Call for Submissions: The Surveillance Industry and Human Rights

The acquisition and abuse of private surveillance technologies in Latin America

Introduction

The fundamental rights to freedom of opinion and expression are intimately intertwined with the exercise of the right to privacy. As such, state surveillance has a considerable impact on these rights. Especially, taking into consideration its potential to provoke a chilling effect on the online expression of any individual, which may derive in the predominance of self-censorship out of fear of being constantly monitored or tracked.[1]

As the UN Special Rapporteur has already recognized, "surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children.[2] The capacity of surveillance to produce such a disproportionate impact becomes particularly relevant considering that, in recent years, there has been an increased acquisition and use of commercial surveillance by States in Latin America, often without adequate safeguards in place which has resulted in several cases of abuse, particularly against human rights defenders, journalists and activists.

This trend is especially worrisome taking into account the rooted context in the region, derived from a tradition of long-standing dictatorships and armed conflicts, of systematic and generalized human rights violations, implying recourse to unclear and disproportionate data collection and surveillance mechanisms, all within a predominant culture of lack of transparency, corruption and impunity.

Accordingly, nowadays the exercise of surveillance practices in Latin America has not been in line with a comprehensive human rights approach, comprising the appropriate control mechanisms and safeguards against abuse. The lack of such an approach has given rise to the infringement of the rights to privacy, freedom of expression and freedom of peaceful assembly, thus undermining the basis of democracy, of institutions and of the overall respect for the rule of law.

---

[1] General Assembly, Human Rights Council. (May 22, 2015) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Available in: https://undocs.org/A/HRC/29/32

[2] General Assembly, Human Rights Council. (May 11, 2016) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. p.8. Available in: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement

Bearing in mind the above, along with the rise of the surveillance industry and the intrusiveness and sophistication of the technology used, the existence of appropriate legislation to limit, regulate and control the exportation, acquisition and deployment of commercial surveillance tools becomes essential.

Nevertheless, to date there is an overall lack of clear, precise, unambiguous and detailed laws, administrative regulations, judicial decisions and/or other policies to regulate the export, import and use of surveillance technology in the region. For example, only Argentina and Mexico are participating states in the Wassenaar Arrangement, although this hasn't had any meaningful effect in those countries either.[3] This scenario does nothing more than promote or, to say the least, fails to prevent the misappropriation of public funds to acquire surveillance technology, the usage of pervasive surveillance technologies by private sector itself or in partnership with the public sector, nor the abuse of this technologies against the civilian population, including journalists and human rights defenders.

1. Information concerning the use of surveillance technologies developed by private companies in Latin America

According to a report from Privacy International, the top five countries who host surveillance companies are the United States, the United Kingdom, France, Germany, and Israel.[4] Notably, during recent years at least three of them, either directly or through companies headquartered in their territory, have demonstrated a strong presence in the region with respect to State negotiations for the acquisition of surveillance technologies.

China is also likely to be added to this list. At least for the new far-right Brazilian government, the country have been mentioned as reference and visited for the purpose of doing business on the sector. In late January, 12 congressmen from the far-right's Brazilian President Party (PSL) went on an official mission to China in order to check out Chinese facial-recognition technology, with a view to maybe use it in Brazil to combat crime[5]. The mission was later revealed to be paid by the Chinese Government. Cities like Rio de Janeiro already count with the technology in buses, streets and Drones.

---

[3] Kimball, Daryl. (December 11, 2017) *The Wassenaar Arrangement at a Glance*. Available in: https://www.armscontrol.org/factsheets/wassenaar

[4] Privacy International. (July 2016) *The Global Survaillance Industry*. p. 5. Available in: https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

[5]Association Free Press. (January 18, 2019) *Brazil lawmakers' trip to China stirs anger*. Daily Mail. Available at: https://www.dailymail.co.uk/wires/afp/article-6608275/Brazil-lawmakers-trip-China-stirs-anger.html

In Argentina, for example, the Ministry of Defense signed a contract amounting to US$ 5.2 million with its counterpart from Israel, for the provision of cyberdefense and cybersecurity services. Also, in Colombia, every year a trade show and conference, sponsored by the Government of Israel, is hosted to exhibit mainly surveillance products from the latter.

