Núcleo de la Sociedad Civil para el Gobierno Abierto en México

Open Government Partnership
1110 Vermont Avenue NW
Suite 500/ Open Gov Hub
Washington, DC 20005
United States

Letter of Concern

July 16th, 2018

Dear Members of the OGP Steering Committee,

In February 2017, evidence on the potential involvement of different Mexican government offices in illegal and disproportionated digital surveillance against at least three prominent research scientists and health advocates in Mexico was revealed by a technical report done by Citizen Lab with help of Mexican digital rights NGOs Article19, SocialTIC and R3D and reported by the New York Times. This attack targeted two individuals in organizations that have actively participated in the open government commitment building processes.

At the Mexican Open Government Secretariat meeting of February 16th, 2017, a letter signed by all 10 Mexican civil society organizations that lead the Open Government Partnership (OGP) actions in Mexico, was delivered to the Mexican government leads in OGP expressing profound preoccupation on government-lead surveillance on civil society, asking for an urgent inquiry on illegal surveillance against civil society and demanded that the Mexican Technical Tripartie Secretariat meeting proactively established the necessary efforts (such as an open government additional commitment) to enable regulation and transparency and accountability controls that can prevent illegal and disproportionate surveillance.

After 3 months of a lack of response from the Mexican authorities, on May 23rd 2017 the Mexican civil society core group decided to quit its participation in the 3rd Action Plan and the Tripartie Secretariat (see letter sent to the Mexican Government[1] and letter to OGP Steering Committee[2]). In the months to follow, more surveillance cases were revealed becoming an international scandal. Dozens of Mexican and international organizations have condemned illegal government surveillance, including both the UN and OAS special rapporteurs on freedom of expression. Over one year later, the current administration has shown no political will to solve the problematic and the open government process with civil society is still broken.

Scientific evidence and country in-depth surveillance reports indicate that the Mexican government offices purchase and use high-end technology against civil society and journalists without any public judicial evidence nor accountability frameworks to support it. As of August 30th 2017, technical proof has revealed that there have been over 100 infection attacks targeting 22 individuals including renowned journalist Carmen Aristegui and her son (then a minor), CEO of anti-corruption NGO IMCO and OGP member of the 1st Steering Committee Juan Pardinas, human rights lawyers and even the

[1] See letter sent to STT in May 23rd, 2017 in English (https://goo.gl/78q6tt) and Spanish (https://goo.gl/4nh8wM)
[2] See letter sent to OGP in May 23rd, 2017: https://goo.gl/hGGkfC

Interdisciplinary Group of Independent Experts sent by the Organization of the American States (OAS) to inquiry on the 2014 disappearances of 43 students in Iguala, Guerrero.

Different top Mexican government officials (including the President Enrique Peña Nieto) have addressed the issue in an erratic, late and light manner deeply breaking the most basic trust from civil society. In February 2017, no reaction was made by the executive branch, including the Secretary of Public Affairs and lead of the open government process. As more surveillance cases were made public in June 2017, the President's spokesman first denied the cases but days later the President himself publicly acknowledged the ownership of surveillance technologies, minimized the importance of surveillance and even threatened to prosecute those spreading rumors on the matter. The President withdrew his statement one day later.

In response to the legal case presented by several surveillance targets, the Attorney General's Office on Freedom of Expression publicly announced that they would lead the criminal inquiry but one year later no progress has been made. In late 2017 and early 2018, the Ministry of Public Affairs addressed the Mexican civil society with a proposal to resume dialogue and joint open government activities but failed to address the core civil society's demands on the issue: have the political will so that an in-depth inquiry on the surveillance cases can be done and establish a co-creation process that can identify and implement regulation that enables transparency and accountability controls that can prevent illegal and disproportionate surveillance in Mexico.

We, as the civil society core group of organizations that have fostered and engaged with government OGPs processes in Mexico since its adoption, write this letter of concern as a last resource to help clarify and address the involvement of the Mexican government in the use of digital surveillance against Mexican civil society. We believe that the actions described in this letter are of the highest concern for Mexican civil society open and safe civic participation and directly affect OGP's reputation.

