Submission for consideration
Human Rights Committee

The right to privacy in Mexico

Presented by Red en Defensa de los Derechos Digitales (R3D), Privacy International and ARTICLE 19 (Office for Mexico and Central America)
August 2025

INTRODUCTION

1. This submission is presented by Red en Defensa de los Derechos Digitales (R3D), Privacy International (PI) and ARTICLE 19, Office for Mexico and Central America. 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. ARTICLE 19 is an independent non-governmental organisation that promotes and defends the progressive implementation of freedom of expression and freedom of information worldwide in accordance with the highest international human rights standards.

2. The three organizations wish to raise concerns regarding the right to privacy (article 17 of ICCPR) in Mexico, for consideration in advance of the adoption of the list of issues prior to reporting for Mexico by the Human Rights Committee (HRC).

The Right to Privacy in Mexico

3. 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.'*

4. 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.'

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

6. 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.

[1] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

[2] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

ISSUES OF CONCERN

A. Inadequate regulation of surveillance and lack of safeguards

7. In December 2024, a constitutional amendment in Mexico disestablished the autonomous body responsible for personal data protection and transparency: the National Institute of Access to Information and Protection of Personal Data (INAI).

8. Reforms in March 2025 to Data Protection Laws[3]: **(i)** eliminate the powers of transparency authorities[4] to bring actions of unconstitutionality against legislation or executive acts, as well as criteria that strengthened transparency, maximum publicity, and the right of access to information; **(ii)** include vague concepts to restrict access to information of public interest, such as "social peace" and "damage to the interests of the State"; and, **(iii)** create a decentralized body called "Transparency for the People" that lacks autonomy and eliminates requirements that affect the impartiality and professionalization of transparency authorities.

9. In July 2025, the Mexican government also fast-tracked a series of laws in the Congress to establish an uncontrolled system of massive surveillance and social control that is incompatible with the rights to privacy, data protection, freedom of expression, presumption of innocence, non-discrimination, and the principle of non-incrimination of the whole population.

10. Laws on Telecommunications and Broadcasting[5], Public Security[6], Investigation and Intelligence[7], General Population[8], Enforced Disappearances[9], and the National Guard[10], establish a permissive architecture for state surveillance without safeguards for the protection of human rights.

11. For instance, a biometric ID system has been established and will be mandatory to access any public or private service in Mexico. Article 91 bis of the General Population Law

---

[3] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados and Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[4] Of 33 agencies: 32 state level institutes and INAI at the national level. These agencies were responsible for ensuring access to public information and protection of personal data and acted as mediators when authorities failed to comply with their obligations.

[5] Ley en Materia de Telecomunicaciones y Radiodifusión, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LMTR.pdf

[6] Ley General del Sistema Nacional de Seguridad Pública, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf

[7] Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LSNIIMSP.pdf

[8] Ley General de Población, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LGP.pdf

[9] Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas, available at https://www.diputados.gob.mx/LeyesBiblio/ref/lgmdfp.htm

[10] Ley de la Guardia Nacional, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf

indicates that this ID must be used in identification validation and authentication processes on electronic platforms, and that it will be required to access all public and private procedures and services. Not having a biometric ID will hinder individuals' capacity to carry out bureaucratic procedures and access both public and private services, affecting the economic, social, political, civil and cultural rights of anyone who resides in Mexico.

12. Furthermore, these biometric ID will be stored in a Single Digital Identity Platform and will be interconnected to a Central Intelligence Platform, and any activity carried out with this identification code will leave a trail that can be tracked by an unspecified number of public authorities, permanently, unrestrictedly and in real time, without a court order or any type of control.

13. The package of laws approved in July 2025 also mandate the interconnection of all national and international databases, both public and private, so that authorities can access them without the necessary controls. Regulation of surveillance powers lack effective safeguards to prevent abuse, such as independent oversight, notification and transparency measures. As it will be expanded further, the lack of safeguards has made it difficult to prevent or detect abuse, but even when abuse has been found, it has made it difficult to avoid impunity and non-repetition.

14. Additionally, civil and military authorities will be able to access highly sensitive personal data of citizens without a judge authorising such access. This is particularly troublesome in a context where judicial oversight has been often eluded or insufficient to prevent abuse.

