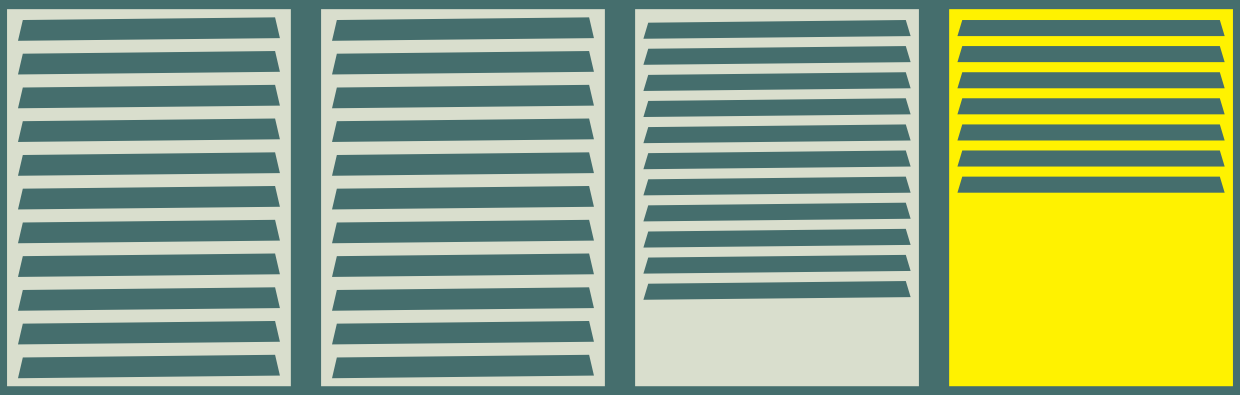

THE RIGHT TO PRIVACY IN MEXICO

STAKEHOLDER SUBMISSION

UNIVERSAL PERIODIC REVIEW

45TH SESSION - MEXICO

STAKEHOLDER SUBMISSION
UNIVERSAL PERIODIC REVIEW
45TH SESSION - MEXICO

THE RIGHT TO PRIVACY IN MEXICO

PRESENTED BY RED EN DEFENSA DE LOS DERECHOS DIGITALES (R3D) AND PRIVACY INTERNATIONAL (PI)

JULY 2023

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 that researches and advocates globally against government and corporate abuses of data and technology.

2. PI and R3D wish to raise concerns regarding the right to privacy (article 17 of ICCPR) in Mexico, for consideration in the next review of Mexico as part of the 45th session of the Universal Periodic Review (UPR).

RIGHT TO PRIVACY

3. 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.

4. 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.

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, and such principles have been developed further by international instruments such as the Council of Europe Convention 108+, of which Mexico is a party to since October 1st, 2018.

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, 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.'*

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 and the Federal Law for the Protection of Personal Data in Possession of Individuals 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.and others pertinent, must be reformed.

ISSUES OF CONCERN

A. INADEQUATE REGULATION OF SURVEILLANCE AND LACK OF SAFEGUARDS

10. The Mexican legal framework establishes various surveillance powers carried out by different authorities, including the interception of private communications, as well as massive and indiscriminate retention of communications data and real-time geolocation, without including adequate safeguards.

11. The National Security Law, the National Guard Law and the National Code of Criminal Proceedings authorise the National Intelligence Center (CNI), the National Guard (GN), the Federal Prosecutor Office (FGR) and the local prosecutor offices, respectively, to carry out different forms of electronic surveillance. However, these laws do not offer sufficient clarity and safeguards to prevent abuses.

12. For example, the National Guard Law establishes the use of "preventive intelligence" and "investigation" services through covert surveillance measures, such as access to stored data, interception of communications, geo-referencing of mobile communication equipment, as well as surveillance, identification, monitoring and tracking on the public Internet network. These surveillance measures violate the principle of legality by not establishing in a clear, precise or detailed manner the nature, scope, procedures and circumstances under which the National Guard will use these investigative and intelligence techniques for the claimed purpose of preventing crime.

13. Surveillance activities pose an inherent risk to human rights, both because of the intensity with which they interfere with rights such as privacy and because such interferences are not usually known by the persons whose rights are interfered with. This increases the risks of abuse, makes detection difficult and fosters impunity.

