38) that on 10 July 2017, a telephone belonging to the **Interdisciplinary Group of Independent Experts (GIEI)[[39]](#footnote-39)** 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.
2. 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.
3. On 19 June 2017, accompanied by civil society organisations, nine of the persons targeted filed a criminal complaint regarding the facts revealed in the ‘Gobierno Espía’ report, demanding transparency about the Pegasus acquisition processes and an independent investigation.
4. 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’.[[40]](#footnote-40)
5. 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.’[[41]](#footnote-41)
6. And yet, weeks after the publication of the ‘Gobierno Espía’ 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.[[42]](#footnote-42) 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 relevant investigation into the Criminal Investigation Agency.
7. 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.[[43]](#footnote-43)
8. The seriousness of the alleged acts has also motivated statements by international human rights expert bodies. For example, four experts from the United Nations issued a statement[[44]](#footnote-44) 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.
9. Moreover, on 17 July 2017 the Nobel Prize Women’s Initiative[[45]](#footnote-45) 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.
10. 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.[[46]](#footnote-46)
11. Likewise, the UN and Inter-American Court of Human Rights (IACHR) Rapporteurs for Freedom of Expression, David Kaye and Edison Lanza, in their joint report presented in June 2018 on their mission to Mexico conveyed their concern about the case and made two recommendations to Mexico[[47]](#footnote-47):

*(a)* ***Conduct an independent investigation*** *into the purchase and use of malware (including “Pegasus”) to monitor journalists, activists, and human rights defenders. Such an investigation should be conducted independent of the federal and state governments alleged to have purchased or used the spyware and include experts from academic and civil society organizations, including potentially from outside of Mexico. In the meantime, any ongoing investigation must respect the rights of targets of surveillance, including their security and privacy;*

*(b)* ***Establish a legal framework to protect people from arbitrary and/or clandestine interferences in their privacy****, including the protection of journalistic sources according to international standards on the matter. Guarantees and judicial oversight of state agencies engaging in surveillance should be established, within the permissible limitations of a democratic society. Mexico should consider creating an independent body to effectively oversee the State’s surveillance tasks.*

1. Notwithstanding, these recommendations have not been implemented to date. In his most recent report presented to the UN Human Rights Council in May 2019 on the surveillance industry and its impact on human rights, David Kaye expressed that despite their urge to the Mexican Government to allow an independent investigation of this case, along with the orders of INAI to reveal the nature of its contracts to obtain Pegasus, as “to date, the efforts to investigate the allegations have not clarified the situation”[[48]](#footnote-48).
2. As R3D and Privacy International have previously recommended to Mexico[[49]](#footnote-49), the Mexican government hacking, including the use of NSO Group spyware, raises grave human rights concerns and calls into question whether Mexico is meeting its obligations under international human rights law therefore it should immediately cease all hacking activities.

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

1. Despite the seriousness of the reports, 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.
2. More than two years 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 most of the investigative procedures requested by the complainants.
3. Hence, the complainants had to recur to the judicial system, obtaining two favorable decisions[[50]](#footnote-50) from two different federal judges, ordering the Prosecutor’s Office not to place the burden of proof on the victims and to respect their rights, amongst others, demonstrating the deficiencies on the investigation the prosecution has been conducting. For instance, they have denied a copy of the investigation file to the victims and refused to carry out indispensable investigations, such as identifying General Prosecutor officials trained and authorised to use the Pegasus system; or undertaking independent forensic tests on equipment, servers and materials used by General Prosecutor officials who operate the Pegasus system.
4. It is important to highlight that 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[[51]](#footnote-51). 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 Combating 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, these authorities claim that there is not a database or formal documentation that records the persons or numbers that were targeted.
5. 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.
6. 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.
7. As forensic experts and the NSO Group, the malware manufacturer itself, have pointed out to The New York Times, a proper, objective and impartial 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 serious and independent investigation into this matter.
8. Moreover, the investigation announced by the National Commission of Human Rights (CNDH) has not brought significant advances, in part, as it has been informally noted to R3D by this institution, due to the obstruction of their proceedings by the Office of the General Prosecutor.
9. Notably, however, on February 20th, 2019, the National Institute of Access to Information and Protection of Personal Data (INAI) issued its decision on the investigation it initiated on November 2018 against the Prosecution’s Office, determining that the Office had breached its obligations per the Personal Data Protection legislation[[52]](#footnote-52). Furthermore, it concluded that given the inconsistencies derived from the information disclosed to INAI by the Office (for example, first they informed they only had one contract for the acquisition of Pegasus, stating it expired in 2014 but later on, a couple of days prior to INAI’s decision, they informed they actually had two more contracts, valid for the execution of Pegasus during 2016 and 2017) it would also present a criminal complaint and recur to the oversight body of the Prosecutor’s Office so they investigate and sanction the possible commission of crimes against the administration of justice and improper practice of public service. To date no charges have been presented regarding the obstruction of justice that has been documented.