15. 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.[11]

[11] This information was 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.

During 2016 and 2017, data was also published by telecommunications concessionaires and authorized entities. However, the Federal Telecommunications Institute (IFT) removed the obligation to publish such information without justification.

For further information, see: R3D: Red en Defensa de los Derechos Digitales, "*El Estado de la Vigilancia*" (The State of Surveillance), January 2025, p. 52, available at: https://r3d.mx/wp-content/uploads/EDLV_2025.pdf

16. The Secretary of National Defense is also now empowered under the Organic Law of Public Administration[12] to process and use information for intelligence activities that have national security purposes, without any judicial or other independent authorisation or oversight or safeguards to limit these powers or prevent abuse. Furthermore, the National Guard can access stored data (call logs) and geolocation information without a court order, that is, without any control to verify and justify that this information is necessary for the alleged purposes for which it is required. The National Guard is also authorized to conduct covert surveillance operations, which could result in the illicit collection of evidence and violate the right to privacy and due process considerations (including the exclusionary rule).

17. 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.[13] 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 investigative and intelligence services for preventive purposes.

18. The consolidation of unchecked surveillance powers for authorities—especially armed forces—, the weakening of oversight mechanisms, and the establishment of a system that can constantly monitor society through the requirements of mandatory centralized and massive databases of personal data are a serious violation of the right to privacy and will have a chilling effects on other human rights, such as freedom of expression, assembly and association. As such, these reforms represent a serious setback and contravene the international human rights obligations of Mexico including under the ICCPR.

B. Irregular acquisition of surveillance technologies

19. Several concerns have been reported in the acquisition and use of surveillance technologies. The opacity and absence of adequate regulation and independent oversight regarding the contracting processes of equipment and systems for the interception of private communications has encouraged corruption, hindered accountability and promoted impunity for the abuse of such systems.

20. 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

[12] Ley Orgánica de la Administración Pública Federal, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LOAPF.pdf

[13] Articles 7 XI and 9 V-VII, XXVI, Ley de la Guardia Nacional, *op. cit.*

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.[14]

21. 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.

22. Since surveillance abuse cases have been made public, transparency has also been demanded on all the contracts for the acquisition of surveillance technologies by Mexican authorities.[15] However, requests for information about these contracts are often met with a denial by authorities by claiming confidentiality or that the information is reserved in absolute terms, which violates the right to access information, particularly considering the public interest in transparency surrounding surveillance technologies.

23. 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.

24. Transparency regarding the authorities involved in the procurement processes is also particularly relevant considering the findings of surveillance tools from authorities without the legal competences to use them. For example, among the Mexican authorities that have reportedly 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 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

---

[14] "The State of Surveillance" by R3D includes a diagnosis of communications surveillance in the country carried out from 2012 to 2023, according to official records of acquisitions. Available at https://r3d.mx/wp-content/uploads/EDLV_2025.pdf

[15] 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

Federal Police, the Office of the General Prosecutor, and even Petróleos Mexicanos (PEMEX).[16] The vast majority of listed authorities do not have legal powers to conduct surveillance of private communications, so both the acquisition and use of such technologies would have been unlawful.

25. Another relevant aspect has been the corruption associated with the purchase of malware. For example, investigative journalism 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.[17] 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.

C. Abusive surveillance of human rights defenders and journalists

a. Malware abuse

26. In 2016, research done by Citizen Lab[18] found that most of the domain names that NSO Group's infrastructure used to infect 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.

27. The suspicions were confirmed in 2017 by Mexican civil society organisations through investigations such as "Gobierno Espía"[19], along with reports from Citizen Lab[20]. 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 infecting their devices with *Pegasus* malware. So far, more than

---

[16] See, R3D: Red en Defensa de los Derechos Digitales, *El Estado de la vigilancia. Fuera de control* (The State of Surveillance. Out of Control), November 2016, p. 89, available at: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

[17] 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/

[18] Marczak, Bill & John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," Citizen Lab Research, Reporte No. 78, University of Toronto, Agosto 2016, disponible en: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[19] 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* (Spying Government. Systemic surveillance of jorunalists and human right defenders in Mexico), June 2017, https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf

[20] 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/

25 surveillance cases against journalists and human rights defenders in Mexico have been documented.[21]