Digital surveillance against civil society constitutes a direct threat to civic participation and is inconsistent to the basic principles of open government. Such actions directly affect the activities of civil society, the lives of individuals participating in civic spaces and the trust on the government. It is impossible to establish any true and equal co-creation space in open government if civil society is being targeted illegally and disproportionately by digital surveillance.

The civil society organizations that sign this letter have deeply questioned the Mexican government authorities real will to address the issues behind the most basic threats against secure and free citizen participation. We believe that Mexico, as one of the founding countries and current Steering Committee member should permanently uphold the values and principles expressed in the Open Government Declaration and in the Articles of Governance. The Mexican government has shown deep incongruencies in its actions and discourse regarding open government to the extent that it has undermined the current national open government progress and may likely undermine OGP's international credibility.

Therefore, we ask you to take action under the Policy of “Upholding the Values and Principles of OGP, as articulated in the Open Government Declaration” adopted on September 25th 2014 aiming to:

a) Assist a country in question to overcome difficulties and to help re-establish an environment for government and civil society collaboration, and
b) Safeguard the Open Government Declaration and mitigate reputational risks to OGP.

Civic space is what maintains open government real, true and effective. Any strategy, commitment and co-creation processes to build and maintain open government requires a safe, open and just civic

space. In Mexico, safe and open spaces for civic society participation and criticism have been drastically reduced (see Annex for digital surveillance national context and Annex 3 for national context). The surveillance attacks against journalists, civil society leaders and human rights advocates are perverse, silent and sophisticated actions by the Mexican government to control, threaten and close citizen participation. And, the lack of actions to address such reality will only perpetrate impunity and foster a state of surveillance in the country.

We still believe in open government and the OGP platform. All negotiation, instances and dialogue with the Mexican open government process have been followed to address the issues stated in this letter. Despite the lack of significant advances since February 2017 and the broken trust between government and civil society, we identify the response policy as the last resource to address the deep crisis that open government process platform is currently living. We demand that OGP intervene in the country's situation so that dialogue, trust and co-creation can be achieved either with the current or the next government administration.

Sincerely yours,

Ana Cristina Ruelas - Article19
Edna Jaime - CIDAC, Centro de Investigación para el Desarrollo
Ernesto Gómez - Contraloría Ciudadana
Tomás Severino - Cultura Ecológica
Haydeé Pérez - Fundar, Centro de Análisis e Investigación
Alejandro González - GESOC, Agencia para el Desarrollo
Juan E. Pardinas - IMCO, Instituto Mexicano para la Competitividad
Francisco Rivas - Observatorio Nacional Ciudadano
Juan Manuel Casanueva - SocialTIC
Eduardo Bohórquez - Transparencia Mexicana

ANNEX 1 - DIGITAL SURVEILLANCE USING NSO GROUP PEGASUS SPYWARE

In July and August 2016 at least three prominent Mexican health rights researchers and advocates, received suspicious SMS with malicious links while they were advocating to increase the soda tax in Mexico, improve consumer product labeling, and raise awareness of health risks associated with sugary drinks. These individuals are Dr. Simon Barquera, a researcher at Mexican Government's Instituto Nacional de Salud Pública (National Institute of Public Health), Alejandro Calvillo, Director of consumer rights and health advocacy NGO El Poder del Consumidor, and Luis Encarnación, Director of Coalición ContraPESO that works on obesity prevention.

These targeted individuals noticed that the text messages were provocative, personally directed and even threatening (see CitizenLab Report[3]). With concern they shared the text messages with Mexican digital rights and security NGOs SocialTIC and R3D who identified a similar attack pattern previously described by CitizenLab's August 25th 2016 report on NSO's technology that had been used to spy a renowned UAE rights advocate Ahmed Mansoor and Mexican investigative journalist Rafael Cabrera.[4] The technology used was created and sold by the NSO Group which has the capacity to silently exploit an iPhone and install the Pegasus spyware. The Pegasus spyware is known to be able to actively record or passively gather a variety of different data about the device. By giving full access to the phone's files, text and chat messages, microphone and video camera, the operator is able to turn the device into a silent digital spy in the target's pocket. This spyware can also access a wide range of personal data, such as calendar data and contact lists, as well as passwords, including Wi-Fi passwords. It is important to note that these attacks are targeted to specific individuals since Pegasus, as many other similar high-tech spyware, is sold under a licensing scheme where each infection unit is associated to a target.