14. Judicial oversight has been often eluded or insufficient to prevent abuse. For example, between 2016 and 2019, about 60 percent of the requests for access to retained data were made without judicial oversight. This percentage includes both the requests made without judicial authorization and the requests made through emergency mechanisms. About 75 percent of requests without prior

judicial authorization were made through emergency mechanisms, and around 50 percent of these requests were not ratified or were only partially ratified.[1]

B. IRREGULAR ACQUISITION OF SURVEILLANCE TECHNOLOGIES

15. Several irregularities have been found in the acquisition and use of surveillance technologies.[2] The opacity and absence of adequate regulation and controls regarding the procurement and contracting processes of surveillance equipment and systems for the interception of private communications has encouraged corruption, hindered accountability and promoted impunity for the abuse of such systems.

16. In several jurisdictions, an authorization or licence is required for the commercialization of equipment or systems for the interception of private communications, similar to the requirements for the commercialization of weapons. In Mexico, however, these procurement processes do not require a special procedure or authorization, and usually only involve the contracting authority and companies, without the intervention of any other agency. This encourages contracting by authorities without powers and discretion in the awarding of contracts, as well as in the setting of amounts and conditions.

17. Additionally, the acquisition of systems designed to circumvent accountability, i.e. systems that leave no traces or records of their operation, hinder future investigations into allegations of abuse of such systems, as in the case of the *Pegasus* malware.

18. Pegasus is a spyware created by NSO Group, an Israeli company, which, once successfully implanted on a phone, can actively record or passively gather a variety of different data about the device. According to The Citizen Lab – an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto – by giving full access to the phone's files, messages, microphone and video camera, the operator can turn the device into a silent digital spy in the

1. Information obtained through access to information requests between 2017 and 2020 to local and federal authorities with powers to carry surveillance activities. E.g. Fiscalía General del Estado de Tabasco, request number 611218; Fiscalía General del Estado de Yucatán, request number 256421; Fiscalía General del Estado de San Luis Potosí, request number 711521.

2. Rubí, Mauricio, "La PGR compró Pegasus a un fantasma", Mexicanos contra la Corrupción y la Impunidad, available at: https://contralacorrupcion.mx/la-pgr-compro-pegasus-a-un-fantasma/

target's pocket. The infected device, then, transmits collected information back to a Pegasus Data Server at the operator's premises.[3]

19. Since surveillance abuse cases have been made public, transparency has also been demanded, in a public version, of all the contracts for the acquisition of surveillance technologies by Mexican authorities.[4] However, information related to the contracting processes is frequently reserved or considered confidential, violating the right to access to information.

20. There is a lack of transparency of the records that would allow a supervisory body, or the public, to know how many contracts of this type exist, which authorities and companies are involved, what are the amounts disbursed and the general purpose of such contracts. The knowledge, for example, of technical information such as the general capacities of the equipment and systems is fundamental for the public to know the invasive capacities of the State, as well as to evaluate and supervise the pertinence of the operation of such tools.

21. Transparency regarding the officials involved in the procurement processes is also particularly relevant considering the reports of surveillance activities by authorities without the legal competences to use them. For example, among the Mexican authorities that have used the malware commercialised by the Italian company Hacking Team, were the Governments of Baja California, Campeche, Chihuahua, Durango, Guerrero, Jalisco, Nayarit, Puebla, Querétaro and Yucatán; the Ministry of Public Security of Tamaulipas; and federal agencies such as the Ministry of National Defense, and even Petróleos Mexicanos (PEMEX).[5] These authorities do not have legal powers to conduct surveillance of private communications, so both the acquisition and use of such technologies were clearly unlawful.

22. Another relevant consequence of the lack of transparency and accountability of the procurement of surveillance tools has been the corruption associated with the purchase of malware. For

3. Marczak B. & John Scott-Railton, Report: "The Million Dollar Dissident, NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", The Citizen Lab, August 24, 2016 https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

4. R3D: Red en Defensa de los Derechos Digitales, "SEDENA debe entregar toda la información sobre contratos con proveedora de Pegasus", January 2023, available at: https://r3d.mx/2023/01/26/sedena-debe-entregar-toda-la-informacion-sobre-contratos-con-proveedora-de-pegasus/; Zerega, Georgina, "El Instituto de Transparencia obliga al Ejército a publicar los contratos por el 'sotfware' espía Pegasus", El País, January 2023, available at: https://elpais.com/mexico/2023-01-26/el-instituto-de-transparencia-obliga-al-ejercito-a-publicar-los-contratos-por-el-sotfware-espia-pegasus.html; Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Informative Note: INAI/010/23, January 2023, available at: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Nota%20INAI-010-23.pdf