**RECOMMENDATIONS**

1. In light of the above consideration, we encourage the Human Rights Committee to include in its concluding observations the following recommendations to Mexico:
2. **Immediately cease any acts of surveillance conducted by means of hacking to electronic devices through intrusive software, and launch a thorough assessment based on international human rights law to establish if hacking- based surveillance powers are compatible Article 17 of the Covenant and in particular with the principles of legality, necessity and proportionality as interpreted by the Committee.**
3. **Establish an international group of experts to autonomously and independently investigate reported cases of unlawful surveillance of journalists and human rights defenders.**
4. **Dutifully investigate and sanction those intellectually and materially responsible for the reported unlawful surveillance of journalists and human rights defenders with Pegasus malware.**
	1. 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.
	2. 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.
	3. 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.
	4. 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.
5. **Legislate and implement the reforms necessary to ensure that the acquisition and operation of surveillance tools is carried out in a transparent manner that is legal, necessary, proportionate and respectful of human rights.**
	1. The National Code of Criminal Procedures, the Federal Telecommunications and Broadcasting Law, the Federal Police Law, the National Guard Law, the National Security Law, the Federal Law to Prevent and Sanction Kidnapping Crimes, the Law against Organised Crime, the Military Justice Code and the Military Code of Criminal Procedures and others pertinent, 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.

* 1. 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.