The NSO Group is an Israeli "cyber war" company that sells sophisticated intrusion tools to "authorized governments with technology that helps them combat terror and crime". The NSO Group claims to obey "strict export control laws and regulations".[5] There is information that the Mexican government purchased NSO Group's spyware for 20 million USD in 2012.[6]

CitizenLab has identified that the most exploit infrastructure names are associated with Mexico, most probably used to attack Mexican targets. The other NSO exploit top infrastructure domains are from United Arab Emirates and Uzbekistan.[7]

SocialTIC and R3D requested CitizenLab's technical support in order to technically assess the attacks. After an in-depth analysis, CitizenLab published a report that identifies that the messages sent to Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación all contained links pointing to domains previously identified as part of our investigation into NSO's infrastructure. The URLs in several text messages directly linked to exploit infrastructure.

On February 11th 2017, CitizenLab issued an in-depth report on the attacks on Barquera, Calvillo and Encarnación in which they describe the infection process in detail. Also, the New York Times published a story on this case on its front page where recalls the context of the attacks and highlights that "NSO emails leaked to The New York Times referred to multimillion-dollar, continuing NSO Group

[3] See full report: https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/
[4] See full report: https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
[5] More information in https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#6cf19ae73997
[6] See http://www.haaretz.com/israel-news/business/economy-finance/1.574805
[7] See infrastructre section at https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

contracts with several government agencies inside Mexico, and the Mexican government has been an enthusiastic buyer of foreign spy tools".[8]

On February 13th 2017, attacked Mexican NGOs El Poder del Consumidor and Coalición ContraPESO, alongside with Article19, R3D and SocialTIC, held a press conference and issued open letters visualizing these attacks and asking the Mexican Government for an explanation and an in-depth inquiry.[9] No public or official response from any Mexican Government office or official occurred.

At the Mexican Open Government Secretariat meeting of February 16th, 2017, a letter signed by all 10 Mexican civil society organizations that lead the open government partnership actions in Mexico, was delivered to the Mexican government leads in OGP (Arely Gómez from the Secretary of Public Function, Alejandra Lagunes of the National Digital Strategy Coordination at the President's office and all 7 commissioners of the Mexican Access to Information Institute - INAI) expressing profound preoccupation on government-lead surveillance on civil society, asking for an urgent inquiry on illegal surveillance against civil society and demanded that the Mexican OGP Secretariat proactively established the necessary efforts to enable regulation and transparency and accountability controls that can prevent illegal and disproportionate surveillance.[10] No public nor official response to address these issues was expressed by the Mexican Government or INAI at the time.

On June 19th 2017, CitizenLab's second technical report on new proven cases of Mexican individuals targeted with NSO Group's Pegasus spyware was made public.[11] New York Times published the story in it's front cover and Mexican NGOs held a press conference alongside the testimonies of surveillance victims.[12] The targets were renowned journalists, human rights and anti-corruption civil society specialists all working in different high-profile investigations, human rights abuse cases defense and anti-corruption initiatives. Mexican NGOs R3D, Article19 and SocialTIC published an in-depth report that described how the targets had been lured to click links with NSO malware exploits in specific timing linked to milestones of activity that could expose and challenge Mexican government authorities, including the president.[13]

Nine surveillance targets assisted by Digital Rights NGO R3D filed a joint formal criminal complaint at the Mexican General Attorney's Division on Crimes Against Freedom of Expression also on June 19th 2017.[14] This accusation started the formal criminal proceedings in compliance with Mexican law. In reaction, three days later, the Mexican President, Enrique Peña Nieto declared in a public event that the Mexican government does own surveillance technology, minimized the importance of surveillance against citizens, claimend the accusations to be false and threatened to file legal action against those "spreading false accusations".[15] Civil society organizations publicly condemned the President's statements as it, instead of aiming to defend people's right and basic legal due process, he explicitly limited a criminal investigation that had not even started and directly threatened civil society