Moreover, the Israeli-American company Verint Systems Ltd, the Israeli sister company to the US-headquartered Verint Systems Inc, provided to Colombia critical interception infrastructure, as well as NICE Systems, Pen-Link and Palantir from United States, Smith Myers, Network, Critical and Komcept from the United Kingdom and Exfo from Finland.[6] Another example is the case of Chile, where a German parliamentary inquiry revealed Chile had entered into negotiations with the German government for the acquisition of surveillance technologies and the company Global Systems Chile SpA, affiliated to the Israeli company Rebrisa, has sold surveillance balloons to the commune of Las Condes in the province of Santiago.[7] Also in Chile, the law enforcement police acquired in 2015, malware from Hacking Team with the declared purpose of using it as a support tool to obtain customer's IP data and access information that will not be obtained through a court order.[8]

It has been revealed that countries like Mexico and Panama have acquired an extremely sophisticated and intrusive malware, commercialized exclusively to governments by the Israel-based company the NSO Group, called “Pegasus”[9], which allows its operators to obtain absolute access and control over the devices where it is deployed, making it possible to activate their camera, microphone, geographic location and to record keyboard inputs, keyboard, etc.

Moreover, in Argentina, Mexico, Brazil, Chile[10], Colombia[11], Ecuador, Honduras and Panama, diverse authorities, many of them not authorized legally to carry out surveillance tasks, have acquired a powerful, sophisticated malware commercialized by the Italian company Hacking Team. Other countries like Argentina, Peru,

---

[6] Privacy International. Demand/Supply: Exposing the Surveillance Industry in Colombia. Available at: https://privacyinternational.org/sites/default/files/2017-12/DemandSupply_English.pdf

[7] Privacy International. *State of Surveillance for: Argentina, Colombia, Chile*. Available at: https://privacyinternational.org/state-privacy/28/state-privacy-chile

[8] Partarrieu. B y Jara. M. (10 de julio de 2015). Los correos que alertaron sobre la compra del poderoso programa espía de la PDI. CIPER. Available at: http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi

[9] Marczak, Bill & Scott-Railton John. (August 24, 2016) *The Million Dollar Dissident; NSO Group’s iPhone Zero-Days used against a UAE Human Rights Defender*. The Citizen Lab. Available at: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[10] Ver también: Violler, Pablo (February 1, 2019) *Operación Huracán. Cómo el gobierno de Chile ha dado rienda suelta a sus policías*. Derechos Digitales. Available at: https://www.derechosdigitales.org/11916/como-el-gobierno-de-chile-ha-dado-rienda-suelta-a-sus-policias/

[11] Fundación Karisma. (December 15, 2015) *So-called hacking does exist*. Available on https://karisma.org.co/police-has-hacking-tools-and-use-them/.

Paraguay, Uruguay, Venezuela and Guatemala also entered into negotiations with the company.[12]

Finally, it has been reported that countries like Mexico, Paraguay and Venezuela could be users of the FinFisher *malware,* from the UK company Gamma Group International.[13]

All those companies continue to sell and target the region for business. Since the announcement of being host of Mega-Events such as the World Cup and the Olympics, Brazil became a huge market of surveillance technologies[14], annually hosting regional surveillance fairs such as LAAD Defense and Security, hosting companies such as Hacking Team, Cellebrite, Gamma International and others already recognized for selling pervasive surveillance technologies. Hacking Team, which became famous after a major leak of internal emails in 2015 revealed that the company had business with several countries in Latin America,[15] also had negotiated a trial version of it's malwares with the Brazilian Federal Police.[16] But, even after this scandal, the company continued to expose it's technologies in LAAD.

It is also common that Israel have a whole separate pavillion in LAAD, specially dedicated to negotiate their surveillance technologies with attendees from the region. The tactics seems effective, among other equipments, Brazil had already acquired several israeli drones.[17] A closer proximity among both Brazilian and Israeli governments, particularly focused on exports of surveillance technologies,[18] was also announced last January, in the inauguration day of president Bolsonaro, with Israeli Prime Minister attending the ceremony.[19] Weeks after, the Prime Minister sent

---

[12] Pérez de Acha, Gisela. (March 2016) *Hacking Team Malware para la vigilancia en América Latina*. Derechos Digitales. Available at: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