5. *See*, R3D: Red en Defensa de los Derechos Digitales, *El Estado de la vigilancia. Fuera de control*, November 2016,p. 89, available at: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

example, *Aristegui Noticias*[6] has revealed a network of intermediaries that created a parallel structure through private actors to commercialise and participate in the operation of *Pegasus* on instructions from high-level Mexican authorities. The problem is exacerbated with the added factor that manufacturers or final service providers have argued alleged legal or contractual impediments to cooperate with investigations related to abuses committed with the equipment and systems they market.[7]

23. Consequently, despite the fact that the Constitution and international human rights treaties impose limits on the authorities regarding admissible interference in the right to privacy, there is no mechanism capable of detecting and preventing the acquisition of equipment and systems that exceed these limits or facilitate the circumvention of accountability mechanisms.

24. In summary, the above examples demonstrate that there is no mechanism capable of detecting and preventing the acquisition of equipment and systems that exceed these limits or facilitate the circumvention of accountability mechanisms, in violation of the Constitution and the International Covenant on Civil and Political Rights that impose limits on the authorities regarding admissible interference in the right to privacy,

6. Aristegui, Carmen, *et. al.*, "Pegasus Project: la red de empresas que vendió Pegasus al gobierno de Peña Nieto", Aristegui Noticias, July 21, 2021, available at: https://aristeguinoticias.com/2107/mexico/pegasus-project-la-red-de-empresas-que-vendio-pegasus-al-gobierno-de-pena-nieto/

7. FEADLE investigation file (carpeta de investigación) FED/SDHPDSC/UNAI-CDMX/0000430/2017; Amnesty International, "Novalpina Capital's reply to NGO coalition letter (15 April 2019) and Citizen Lab letter (06 March 2019)", May 15, 2019, available at: https://www.amnesty.org/en/documents/doc10/0436/2019/en/

C. ABUSIVE SURVEILLANCE OF HUMAN RIGHTS DEFENDERS AND JOURNALISTS

a. Malware abuse during the previous administration.

25. In 2016, research done by Citizen Lab[8] found that most of the domain names that NSO Group's infrastructure used to target devices with *Pegasus* were linked to Mexico, leading researchers and organisations to presume that Mexican authorities were NSO clients, and that people in Mexico could have been targets of surveillance.

26. The suspicions were confirmed in 2017 by Mexican civil society organisations through investigations such as "Gobierno Espía",[9] along with reports from Citizen Lab.[10] Human rights defenders, journalists, anti-corruption activists and even children were included among the more than 20 people and organisations documented as having received messages with the aim of compromising the confidentiality and security of their devices with *Pegasus* malware. So far, more than 25 surveillance cases against journalists and human rights defenders in Mexico have been documented.[11]

27. Civil society organisations also documented that Mexican authorities, such as SEDENA, the (then) Center for Investigation and National Security (CISEN) and the (then) Attorney General's Office (PGR), through the Criminal Investigation Agency (AIC), had purchased this software. However, these authorities have claimed no database or formal documentation of the records regarding the persons or numbers targeted exist.[12]

28. The alleged absence of records on the use of *Pegasus* in Mexico reveals what was initially stated in this submission about the absence of controls and safeguards under which surveillance operates in Mexico; without adequate controls on its use, including but not limited to prior judicial

8. Marczak B., Report: "The Million Dollar Dissident, NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", *op. cit.* 3.

9. Article 19, R3D: Red en Defensa de los Derechos Digitales, Social Tic, *Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México*, June 2017, https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf

10. Scott-Railton, J., *et al.*, Report: "Bitter Sweet Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links", The Citizen Lab, February 11, 2017, available at: https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/

11. Scott-Railton, J., *et al.*, Report: "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware", The Citizen Lab, March 20, 2019, available at: https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/

12. FEADLE investigation file (carpeta de investigación) FED/SDHPDSC/UNAI-CDMX/0000430/2017.

authorisation and effective oversight, it is practically impossible to subject such surveillance to a subsequent review to identify when it is lawfully used or, when applicable, to sanction arbitrary or unlawful use.

b. Malware abuse during the current administration.