[8] See full story: https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?_r=0
[9] See press release: http://elpoderdelconsumidor.org/saludnutricional/el-espionaje-del-gobierno-de-mexico-a-defensores-del-derecho-a-la-salud-no-debe-quedar-impune/
[10] See letter sent to the Mexican OGP Secretariat; https://goo.gl/z4reBU
[11] See CitizenLab full report: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/
[12] See NYT full story: https://nyti.ms/2sGmhJ0
[13] See full #GobiernoEspía report: https://r3d.mx/gobiernoespia
[14] See accusation document sent to start the criminal inquiry: https://r3d.mx/wp-content/uploads/Denuncia-FEADLE-P%C3%BAblica.pdf
[15] See video: https://twitter.com/R3Dmx/status/878259101595090944

organizations and surveillance targets.[16] The next day, on June 23rd, the President publicly withdrew his previous statements highlighting that he would not prosecute those accusing the Mexican government of illegally surveilling journalists, activists and civil society members.[17]

On June 26th, the General Attorney's office made their criminal investigation plan public.[18] In response, civil society organizations responded with a public statement highlighting the plan's lack of detail and impartiality on the involvement of external technical advice and demanded that an international expert group be formed to give professional, non-bias and specialized oversight to the investigation.[19] This demand was never granted. Also, no official statement, collaboration or proactive action was done by the Ministry of Public Administration, which is the Mexican Government's lead at the Tripartite Secretariat, to support, drive or channel civil society's observations regarding the criminal investigation.

These surveillance revelations have outraged Mexican, Latin American and international organizations and prominent individuals. On February 14th 2017, a letter signed by leading digital rights, civic-technology and data organizations and technology groups was publicly shared. This case was showcased by CitizenLab at a plenary conference at the Internet Freedom Festival in March 2017.[20] And, on March 22nd, a letter signed by prominent public health specialists, scientists and organizations urged the Mexican president to “respect the values of freedom of expression, human rights and public health, investigate this situation in-depth and bringing justice”.[21]

As time passed and no advances were made in the criminal inquiry, international bodies focused on human rights have addressed the surveillance cases in Mexico as part of their country reports and declarations. On July 19th 2017, United Nations (UN) experts urged the Mexican Government to cease digital surveillance activity and to guarantee an impartial and independent investigation.[22] On December 4th 2017 and later on June 19th 2018, special rapporteurs on freedom of speech, David Keye (United Nations) and Edison Lanza (Organization of American States) on their joint visit to Mexico publicly asked the Mexican Government to guarantee the independence of the investigation.[23] Such claim has repeatedly been done by the victims and their lawyers as there is valid suspicion of the impartiality of the General Attorney's Office on an internal investigation as evidence shows that office was the one that purchased the NSO Group Pegasus malware.[24] And on March 2nd 2018 Human Rights special rapporteur Michael Frost addressed in his report from his 2017 visit to Mexico that illegal digital surveillance is worrisome under the Mexican context and it constitutes a violation to the right to privacy and the freedom of expression and association.[25]

---

[16] See public statement by civil society organizations: http://centroprodh.org.mx/index.php?option=com_content&view=article&id=2404:2017-06-23-00-19-01&catid=209:front-rokstories&lang=es

[17] See video of the President’s statements: https://www.youtube.com/watch?v=vOVJ_9tx2lU&feature=youtu.be

[18] See full statement from the Attrorney General’s office: https://twitter.com/PGR_mx/status/879405294337441792

[19] See full response: https://socialtic.org/blog/organizaciones-responde-a-feadle-de-la-pgr-sobre-espionaje/

[20] See IFF 2017 program https://internetfreedomfestival.org/schedule/ and session documentation https://internetfreedomfestival.org/wiki/index.php/Investigating_and_defending_against_Malware_Operations

[21] See support letter:http://elpoderdelconsumidor.org/comunidad-internacional-vs-espionaje/

[22] See OHCHR press release: https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=S

[23] See Mexico’s preliminary report http://hchr.org.mx/images/doc_pub/ES-final-version-preliminary-observations.pdf and final report http://hchr.org.mx/images/doc_pub/20180618_CIDH-UN-FINAL-MX_reportSPA.pdf

[24] See journalistic report on the purchase of the Pegasus malware https://contralacorrupcion.mx/pegasus-pgr/