[13] Marckzak, Bill, Scott-Railton John, Senft Adam, Poetrand ,Irene mckune Sarah. (October 15, 2015) *Pay No Attention To The Server Behind The Poxy; Mapping FinFisher's Continuing Proliferation*. The Citizen Lab. Available at: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

[14] Coding Rights. Megaeventos: Um legado de vigilancia. (*Legado Vigilante)*. Available at: https://legadovigilante.codingrights.org/

[15] Pérez de Acha, Gisella. (March 2016) *Hacking Team Malware para la vigilancia en América Latina*. Derechos Digitales. Available at: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

[16] Oficina Antivigilancia. *(July, 2015).* Hacking Team é hackeada e tem seus documentos vazados. Available at: https://antivigilancia.org/pt/2015/07/hacked-team/

[17]Coding Rights. Megaeventos: Um legado de vigilancia. (*Legado Vigilante)*. Available at: https://legadovigilante.codingrights.org/

[18] Montesanti, Beatriz. (December, 2018). *Estados brasileiros negociam tecnologia de segurança e de água com Israel.* Uol Notícias. Available at: https://noticias.uol.com.br/internacional/ultimas-noticias/2018/12/13/estados-brasileiros-negociam-tecnologia-de-seguranca-e-de-agua-com-israel.htm

[19] BBC Brazil. (December, 2018). *Governo Bolsonaro: Qual é o impacto da presença do premiê israelense Benjamin Netanyahu na posse?* Available at: https://www.bbc.com/portuguese/brasil-46685876

Israeli military forces and non-fitted[20] technology to try to assist in the social-environmental catastrophe caused by the mining company Vale S.A. in Brumadinho.

It is important to mention that private companies are also deploying very pervasive surveillance technologies against latin american citizens. In Brazil, Vale S.A. is alleged responsible for surveilling land rights defenders and environmental activists, as well as journalists and it's own workers in order to avoid denounces of several human rights violations and social-environmental impact that occur in their businesses.[21] That is the case of other companies as well, such as Anglo American, another mining company accused to surveil and threat citizens of Conceição do Mato Dentro,[22] where the company is being exposed by community leadership who are critical about the construction of a giant dam.[23] Part of these citizens had to request to be part of the national program to protect human rights defendants.[24] In Chile, last November, a shopping center chain implemented facial recognition cameras to monitor its visitors. The company announced that the processing is being supported by the police, without any further legal authorization for it.[25] Therefore, it is of ultimate importance that we see companies as both sellers and deployers of surveillance technologies, as well as consider the different rationales for legality, limits and levels of responsibilities that these practices entails.

And, even more complicated is to note that, besides selling or deploying surveillance technologies as their own business, companies are also entering into partnerships with governments to implement such systems, normally with the argument of security, innovation and "smart cities". As governments from the region normally do not handle the massive databases these surveillance systems produce. In this sense, companies such as IBM, Cisco and Microsoft have played an important role.

---

[20] Valente, Rubens. (January, 2019). *Equipamentos de israelenses não são efetivos para as buscas, diz chefe do resgate.*Folha de São Paulo. Available at: https://www1.folha.uol.com.br/cotidiano/2019/01/equipamentos-de-israelenses-nao-sao-efetivos-para-as-buscas-dizem-bombeiros.shtml

[21] Pozzebom, Elina Rodrigues. (October, 2013). *Vale espiona líderes e se infiltra em movimentos sociais, diz ex-funcionário.* Senado Noticias. Available at: https://www12.senado.leg.br/noticias/materias/2013/10/24/vale-espiona-lideres-e-se-infiltra-em-movimentos-sociais-diz-ex-funcionario

[22]Sant'anna, Daniel. Maciel, Alice. (March, 2018). A*GRESSÕES, VIGILÂNCIA, DESEMPREGO, PERSEGUIÇÃO E ISOLAMENTO: COMO VIVEM OS MORADORES QUE ENFRENTAM A GIGANTE DA MINERAÇÃO. Intercept Brasil. Available at:* https://theintercept.com/2018/03/27/ameacas-moradores-mineracao-anglo-american/

[23] Ferraz, Lucas. (January, 2018). Anglo American quer barragem quatro vezes maior que a de Fundão, que rompeu em Mariana. Pública. Available at: https://apublica.org/2018/01/a-sombra-da-tragedia-de-mariana-video/