29. Despite the change of government and the repeated declarations by the current President that surveillance on journalists and human rights defenders would no longer occur, and that Pegasus malware or any other similar private communications interception system would no longer be operated, unlawful surveillance prevails in Mexico. Recently, the investigation "*Ejército Espía*", carried out by media and civil society organisations, revealed new cases of Pegasus surveillance attributable with a high degree of certainty to the Mexican Army.[13]

30. This investigation highlights a leaked internal Sedena document, addressed to the Secretary of National Defense,[14] obtained by Colectivo Guacamaya, which demonstrates the conclusion of a contract between the SEDENA and the company Comercializadora Antsua[15] — the company designated with the exclusive rights for the sale of *Pegasus* — in April 2019, whose objective was the acquisition of a "Remote Information Monitoring Service". It is important to highlight that under Mexican law SEDENA does not have legal authorization to intercept private communications.

31. Up to now, according to civil society organisations, The Citizen Lab and media organisations, the documented victims are the Under-Secretary for Human Rights, Alejandro Encinas,[16] the Coordinator of the Truth Commission for the "Dirty War" —the period of enforced disappearances, torture and executions committed by Mexican security forces, including the army, from

13. R3D: Red en Defensa de los Derechos Digitales, Article 19, Social Tic, *et. al.*, *Ejército Espía*, available at: https://ejercitoespia.r3d.mx/

14. R3D: Red en Defensa de los Derechos Digitales, "Ejército Espía, available at: https://ejercitoespia.r3d.mx/wp-content/uploads/2022/10/Mortal-de-Oficio.png

15. Evidence has been published that a person who serves as legal representative of Comercializadora Antsua, served as commissioner and member of the supervisory body of *Proyectos y Diseños VME S.A. de C.V.*, a company used during the Peña Nieto administration to market Pegasus licenses.

16. Kitroeff, Natalie & R. Bergman, "Mexican President Said He Told Ally Not to Worry About Being Spied On", The New York Times, May 23, 2023, available at: https://www.nytimes.com/2023/05/23/world/americas/mexico-president-spying-pegasus.html

the 1960s to the 1980s—, Camilo Vicente Ovalle,[17] a human rights organisation, Miguel Agustín Pro Juárez Human Rights centre (Centro Prodh), human rights defender Raymundo Ramos, and two journalists, one of them Ricardo Raphael de la Madrid.[18] The Pegasus infections occurred at times when the victims were carrying out work related to human rights violations committed by the Armed Forces.

32. For example, Under-Secretary Encinas is in charge of the truth commission for the disappearance of 43 students from Ayotzinapa, in which army personnel participated. Centro Prodh represents the families of the victims in this case and represents many other victims of human rights violations by the military. Centro Prodh had also been previously found to be targeted with Pegasus in the previous government from April to June 2016.[19] Also, the journalists were attacked when they were publishing information related to human rights abuses committed by the military.

33. The investigation also published information showing that the Secretary of National Defense, as well as other high military commanders, reviewed an information card that reports the illegal surveillance on Raymundo Ramos done with *Pegasus* by SEDENA, including his conversations with journalists on dates in which Citizen Lab confirmed his phone was infected with *Pegasus*.[20] During those dates, a video that showed an extrajudicial execution by the Army in Nuevo Laredo, Tamaulipas, was published. Raymundo Ramos was assisting the families of the victims at that time.

34. In addition, documents obtained and leaked by hacktivist collective Guacamaya[21] to several civil society and media organisation including R3D, revealed the military structure behind the use of

17. Lopez, Oscar & M. Sheridan, "He's leading Mexico's probe of the Dirty War. Who's spying on him?". The Washington Post, June 3, 2023, available at: https://www.washingtonpost.com/world/2023/06/03/mexico-pegasus-dirty-war-lopez-obrador/

18. *See*, R3D: Red en Defensa de los Derechos Digitales, "Ejército Espía", available at: https://ejercitoespia.r3d.mx/

19. Scott-Railton, J., *et al.*, Report: "Reckless Exploit, Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware", The Citizen Lab, June 19, 2017, available at: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