28. Civil society organisations also verified that Mexican authorities, such as the Ministry of National Defense (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 malware. However, these authorities have claimed no database or formal documentation of the records regarding the persons or numbers targeted exist.[22]

29. Despite the change of government and the repeated declarations by former President López Obrador that surveillance on journalists and human rights defenders would no longer occur, and that *Pegasus* or any other similar private communications interception system would no longer be operated, unlawful surveillance practices are likely ongoing. The investigation "Ejército Espía" revealed new cases of *Pegasus* surveillance attributable with a high degree of certainty to the Mexican Army.[23]

30. The investigation highlights a leaked internal SEDENA document[24], addressed to the Secretary of National Defense, obtained by Colectivo Guacamaya, which demonstrates the conclusion of a contract between the SEDENA and the company Comercializadora Antsua[25] — 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 SEDENA does not have legal authorization to intercept private communications of civilians.

31. Up to now, the victims of surveillance documented under MORENA's administration are the Under-Secretary for Human Rights, Alejandro Encinas[26], 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 the 1960s to

---

[21] 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/

[22] Fiscalía Especial para la Atención de Delitos cometidos contra de la Libertad de Expresión investigation file (carpeta de investigación) FED/SDHPDSC/UNAI-CDMX/0000430/2017.

[23] *See*, R3D: Red en Defensa de los Derechos Digitales, "Ejército Espía", available at: https://ejercitoespia.r3d.mx/ejercito-espia/

[24] *See*, https://ejercitoespia.r3d.mx/wp-content/uploads/2022/10/Mortal-de-Oficio.png

[25] 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.

[26] 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.

the 1980s—, Camilo Vicente Ovalle[27], 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. 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 was 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 said case and represents many other victims of military abuses. Centro Prodh had also been previously found to be targeted with Pegasus in the previous government.[28] Also, the journalists were attacked when they were publishing information related to human rights abuses committed by the military.[29]

33. Documents shared by Colectivo Guacamaya[30] show how 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*[31]. 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 from the Guacamaya collective leak revealed the military structure behind the use of *Pegasus*: the Military Intelligence Center[32] (C.M.I.). 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.

---

[27] 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/

[28] 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/

[29] Bill Marczak, et al., "Triple Threat NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains", April 18, 2023, available at: citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/

[30] *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

[31] A secret information card was prepared on September 2, 2020 under the name "Activities Raymundo Ramos", 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 Centro Militar de Inteligencia.

[32] 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

35. Also, according to court documents[33] from the litigation between WhatsApp and the Israeli company NSO Group, 456 people in Mexico were spied on with Pegasus spyware between April and May 2019, during the six-year term of President Andrés Manuel López Obrador, with the number of attacks corresponding to Mexico representing 37 percent of the total documented incidents.

D. Impunity for surveillance abuse

36. 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.[34]

37. Despite the call of multiple instances, national and international —such as the Office of the UN Human Rights Office of the High Commissioner (OHCHR) and the UN Special Procedures, the Inter-American Commission on Human Rights (IACHR)— regarding the need to carry out a diligent investigation, with reinforced autonomy guarantees, more than eight years after the announcement of the launch of the first investigation, and three years after the launch of the second, no 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.[35]

38. Justice and accountability are also obstructed by the denounced authorities, who consistently claim no database or formal documentation of the records regarding the persons or numbers targeted exist. In 2019, the INAI determined that the Prosecution's Office had breached its obligations per the Personal Data Protection legislation by

---

[33] *See*, WhatsApp Inc vs NSO Group Technologies Limited et al, available at: https://www.documentcloud.org/documents/25892995-whatsapp-v-nso-exhibits-2-3-15-19-21-23-25-28-35-37-42-declaration-micah-g-block/

[34] Comisión Interamericana de Derechos Humanos, "CIDH manifiesta su preocupación por el aumento de casos sobre uso de Pegasus en México", June 2, 2023, available at: https://www.oas.org/en/IACHR/jsForm/?File=/es/cidh/prensa/comunicados/2023/109.asp

[35] 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/

concealing contracts with NSO Group.[36] However, to date, the Office of the General Prosecutor has refused to undertake any serious and independent investigation regarding the obstruction of justice documented.