[24] Ministry of Human Rights of Brazil. Programa de Proteção aos Defensores de Direitos Humanos. Available at: https://www.mdh.gov.br/navegue-por-temas/programas-de-protecao/ppddh-1/sobre-o-ppddh

[25] Delgado, Felipe (November, 2018).Polémica por instalación de cámaras de reconocimiento facial en mall capitalino. Available at: https://www.biobiochile.cl/noticias/nacional/region-metropolitana/2018/11/11/polemica-por-instalacion-de-camaras-de-reconocimiento-facial-en-mall-capitalino.shtml

For instance, the Mega-events also pushed for the creation of new institutions to support the public security, such as the Integrated Centers of Command and Control (CICC) and the Integrated System for Command and Control (SICC), [26] IBM was the company chosen to implement the technology of these Centers which monitor and collect data of entire cities, through cameras and other inputs.

In Paraguay, the Ministry of Interior was responsible for the purchase of national security face recognition software in 2018. The software was lately installed in the capital downtown[27] as well as in football stadiums[28]. The official argument is that they wanted to offer higher security in crowded areas.

In Brazil, the implementation of facial recognition technologies has also been growing in the past years under the narrative of security, but also for "innovative" business purposes. For instance, it is being announced that the State of Rio will partner with the telecommunications company Oi Telecom to deploy a test of facial recognition cameras in the neighborhood of Copacabana during the Carnaval.[29] In 2018, Via Quatro, the number one concession holder of São Paulo Metro's Line, also installed a set of interactive platform doors that display ads and information in three stations. The same platform doors use sensors with screens and facial recognition technology to monitor the reaction of viewers to the displayed ads.[30] The doors were part of an experimental project with LG, a multinational electronics company, which provided the screens, and Hypera Pharma, a large Brazilian pharmaceutical company.

Beyond facial recognition technologies, in 2014 Venezuelan government implemented a biometric system that requires the fingerprint enrollment of any citizen to buy food and medicines at regulated prices in order to address supplies constrictions and avoid speculation with basic goods. The database was initially populated with data coming from Electronic Vote system, so there is a legitimate concern in how the information about voting could be used to restrict access to supplies. There is no evidence in how that database is being used or secured by

---

[26] Mota, Jéssica et al. (September, 2013). *Com a Copa, Brasil vira mercado prioritário da vigilância.* Pública. Available at: https://apublica.org/2013/09/copa-brasil-vira-mercado-prioritario-da-vigilancia/

[27] Biometría y video-vigilancia en Paraguay. TEDIC (July 11, 2018) https://www.tedic.org/biometria-y-video-vigilancia-parte1/

[28] La inteligencia artificial como aliada en la cruzada antiviolencia (January 12, 2019) https://www.hoy.com.py/deportes/la-inteligencia-artificial-como-aliada-en-la-cruzada-antiviolencia

[29] Do Brasil, Cristina Indio. (January, 2019). *Rio: programa de reconhecimento facial entra em operação no carnaval. Agência Brasil.* Available at: http://agenciabrasil.ebc.com.br/geral/noticia/2019-01/rio-programa-de-reconhecimento-facial-entra-em-operacao-no-carnaval

[30] Amigo, Ignacio. (May 8, 2018) *The Metro Stations of São Paulo That Read Your Face*. Citylab. Available at: https://www.citylab.com/design/2018/05/the-metro-stations-of-sao-paulo-that-read-your-face/559811/

government or with who else is shared. This system started as voluntarily but quickly became mandatory.[31]

Drones are also on the agenda of public officials. In Rio de Janeiro, programme "Sentinela Carioca" imposes the use of drones to monitor "crowded places and large events"[32]. The program allows drones to be flying over the capital of Rio de Janeiro, collecting information from cars, buildings and, of course, people - which can jeopardize the citizens' right to privacy and informational self-determination. One possible application to the RPAs (Remotely Piloted Aircrafts) would be for monitoring traffic and eventually collecting data on vehicle registration plates, but the purpose of which the images will be collected is still unknown. The most noteworthy assignment to the program is the one related to supervision of communities and favelas and it could also tracking demonstrations and activists who participate in any activity in a public place (the collected information can be crossed-over with the already existing archives in intelligence centers and police forces about activists). Using such technologies without the necessary guarantees of transparency and regulation opens space for other rights to be violated. In Chile, during recent years, different local authorities in Santiago province have implemented the use of unmanned spacecraft - such as surveillance balloons and drones - equipped with high resolution cameras in massive surveillance programs intended to provide public safety.[33] In the same lines drones have been used to constantly surveil and repres indigenous communities in the south of the country in recent years.[34]

The acquisition and use of these increasingly powerful and silent surveillance technologies constitute a particularly serious interference with the privacy of the individuals targeted and pose a significant difficulty for oversight and accountability. Notwithstanding, no country in the region has specific regulations with regard to the use of these unprecedentedly invasive tools.