[25] See Human Rights Council 37th session agenda http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Documents/A_HRC_37_51_Add_2_EN.docx

At at national level, Mexican authorities have done very little to address the issue and the demands of the victims and civil society organizations. The only formal approach was done on May 28th 2018 when a Mexican Federal Judge ordered the Attorney General Office to seriously attend the surveillance case inquiry, including to include in the investigation the proof that the victims and their lawyers included in the case since the start of the criminal investigation.[26]

More so, over a month after the OGP Steering Committee delegation visit to Mexico in October 2017, the Ministry of Public Administration open government team only sent a superficial work proposal to the civil society group in open government.[27] This proposal aimed to achieve a legal framework analysis and an attention protocol for illegal surveillance victims but did not address how the Mexican Government would try to improve the ongoing inquiry nor established any commitments that would enforce transparency, accountability and legal measures on illegal digital surveillance against citizens. [28] The only collaboration on the matter linked to the original Mexican open government Tripartite Secretariat is a working group between the Mexican Access to Information Institute (INAI) and different civil society organizations (R3D, Article19 and SocialTIC) that since early 2018 aims to analyze how transparency and access to information policies have been applied to surveillance and personal communications interventions in Mexico.

[26] See Mexican civil society press brief:
https://r3d.mx/wp-content/uploads/GobiernoEspia-comunicado-audiencia-21MAYO.pdf
[27] See the civil society group public communication at the OGP Steering Committe visit to Mexico in October 19th 2017:
https://gobiernoabiertomx.org/blog/2017/10/19/posicionamiento-del-nucleo-ante-la-visita-de-visita-de-mision-del-comite-directivo-de-ogp/
See the OGP Steering Committee Delegation report after its visit to Mexico in October 2017:
https://www.opengovpartnership.org/sites/default/files/OGP-SC-Envoys_Visit-Mexico_October2017.pdf
[28] See the Ministry of Public Administration letter and work proposal of December 5th 2017: https://goo.gl/9Movuo (letter) and https://goo.gl/psbdMa (work plan)
See civil society group response in December 14th 2017: https://goo.gl/sVFLWk

ANNEX 2 - DIGITAL SURVEILLANCE MEXICAN CONTEXT

Mexico has a worrisome digital surveillance history. Despite the lack of transparency from the Mexican government and the technical complexity that comes with identifying top-end spyware technology, there is now a track record that links the previous and current government administrations to the illegal purchases and use of highly intrusive technology such as the ones sold by Gamma International (ei. FinFisher spyware), Hacking Team (ei. Da Vinci and Galileo remote control systems) and NSO Group (ei. Pegasus spyware). Government digital surveillance has increased without following national laws, public explanations nor controls that can avoid its unlawful use against civil society. Local digital rights NGO Red para los Derechos Digitales (R3D) 2016's report on Surveillance in Mexico has defined the situation as "out of control".[29]

In 2012 civil society warned on potential use of a very sophisticated and highly intrusive spyware technology sold by FinFisher against activists in Mexico. That concern was reinforced by Privacy International's 2013 report, The Right to Privacy in Mexico, revealing that between 2011 and 2012, the Mexican Department of Defense had bought surveillance technology for USD 350 million.[30] But the lack of transparency by the Mexican government nor army never clarified details of such purchases and how these tools were being used.

Further inquiries from civil society and involvement of different government institutions regarding the use of FinFisher in Mexico is detailed in Hivos and APC's report "Global Information Society Watch 2014" where they highlight that in June 2013 Mexican civil society organizations ContingenteMX, Propuesta Cívica and Al Consumidor filled an inquiry to the National Access to Information Institute (IFAI) and asked the Ministry of the Interior for a detailed report on the government's strategy on digital monitoring and their privacy rights policies. The debate was also taken to the Mexican Congress who determined to also ask the Ministry of Interior if they had acquired the FinFisher software and asked the Office of the Mexican Attorney General whether there had been any complaint about the wiretapping of individual communications.