20. *See*, R3D: Red en Defensa de los Derechos Digitales, "Ejército Espía", available at: https://ejercitoespia.r3d.mx/wp-content/uploads/2022/10/Mortal-de-Oficio.png. It highlights the publication of a secret information card, prepared on September 2, 2020 under the name "Activities Raymundo Ramos" (available at: https://r3d.mx/wp-content/uploads/Tarjeta-Informativa-Raymundo-Ramos-Testada-scaled.jpg), which gives an account of the conversations that the human rights defender had with journalists, between August 16 and August 26, 2020; i.e, exactly during the dates on which the forensic analysis of Citizen Lab concluded that Raymundo Ramos' phone was infected with Pegasus. The aforementioned information card was prepared by the C.M.I.

21. Abi- Habib, María, "Mexico Military Is Hacked, Exposing Abuse and Efforts to Evade Oversight", The New York Times, October 6, 2022, available at: https://www.nytimes.com/2022/10/06/world/americas/mexico-hack-government-military.html

Pegasus: the Military Intelligence Center (C.M.I.).[22] C.M.I. is an agency that was part of the Sub-Chief of Intelligence of the National Defense General Staff, the operational arm of the Secretary of National Defense. In another document, the C.M.I. is mentioned as the final user of the "Remote Information Monitoring System" acquired by SEDENA through Comercializadora Antsua.

D. IMPUNITY FOR SURVEILLANCE ABUSE

35.In 2017, 2022 and 2023, surveilled victims, mainly human rights defenders and journalists, filed criminal complaints with the Special Prosecutor's Office for Crimes against Freedom of Expression (FEADLE) for, among others, the crimes of illegal interception of private communications and illegal access to computer systems. The fact that one of the victims, Centro Prodh, has been subject to surveillance with Pegasus under two different administrations, and filed two different criminal complaints, shows how impunity and the lack of adequate measures led to the repetition of illegal surveillance.

36.Despite multiple calls by national and international actors — such as the Office of the UN Human Rights Office of the High Commissioner (OHCHR)[23] and the UN Special Procedures, the Inter-American Commission on Human Rights (IACHR)[24] — regarding the need to carry out a diligent investigation, with reinforced autonomy guarantees, more than six years after the announcement of the launch of the first investigation, and nine months after the launch of the second, no significant progress has been made. On the contrary, the Prosecutor's Office has, among other shortcomings, refused to assent and to carry out essential acts of investigation, obstructed and fragmented the investigations, placed the burden of proof on the victims and denied them a copy of the investigation files.[25]

22. Centro Militar de Inteligencia (SEDENA), "Misión y Objetivo del C.M.I. E.M.D.N.", May 2021, available at: https://r3d.mx/wp-content/uploads/MISION-CMI.pdf

23. Office of the UN Human Rights Office of the High Commissioner, available at: https://hchr.org.mx/comunicados/la-onu-dh-expresa-su-preocupacion-por-actos-de-vigilancia-ilicita-contra-personas-defensoras-de-derechos-humanos-y-periodistas/

24. UN Special Rapporteur on freedom of opinion and expression & Special Rapporteur for Freedom of Expression (RELE) of the Inter-American Commission on Human Rights (IACHR), *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expression*, June 21, 2013, available at: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

25. FEADLE investigation file (carpeta de investigación) FED/SDHPDSC/UNAI-CDMX/0000430/2017; Ahmed, Azam, "Mexico Spyware Inquiry Bogs Down. Skeptics Aren't Surprised", The New York Times, February 20, 2018, available at: https://www.nytimes.com/2018/02/20/world/americas/mexico-spyware-investigation.html; R3D: Red en Defensa de los Derechos Digitales, "A un año de #GobiernoEspía, prevalece la impunidad", June 20, 2018, available at: https://r3d.mx/2018/06/20/comunicado-a-un-ano-de-gobiernoespia-prevalece-la-impunidad/

37. Justice and accountability are also obstructed by the authorities under scrutiny, who consistently claim no database or formal documentation of the records regarding the persons or numbers targeted by Pegasus exist. In 2019, the National Institute of Access to Information and Protection of Personal Data (INAI) determined that the Prosecution's Office had breached its obligations under the Personal Data Protection legislation by concealing contracts with NSO Group.[26] However, to date, the Office of the General Prosecutor has refused to undertake any serious and independent investigation regarding the documented breach.