2. Information concerning the lack of transparency behind the acquisition of commercial surveillance technologies.

Most, if not all, of the surveillance technologies developed by private companies highlighted above have been negotiated and acquired by Latin American States

[31] Díaz, Marianne. Sistema Biométrico y Carnet de la Patria: Más control y menos acceso (June, 2017) Available at: https://www.derechos.org.ve/actualidad/sistema-biometrico-y-carnet-de-la-patria-mas-control-y-menos-acceso

[32] Tamari, Mariana. (November, 2018) *Em dezembro, sem saber, estaremos "dando close" para drones sentinelas.* Carta Capital. Available at: https://old01.cartacapital.com.br/blogs/intervozes/em-dezembro-sem-saber-estaremos-201cdando-close201d-para-drones-sentinelas

[33] K. González and D. Aguayo. (April, 2017). Las Condes inicia vigilancia con drones. Available at: https://www.latercera.com/noticia/las-condes-inicia-vigilancia-drones/

[34] Barreno J. (24 de enero de 2014). Las comunidades mapuches denuncian el uso de drones espía en sus tierras. El Mundo. Disponible en: http://www.elmundo.es/internacional/2014/01/24/52e20330e2704e1f188b456b.html

under opaque and irregular procedures. There is an overall lack of transparency regarding these procedures under the pretext of "national security", hence most information regarding these acquisitions has been made public by whistleblowers, media reports and civil society investigations.

For example, in the case of Mexico and its acquisition of the *malware* Pegasus from NSO Group, it has been revealed that the acquisition was made through an intermediary company that didn't have any prior history of commercializing surveillance tools and that was founded by a former employee of the General Prosecution Office.

Moreover, it has been revealed that the registered address of the company does not correspond to any actual office of the company and the people registered as founders of the company claim to have no knowledge of the companies activities, which suggest they only acted as frontmen.[35]

Another important example would be the approval of Law n.13.097/2015[36] in Brazil. The legal text amended the Criminal Organizations Law relativizing the rules for hiring specialized technical services, acquisition or leasing of equipment for the judicial police for the tracing and obtaining evidence. This alteration, not only exempted bidding for hiring such services but also waived publication in the official press of the summary of hirings done under this regime - therefore turning this kind of expense less transparent. The above mentioned alteration to the Criminal Organizations Law is rumoured to have made possible the trail of malware from Hacking Team to the Federal Police.[37]

3. Details of emblematic cases of State use of private surveillance technology against individuals or civil society organizations.

There have been several cases throughout Latin America which demonstrate that the deployment of surveillance technologies by law enforcement agencies, thus far, has known no boundaries nor appropriate controls.[38] Especially, considering there has been diverse well-documented cases of State abuse of private surveillance technologies, with no apparent legal justification or judicial authorization, against

---

[35] Olmos, Raul. (20 Febrero 2017) *Subordinado de Murillo Karam, ligado a grupo empresarial que vendió Pegasus a la PGR*. Mexicanos Contra la Corrupción y la Impunidad. Available at: https://contralacorrupcion.mx/pegasus-pgr/

[36] Presidencia da República. Lei n. 13.097, de 19 de janeiro de 2015. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13097.htm

[37] Coding Rights. Megaeventos: Um legado de vigilancia. (*Legado Vigilante)*. Available at: https://legadovigilante.codingrights.org/

[38] Becker, Sebastián, Lara, Carlos, Canales, María Paz. (Septiembre 2018) *La Construcción de Estándares Legales para la Vigilancia en América Latina; Parte I: Algunos Ejemplos de Regulación Actual en América Latina*. Available at: https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-I.pdf

activists or civil society groups particularly critical or inconvenient to the interests of people in power.