The main consequence after these inquiries was that a private company had bought the spyware technology on behalf of government institutions. IFAI imposed a fine of approximately USD $100,200 to the company for obstructing the IFAI's investigation by not providing the full information it requested. The "Global Information Society Watch 2014" report on Mexico highlights that "government espionage is a delicate issue because it is not always clear whether government authorities are acting to protect national security interests and whether they are going beyond their obligations and start infringing on citizens' human rights.[31]

In July 2015, WikiLeaks exposed hacked emails from surveillance vendor Hacking Team. That information revealed that the Mexican government was the top buyer worldwide with purchases of over 5.8 million Euros.[32] Further inquiries linked Hacking Team malware purchases to a wide diversity of Mexican government offices, the vast majority were not legally authorized to buy and use surveillance technology.[33] The Mexican Minister of Interior tried to link Hacking Team purchases to the

[29] See full report: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf
[30] See full report: http://catedraunescodh.unam.mx/catedra/EPU/images/stories/Informes_Pendientes/21-%20PI.pdf
[31] See full report: http://giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf
[32] See leaked source: https://wikileaks.org/hackingteam/emails/
[33] See Hacking Team activity in LATAM in Derechos Digitales Surveillance Report: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

previous administration even though records show that payments were done in both administrations, even after the was a presidential change.[34]

As much of top-end surveillance technology, Hacking Team's products are technically very difficult to detect, assess and track. One visible case of illegal use of such malware was flagged in the state of Puebla where it was identified as the source for surveillance against local independent journalist and political opposition.[35]

As pointed out earlier in this letter, in CitizenLab's report of August 24th 2016, the use of spyware from israeli cyber-ware company NSO Groups technically details how the Trident iOS exploit had been used to infect with the highly intrusive Pegasus malware the phones of UAE Human Rights Defender Ahmed Mansoor. The report highlights a similar attack to Mexican investigative journalist Rafael Cabrera, renowned for reporting the multi-million dollar scandal of the conflict of interest involving the President and First Lady of Mexico known as *La Casa Blanca*.[36]

In late 2016, Mexican digital rights specialists R3D published an in-depth report on surveillance in Mexico which analyzes current legislation, judicial interpretations and reflexions based on the known surveillance practices in the country. This report is based on an extensive access to information exercise and an thorough analysis on the Mexican legal framework.[37] They conclude that:

1. The Mexican legal framework lacks democratic controls enabling government authorities to surveil anyone without controls, transparency or accountability
2. Most surveillance actions have been done without any judicial authorization and / or control
3. The known use of surveillance activity has not delivered penal outcomes as most cases of surveilled people are not sent to trial
4. Access to information and transparency mechanisms are not useful in practice do to the government's resistance to open information on surveillance and when information was granted by government authorities, judges and companies it was found to be incomplete or even contradictory.

[34] See reporting by Animal Político: http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/
[35] See reporting by Animal Político: http://www.animalpolitico.com/2015/07/el-gobiernode-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/
[36] See CitizenLab Report https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ and investigative journalism revelations http://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/
[37] See full report: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf This report was done with suppor of Internews, OSF and Privacy International

ANNEX 3 - MEXICAN CONTEXT ON HUMAN RIGHTS, VIOLENCE AND FREEDOM OF EXPRESSION

The illegal surveillance against Mexican civil society, journalists, academia and human rights advocates is engraved under Mexico's increasing corruption, impunity, violence and human rights violations. Despite the legislative reforms and institutional progress, Mexico's civic space continues to shrink as it lacks to guarantee safe, open and reliable institutional support for its citizens.

In April 2015, the General Transparency and Access to Public Information Law was published strengthening 2002's legislation as it increased access to information guarantees and its applicability beyond the executive branch of government. Furthermore, the National Institute for Access to Information and Personal Data Protection (INAI) gained the power to intercede unconstitutional actions against laws that threaten or limit the access to information and personal data protection rights.[38] This reform gave INAI constitutional autonomy making its decisions definite and unassailable.