38. The, at least, three criminal investigations known have yet to show any signs of progress. The only arrest of a person[27] — who was indicted for the crime of wiretapping for his suspected participation as the operator of the software within one of the intermediary companies between NSO and PGR— was only possible due to information provided by one of the victims, which referred the authorities to the network of intermediaries that operated Pegasus. Nonetheless, to date, the trial hearing has not been held with respect to the only person detained.

39. Of significant concern, little progress has been made to establish the responsibilities of authorities and institutions. 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. Also, no effective investigative actions have been carried out regarding the reports of Pegasus use by the intelligence agency (CISEN) or the Mexican Army during the past government.

40. With regard to the most recent investigation about *Pegasus* abuse by the Army between 2019 and 2022, the Prosecutor Office has not made any progress in more than 9 months. It hasn't even been able to obtain the contracts in which the Army obtained *Pegasus* licences. SEDENA has refused to make public the contracts with NSO for the acquisition of *Pegasus* or other surveillance systems,

26. INAI, "Determina INAI que FGR, respecto al software Pegasus, incumplió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", February 20, 2019, available at: https://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf

27. Article 19 MX-CA, "Avance del caso Pegasus en México debe ser un punto de no retorno que ayude a esclarecer un crimen de talla mundial", November 8, 2021, available at: https://articulo19.org/avance-del-caso-pegasus-en-mexico-debe-ser-un-punto-de-no-retorno-que-ayude-a-esclarecer-un-crimen-de-talla-mundial/%20; Aristegui Noticias, "Detiene FGR a uno de los involucrados en espionaje con Pegasus", November 8, 2021, available at: https://aristeguinoticias.com/0811/mexico/detiene-fgr-a-uno-de-los-involucrados-en-espionaje-con-pegasus/

as publicly promised by the President.[28] This despite ample evidence and documents that show the number and dates of the contract, as well as the payments made by SEDENA.

41. 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 yet to be made public by Mexican State authorities. Not only has the government failed in its obligation to bring truth and justice to the victims, but it has perpetuated impunity and generated the conditions for the repetition of the unlawful surveillance.

E. SURVEILLANCE AND MILITARIZATION

42. Abusive surveillance exacerbates in a context where Mexico has led and maintained for more than fifteen years a military approach to public security risks, granting powers to the military that are constitutionally prohibited. As previously stated, the Army does not have legal powers to intercept private communications. Nonetheless, as demonstrated at least since 2011, it has illegally done so.

43. The Army has systematically abused surveillance technologies to interfere with investigations carried out officially and by human rights defenders and journalists related to the Army's human rights abuses. In fact, information that has been made public as a result of the hacking carried out by Colectivo Guacamaya confirms that the surveillance and monitoring activities carried out by SEDENA are mainly done against civil organisations, human rights defenders, activists and journalists, where they are classified as "pressure groups"[29] for their work in defence of human rights.

44. Furthermore, in a context in which the Army does not only control the federal security and intelligence apparatus, but now controls ports, airports, and roads, as well as operates trains, refineries, airlines, touristic resorts, banks and many other business interests, it is particularly problematic that it deploys surveillance technologies with complete opacity and impunity.[30]

28. R3D: Red en Defensa de los Derechos Digitales, "Persisten interrogantes respecto de la información presentada por la SSPC sobre la adquisición y uso de Pegasus", July 29, 2021, available at: https://r3d.mx/2021/07/29/interrogantes-sspc-pegasus/

29. https://twitter.com/CentroProdh/status/1576928933312102400

30. Centro ProDH: Centro de Derechos Humanos Miguel Agustín Pro Juárez, A.C., *Poder Militar. La Guardia Nacional y los riesgos del renovado protagonismo castrense*, June 2021, available at: https://centroprodh.org.mx/wp-content/uploads/2021/06/Informe_Poder_Militar.pdf

RECOMMENDATIONS

In light of the above considerations, R3D and PI make the following recommendations to Mexico:

1. Adopt a moratorium on the sale, acquisition, transfer and use of surveillance technology conducted by means of hacking electronic devices through intrusive software, until regulatory frameworks exist, and their use is in line with human rights.