For example, in Mexico, as it was previously mentioned, it has been well documented that the extremely sophisticated and intrusive malware, commercialized by the Israel-based company NSO Group, called “Pegasus”, has been used to target journalists, human rights defenders, lawyers, public health and anti-corruption activists as well as the international body of independent experts appointed to investigate the disappearance of the 43 students from Ayotzinapa in 2014.[39]

In June 2017, the seriousness of the case drove diverse UN Special Rapporteurs to call upon Mexico to establish an independent and impartial investigation into the deployment of Pegasus.[40] This has also been a reiterated demand from the victims. Nevertheless, to date, the outgoing and entering governments have failed to recognize the establishment of guarantees of such an investigation and the ongoing criminal proceedings have shown little to none progress; not to mention that no proceedings have been installed to investigate and prosecute the clear indications of corruption behind the acquisition of this *malware*.

Along the same lines, in Panama, a criminal proceeding has been established against former President for his role in the communications surveillance committed with the Pegasus malware against approximately 150 individuals, including journalists, businessmen, civil society leaders and members of the opposition.[41] It has been estimated that between 2009 and 2014, Ricardo Martinelli acquired

---

[39] Artículo 19, Citizen Lab, R3D: Red en Defensa de los Derechos Digitales, SocialTIC. (junio 2017) *Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México.* Disponible en: https://r3d.mx/gobiernoespia/ ; R3D. Destapa la Vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. Disponible en: https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/ ; Perlroth, Nicole (11 de febrero de 2017) Spyware’s Odd Targets: Backers of Mexico’s Soda Tax. The New York Times. Disponible en: https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?smid=fb-share&_r=0 ;Ahmed, Azam. Perlroth, Nicole. (June 19, 2017) *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families.* The New York Times. Disponible en: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html ; Ahmed, Azam. (August 30, 2017) Un empresario activista lucha contra la corrupción en México y se convierte en un blanco del Estado. The New York Times. Disponible en: https://www.nytimes.com/es/2017/08/30/mexico-pegasus-claudio-x-gonzalez-laporte-enrique-pena-nieto-corrupcion/ ; Ahmed, Azam. (July 10, 2017) Spyware in Mexico Targeted Investigators Seeking Students. The New York Times. Disponible en: https://www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-pegasus-spyware.html

[40] United Nations Human Rights: Office Of The High Commissioner (July 21, 2017) *Mexico: UN experts call for an independent and impartial investigation into use of spyware against rights defenders and journalists*. Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892

[41] Bonífaz, R and Delgado-Ron, A. (January 31, 2018) Verified cases of unlawful use of surveillance software by Latin American Governments 2015-2016, PUCE Magazine, ISSN: 2528-8156, p. 315-333

surveillance technologies for 13.5 millions of dollars from the companies M.L.M. Protection Ltd. and NSO Group.[42]

Also, in 2017 the carabineers from Chile announced that eight members of the *mapuche* community had been detained within the implementation of the intelligence operation denominated "*Operación Huracán*". Remarkably, however, the incriminatory evidence used against these members pertained to the exchange of private communications through WhatsApp. In this regard, even though WhatsApp is an encrypted messaging application, and it was not technically possible for the law enforcement agents to access said private communications, they try a combination of phishing software to get access to the cloud backup of messages of some of the leaders implied in the case, in order to fabricate evidence that later allows them to get fraudulently a court order to seize the devices of the leaders and then implant on them incriminatory fake messages. The lack of oversight over law enforcement officers actions result particularly concerning considering, as it was previously mentioned, that the Investigations Police (PDI for its acronym in Spanish) had acquire the malware *Phantom* from the Italian firm Hacking Team, with the stated purpose of "obtaining information for which access would not be granted by means of a judicial order."[43] The lack of transparency and information available in relation to how, when and why this *malware* has been deployed makes it reasonable to conclude so.