39. Furthermore, several investigations have yet to show any signs of progress. The only arrest of a person[37] —who was indicted for the crime of wiretapping for his probable 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.

40. Nonetheless, in January 2024, a judicial decision confirmed that a journalist, Carmen Aristegui, had been surveilled with Pegasus, but considered that the Prosecutor's Office did not sufficiently prove anyone's direct participation in the illegal interception of Aristegui's private communications and regretted that access to justice could not be guaranteed due to the failure of the Prosecutor's Office to meet the standards of proof.[38]

41. Further, little or no progress has been made to establish the responsibilities of other authorities and institutions reportedly involved in unlawful surveillance. The Prosecutor's Office's reluctance to carry out investigative procedures concerning the Office of the General Prosecutor's AIC suggests 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 serious investigative actions have been carried out regarding the intelligence agency (CISEN) or the Mexican Army, despite evidence suggesting them as *Pegasus* operators during the past governments.

42. 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 three years. It has not even been able to obtain the contracts in which the Army obtained

---

[36] 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

[37] ARTICLE 19, "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; and 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/

[38] ARTICLE 19, "Juicio confirma espionaje con Pegasus contra Carmen Aristegui por labor periodística; FGR debe continuar con las investigaciones", January 12, 2024, available at: https://articulo19.org/juicio-confirma-espionaje-con-pegasus-contra-carmen-aristegui-por-labor-periodistica-fgr-debe-continuar-con-las-investigaciones/

Pegasus licences. SEDENA has refused to make public the contracts with NSO for the acquisition of *Pegasus* or other surveillance systems, as publicly promised by the President[39]. This despite ample evidence and documents that show the number and dates of the contract, as well as the payments made by SEDENA.

43. In January 2023 the INAI decided to revoke the response of SEDENA that claimed no information regarding contracts related to the Pegasus spyware existed and ordered the disclose of the information.[40] Despite the fact that this resolution is final and unassailable, SEDENA refused to comply with the resolution. Therefore, R3D presented an amparo that led to a judicial decision in July 2024 by which a judge ordered SEDENA to release public versions of the contracts.[41] To date, SEDENA has not complied with the judicial decision.

44. 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 abuses.

ISSUES/QUESTIONS

Considering the concerns illustrated in this submission and the repeated recommendations by UN and regional human rights mechanisms as well as the 2023 UPR of Mexico, the organisations recommend that the HRC include the following issues/questions in the list of issues for Mexico:

On 2025 legislation

How do the laws enacted in July 2025 respect, protect, guarantee, and promote the right to privacy and other human rights? In particular, which safeguards, transparency and accountability measures are prescribed in the new laws in line with international human rights standards regarding the rights to privacy, data protection, freedom of expression, presumption of innocence, fair trial?

On accountability for the misuse of malware technology

---

[39] 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-pega- sus/

[40] *See*, https://ejercitoespia.r3d.mx/wp-content/uploads/2024/02/RRA-20263-22-JRV.pdf; R3D: Red en Defensa de los Derechos Digitales, "Juez ordena a la SEDENA cumplir resolución del INAI que le obliga a entregar contratos de Pegasus", July 23, 2024, available at: https://r3d.mx/2024/07/23/juez-ordena-a-la-sedena-cumplir-resolucion-del-inai-que-le-obliga-a-entregar-contratos-de-pegasus/

[41] *Ibid.*

Is Mexico planning to 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?

Has Mexico established an independent oversight mechanism or 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?

Which reforms and actions has the Mexican government carried out in order to prevent, effectively investigate and ensure accountability in cases of unlawful surveillance of journalists and human rights defenders through intrusive software, especially where state institutions, including the military, are involved? In particular, what progress has been made in the criminal investigations that started in 2017 and 2022 for the crimes of illegal interception of private communications against human right defenders and journalists?

On the protection of freedom of expression, including the right to receive information

What steps is the government taking to ensure freedom of expression and the safety of journalists and Human Rights Defenders against threats and violence? How does the government plan to protect them and to prevent, investigate, and prosecute crimes against journalists at the state and federal levels?

Will Mexico consider adopting legislation to make it mandatory for public and private sector organisations to publish transparency records regarding the treatment of personal information?