2. Establish an international group of experts to autonomously and independently investigate and punish those responsible for the unlawful surveillance of journalists and human rights defenders with Pegasus malware. In addition,

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 and C.M.I.'s personnel 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 government agencies' 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. Adopt legal and administrative reforms of surveillance powers, implementing the following safeguards to guarantee that the practice of these activities is commensurate with a focus on human rights:

a. Legality.

- **Surveillance powers** must be authorised by law, that clearly and precisely establishes conditions for their use, requirements and identification of agents involved in the decision-making and operation, the circumstances and the procedures for undertaking communications surveillance and access to communication data (metadata), as well as carrying out other forms of surveillance, such as real-time geolocation of communication equipment;

- The **acquisition and commercialization of equipment and systems** for the interception of communications must require a **registry of providers** and of **equipment and/or systems**, also requiring for its commercialization a previous authorization of an independent body based on a review of the information given in the application, as well as a human rights assessment.

b. 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 any surveillance measure. In this regard, the law should

- Establish **the prohibition of mass, indiscriminate surveillance**, such as mass interception of communications, access to the bulk communications stored by telecoms operators and others, mass hacking, indiscriminate use of facial recognition technology, which are inherently contrary to human right standards and compromise the integrity and security of communication systems. For instance, eliminate requirements for massive and indiscriminate retention of communications metadata provided for in Article 190, Section II, of the Federal Telecommunications and Broadcasting Law;

- Establish the obligation to implement technical, administrative and physical measures to prevent unregistered uses, modification, loss, destruction, dissemination

and disclosure of personal data, as well as prevent unregistered surveillance systems or alterations in the use registry;

- **Destruction and return of data:** government authorities must establish a procedure to destroy personal data that is irrelevant to the investigation, in addition to establishing a record of this procedure.

c. 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.

- Establish certification requirements, confidence control evaluations and a detailed registry of the agents who have been trained and participate in data harvesting practices, as well as in surveillance measures, including those that do not require the collaboration of any concessionaire or provider, as well as the cases and circumstances in which the federal judicial authority may authorise surveillance measures.

d. Prior or immediate judicial authorisation. Explicitly establish the need to have prior and duly founded judicial authorisation to carry out surveillance measures, except in emergency cases in which judicial review should be immediate, which may only be authorised by a federal judicial authority when it is a suitable, necessary, and proportionate measure.

e. Independent oversight. Grant effective powers of scrutiny and oversight of surveillance systems to an existent (e.g., the data protection authority, INAI) or new independent and impartial authority, including the possibility of consulting technical experts and experts in other areas, and to impose effective remedies.

f. Right to notification. Recognise the right of every person to be notified of state interferences in their private life. Such notification may only be deferred subject to judicial authorisation when the notification would demonstrably and seriously hinder an investigation or endanger the life or physical integrity of a person, in which case notification take place after the reasons for its delay have passed.

g. Transparency. Establish mechanisms that ensure a detailed record of data usage and processing, surveillance measures (e.g. agents involved, subjects and methods used) and all the information registered and related to the acquisition process.

• Provision to prohibit the automatic classification of all information related to the contracts for the acquisition of these equipment and/or systems as “reserved” or “confidential” information.

h. Accountability.

• **Cooperation in the investigation of unlawful and uncontrolled surveillance.** It is essential for the State to require in its authorization or contracting processes guarantees of cooperation in the investigation of reports of unlawful surveillance. Accountability mechanisms cannot depend on the cooperation of the operator or on the operator’s access to certain essential information. The purchasing government has the power to set the requirements for the acquisition of communication interception equipment and systems and the industry must adapt to them. E.g., systems can be configured to allow external actors (e.g. the judge authorising the wiretapping measure) to verify how it is carried out.

• **Redress:** people subject to unlawful state communication surveillance must have access to an effective remedy.

• Establish clear, harmonised and simple national procedural laws for complaints data subjects can file with specialised Data Protection Authorities and appropriate judicial remedies.

4. Repeal existing legislation and refrain from passing legislation that contains provisions regarding surveillance and interference of private communications that fail to comply with the aforementioned human rights standards and/or vest powers to carry out surveillance measures to authorities not authorised by the Constitution.

— Ensure that military authorities are prohibited from carrying out surveillance of civilians/non-military targets.

— In this aspect, 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**.

THE RIGHT TO PRIVACY IN MEXICO