Nevertheless, several laws criminalize citizens that search for information have been set especially when inquiries are being done over public officers or addressed what can be vaguely identified as "national security".[39] Many access to information requests that have been appealed as they oppose international standards and conventions, especially those aiming for transparency in grave human rights violations and corruption. For instance, INAI recently reserved information regarding the Odebrecht-Pemex corruption case.[40] There are 20 restrictive legal law initiatives and four operational laws associated with crimes against honor, anti-protest and even, against the publication of memes.[41]

Regarding accountability, in April 2015 constitutional reforms were passed to create the National Anticorruption System (SNA) which should coordinate and homolgate actions and policy in three government levels (federal, state and municipal) in the prevention, detection and sanction of corruption cases. Nevertheless, the implementation of this policy has been delayed by the Legislative and to this date it still lacks the nomination of the country's Anticorruption Prosecutor. Nevertheless, Mexico has continuing falling places reaching in 2017 the 135th position in Transparency International 2017's Corruption Perception Index.[42]

Mexico is in a severe violence and security crisis, and the lack of any institutional progress significantly worsened by the lack of access to justice and a state of almost total impunity. Seventeen states of the country, that is, more than half are in red hot spots for high-impact crimes. Baja California Sur, Colima, Zacatecas, Guanajuato, Querétaro, Aguascalientes and Tabasco stood out this year due to the levels of insecurity that they registered. In a rate per 100,000 inhabitants, they are located in the top 5 places of homicide, kidnapping, extortion and robbery.

In human rights matters, the constitutional reforms of 2011 recognized the government's obligation to comply to international human rights principles and laws. Nevertheless, civic space and its three core liberties (association, expression and assembly) have reduced in the past years. The National

[38] The current general law now identifies political parties, labor unions, public trust funds and other fund management organizations, the executive, legislative and judicial branches of government and institutions and people that recieve or spend public resources or participate in public actions.
[39] See Article19's analysis on criminalization of citizen information requests: https://eljuegodelacorte.nexos.com.mx/?p=5740
[40] More information on INAI's ruling of the Odebrecht-Pemex access to information case: http://www.economiahoy.mx/energia-mexico/noticias/8481476/07/17/El-INAI-reserva-la-informacion-del-caso-OdebrechtPemex.html
[41] See Article19 assessment on restrictive laws in Mexico: https://mapa.articulo19.org/#!/principal/2017/
[42] See full report: https://www.transparency.org/news/feature/corruption_perceptions_index_2017

Resistry for Disappeard Persons (RNPED) accounts for 33,482 disappearances.[43] According to Article19, 111 journalists have been murdered since 2000 of which 38 journalist murders have been committed within the current government administration and reaching an impunity rate of over 99%. Additionally, aggressions against journalists have increased by 23% only in 2017 making it the most mortal year against the press.[44]

Freedom of assembly is constantly attacked as it's common to witness break-ins of strategic offices and spaces, threats and attacks against human rights advocates, the increase and lack of derogation of restrictive laws, public shaming of civil society organizations and human rights advocates, as well as targeted civil society organizations are being restricted to become registered charities. In Mexico, there is a daily attack against a human rights advocates, leaders and CSO personnel.[45] In peaceful gatherings, illegal use of force such as tear gas, use of metal bourne weapons, police encapsulation, and illegal incarceration against protesters have been used.

Furthermore, the government has increased military involvement in public safety responsibilities increasing violence and human rights violations maintaining opacity and lack of accountability. In December 2017, the Interior Security Law was bluntly passed which enables the President to authorize military intervention in police duties when "interior security threats" are identified and the federal or local capacities are insufficient to address "the threat". The law was passed despite national and international opposition including the United Nations High Commissioner for Human Rights, over 250 Mexican civil society organizations and academics, the INAI, the National Human Rights Commission, all State Human Rights Commissions and the majority of the state Access to Information Councils.[46] The unconstitutionality of this law is currently being appealed in the Supreme Court.

[43] More detail with focus on forced disappearances, extrajudicial executions, torture, access to justice, violence against the press and human rights advocates is available on the Interamerican Human Rights Council's report. See http://www.oas.org/es/cidh/informes/pdfs/mexico2016-es.pdf
[44] See Article19's latest report on violence against freedom of the press in Mexico: https://articulo19.org/informesemestral2017/
[45] See: http://www.proceso.com.mx/513092/en-mexico-ataque-al-dia-contra-defensoras-derechos-humanos-rnddhm
[46] See: www.seguridadsinguerra.org and https://www.forbes.com.mx/organizaciones-alrededor-del-mundo-declaran-en-contra-de-la-ley-de-seguridad-interior/