1. **Repeal existing legislation and refrain from passing legislation that contains provisions regarding surveillance and interference of private communications that:**
	1. 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.
	2. Establish mass surveillance measures which are inherently contrary to human right standards and obligations.
	3. Fail to precisely and clearly establish the circumstances and procedures that must be followed to carry out surveillance.
	4. Do not contain democratic controls and accountability measures such as prior or immediate judicial review, independent oversight, transparency and the right to notification.
2. **Eliminate requirements for massive and indiscriminate retention of communications metadata provided for in Article 190, Section II of the Federal Telecommunications and Broadcasting Law.**
1. Universal Declaration of Human Rights Article 12, UN Convention on Migrant Workers and their families, Article 14, UN Convention on the Rights of Children, Article 16, International Covenant for Civil and Political Rights, Article 17. [↑](#footnote-ref-1)
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108). [↑](#footnote-ref-2)
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](https://ssrn.com/abstract%3D1951416) [↑](#footnote-ref-3)
4. Available at <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.p> [↑](#footnote-ref-4)
5. Available at <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf> [↑](#footnote-ref-5)
6. 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=> [↑](#footnote-ref-6)
7. UN. Resolution adopted by the Human Rights Council on 23 March 2017 regarding the Right to privacy in the digital age., UN doc. A/HRC/RES/34/7. [↑](#footnote-ref-7)
8. Human Rights Committee., Concluding observations to the 4th periodic report by the United States of America, April 21, 2015, U.N. Doc. CCPR/C/USA/CO/4, para. 22. [↑](#footnote-ref-8)
9. SCJN. Amparo en Revisión 964/2015. Decision of May 4, 2016. [↑](#footnote-ref-9)
10. IACHR. Petition P-273-17. [↑](#footnote-ref-10)
11. See for example: Open Society Justice Initiative, Undeniable atrocities: Confronting crimes against humanity in Mexico, 2016, available at: <https://www.justiceinitiative.org/uploads/7dc9f3b9-21dc-4d14-90fd-aaa29ff12cc3/undenialble-atrocities-2nd-edition-20160808.pdf> [↑](#footnote-ref-11)
12. See for example, article 70, fraction XLVII of the General Law on Transparency and Access to Public Information. Available at: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf> [↑](#footnote-ref-12)
13. See R3D, Transparencia y Vigilancia en México, 2018. Available at: <https://r3d.mx/wp-content/uploads/r3d-transparenciayvigilancia.pdf> [↑](#footnote-ref-13)
14. R3D. Estado de la Vigilancia: Fuera de Control. 2016. Pg. 45. Available at: <https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf> [↑](#footnote-ref-14)
15. Idem. [↑](#footnote-ref-15)
16. SCJN. Amparo en Revisión 964/2015. Decision of May 4, 2016. [↑](#footnote-ref-16)
17. R3D. Estado de la Vigilancia: Fuera de Control. 2016. Pg. 56. [↑](#footnote-ref-17)
18. Data obtained from the reports issued by telecommunications companies 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](https://drive.google.com/drive/) [↑](#footnote-ref-18)
19. R3D. “Estado de la Vigilancia: Fuera de Control”. 2016. Pages 71-74 [↑](#footnote-ref-19)
20. Privacy International (06 July 2015) Surveillance company Hacking Team exposed. Available at: <https://www.privacyinternational.org/node/618> [↑](#footnote-ref-20)
21. Angel, A. (07 July 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-hackersexhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/> [↑](#footnote-ref-21)
22. Citizen Lab (2016) About Citizen Lab. Available at: <https://citizenlab.org/about/> [↑](#footnote-ref-22)
23. MCCI. (July 2017) PGR compró Pegasus a prestanombres. [https://contralacorrupcion.mx/web/ pgrcompropegasus/index.html](https://contralacorrupcion.mx/web/) [↑](#footnote-ref-23)
24. R3D: Red en Defensa de los Derechos Digitales. “PGR adquirió equipo para geolocalizar 255 mil celulares en 2018; se usó “para espiar a todos los candidatos: Reporte Índigo”. June 5, 2019, available at: <https://r3d.mx/2019/06/05/pgr-equipo-espionaje-celulares-geomatrix/> [↑](#footnote-ref-24)
25. 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-conmalware-gubernamental/> [↑](#footnote-ref-25)
26. Available at: <https://r3d.mx/gobiernoespia/> [↑](#footnote-ref-26)
27. 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> [↑](#footnote-ref-27)
28. 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/](http://aristeguinoticias.com/0911/)  [↑](#footnote-ref-28)
29. “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/> [↑](#footnote-ref-29)
30. “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/> [↑](#footnote-ref-30)
31. 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-ejecucionextrajudicial](http://www.eluniversal.com.mx/entrada-de-opinion/columna/carlos-loret-de-mola/nacion/2015/08/5/nueva-ejecucionextrajudicial) ; (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](http://www.eluniversal.com.mx/entrada-de-opinion/columna/carlos-loret-de-mola/)  [↑](#footnote-ref-31)
32. 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](http://ley3de3.mx/wp-content/uploads/2016/02/Ley3de3_) [↑](#footnote-ref-32)
33. 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/> [↑](#footnote-ref-33)
34. 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/](https://www.nytimes.com/) [↑](#footnote-ref-34)
35. Scott-Railton, John. Marczak, Bill. Razzak, Bahr Abdul. Crete-Nishihata, Masashi. Deibert, Ron. (November 27, 2018) RECKLESS VI. Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague. The Citizen Lab. Available at:<https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/> [↑](#footnote-ref-35)
36. Scott-Railton, John. Marczak, Bill. Razzak, Bahr Abdul. Crete-Nishihata, Masashi. Deibert, Ron. (March 20, 2019) RECKLESS VIII. Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group’s Spyware. The Citizen Lab. Available at: <https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/> [↑](#footnote-ref-36)
37. 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/> [↑](#footnote-ref-37)
38. 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> [↑](#footnote-ref-38)
39. The Interdisciplinary Group of Independent Experts (GIEI, by its initials in Spanish) was created in November 2014 through an agreement between the IACHR, the Mexican State, and representatives of the disappeared students in Ayotzinapa. This agreement also established the main activities to be carried out by the GIEI: to draw up plans for searching for the disappeared persons alive; technical analysis of the lines of investigation to determine criminal liabilities; and technical analysis of the Plan for Integral Attention to the Victims (Plan de Atención Integral a las Víctimas) of the events of September 26 and 27, 2014. [↑](#footnote-ref-39)
40. 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-susdeclaraciones-epn-condena-al-fracaso-la-investigacion-por-gobiernoespia-y-amenaza-a-quienes-han-denunciad> [↑](#footnote-ref-40)
41. Idem. [↑](#footnote-ref-41)
42. 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/> [↑](#footnote-ref-42)
43. 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-reportedmexican-governmen](https://www.)t [↑](#footnote-ref-43)
44. 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](http://www.ohchr.org/SP/) [↑](#footnote-ref-44)
45. 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-casogobiernoespia/> [↑](#footnote-ref-45)
46. 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](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/) [↑](#footnote-ref-46)
47. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Mexico, 12 June 2018, A/HRC/38/35/Add.2, Available at: <https://www.oas.org/en/iachr/expression/docs/2018_06_18_CIDH-UN_FINAL_MX_report_ENG.pdf> [↑](#footnote-ref-47)
48. Surveillance and Human Rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 28 May 2019, A/HRC/41/35 (para 27) available at: <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session41/Documents/A_HRC_41_35.docx> [↑](#footnote-ref-48)
49. PI - R3D. Briefing on the International [↑](#footnote-ref-49)
50. R3D: Red en Defensa de los Derechos Digitales, “Juez federal ordena a la PGR admitir pruebas de víctimas en la investigación sobre #GobiernoEspía”, 28 May 2018, available at: <https://r3d.mx/2018/05/28/juez-federal-ordena-a-la-pgr-admitir-pruebas-de-victimas-en-la-investigacion-sobre-gobiernoespia/> [↑](#footnote-ref-50)
51. INAI. Decision regarding the verification process INAI.32.07.01-007/2018. Available at: <http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf> [↑](#footnote-ref-51)
52. INAI, “Determina INAI que FGR, respecto al software Pegasus, incumplió la Ley General de Protección de Datos en Posesión de Sujetos Obligados”, February 20th, 2019: <http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf> [↑](#footnote-ref-52)