Brazil is currently facing an increase in surveillance practices against social movements. The Mega-events sparkled discussions aimed at the expansion of intelligence and surveillance powers. As a result, the approval of the Criminal Organizations[44] and Counter-terrorism[45] laws increased the legal permissions for the Brazilian State to deploy monitoring and intelligence mechanisms in a very questionable way, particularly in a context in which State abuses and violations were already common. For instance, from 2005 until 2015, the Brazilian Institutional Security Office (GSI) and the Brazilian Intelligence Agency (ABIN) administered a database called GEO-PR.[46] Theoretically constituted for the sole purpose of protecting indigenous territories, small farmers' lands and the environment through data gathered by public agencies, the database ended up also allowed for

---

[42] Acento (June 13, 2017) *Cronología del caso de escuchas en Panamá por el que detienen a Ricardo Martinelli en EEUU.* Available at: https://acento.com.do/2017/actualidad/8465768-cronologia-del-caso-escuchas-panama-detienen-ricardomartinelli-eeuu/

[43] Garay, Vladimir. (September, 28 2017) *Poco y nada (o cuánto sabemos realmente sobre cómo nos vigilan)*. Derechos Digitales. Available at: https://www.derechosdigitales.org/11446/poco-y-nada-o-cuantosabemos-realmente-sobre-como-nos-vigilan/

[44] Presidência da República do Brasil. Lei n. 12.850, de 2 de agosto de 2013. (Lei de Organizações Criminosas). Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

[45] Presidência da República do Brasil. Lei n. 13.260 de março de 2016. (Lei Antiterrorismo). Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm

[46] Figueiredo, Lucas. (December, 2016). O Grande Irmão: Abin tem mega-banco de dados sobre movimentos sociais. Intercept. Available at: https://theintercept.com/2016/12/05/abin-tem-megabanco-de-dados-sobre-movimentos-sociais/

monitoring NGOs, mobilizations, strikes and demonstrations that occurred in the country. The program was resumed over the course of 2015, but the database was donated to the Brazilian Intelligence Agency. Under Bolsonaro government, all these tools and permissions tend to be even more threatening, as the president himself promised to "end with activism in Brazil". Indeed, one of this first actions was an executive order[47] commanding the office of the Government Secretary to “supervise, coordinate, monitor and accompany the activities and actions of international organizations and non-governmental organizations in the national territory”.

4. Information regarding the impunity and overall lack of accountability regarding the abuse of private surveillance technologies

Despite the seriousness of the cases of abuse that have been mentioned, most of this cases have not been properly investigated nor prosecuted and there is an overall lack of accountability for the irregular acquisition of private surveillance technology and the abuse of said tools against civil society, including journalists and human rights defenders.

For example, impunity prevails regarding the abuse of the *Pegasus* malware in Mexico against several journalists, human rights defenders and activists. An important factor for this situation is the fact that the primary suspect of being behind the attacks is the same institution in charge of the official criminal investigation. In this regard, a major obstacle for accountability has been the lack of legal and/or political independence by the authorities in charge of investigating the cases of abuse.

The lack of regulations and protocols regarding the use of sophisticated surveillance tools like the *Pegasus* malware has also created obstacles for the accountability of the institutions that use these technologies. For example, in Mexico, the General Prosecution Office (PGR) has claimed that it does not have a record of the people that has been targeted with the *Pegasus* malware and has denied the existence of any logs or any way to audit the use of these tools.

Likewise, even though the company NSO Group has made public statements in which it has claimed that when cases of abuse are reported, it conducts an internal investigation and it suspends the relationship with the abusive client, it has been documented that targeting of journalists happened even months after cases of abuse

[47] Presidência da República do Brasil. Medida Provisória nº 870, de 1º de janeiro de 2019. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Mpv/mpv870.htm

had been already been made widely publicized.[48] Also, despite being requested to cooperate with the official criminal investigation, it has not provided any type of assistance to the official investigation.

The lack of public information with regards to the deployment of such technologies is also worrisome. In the example of the use of drones to monitor the city of Rio de Janeiro, some of the information obtained about the program was through access to information requests[49] that revealed some level of disregard for the citizens privacy with the massive collection of data that the program promotes. But overall, it is very hard to get any detailed information about deployments and safeguards in the usages of such technologies and about abuses.

Additionally, prosecutors lack the knowledge, expertise and/or resources to carry out investigations into suspected abuse of surveillance technologies. In some occasions, as in the case of Mexico, prosecutors are denied access to crucial information under the pretext of national security, which represents a serious obstacle for access to justice.

Lastly, the usage of pervasive surveillance technologies represents a direct infringement of human rights. Therefore, it is of utter importance for companies and states to continue to build up on the work of the U.N. Guiding Principles on Business and Human Rights[50] and also the U.N. Human Rights Council's open-ended intergovernmental working group on transnational corporations and human rights[51], especially with regards to the development of a legally binding treaty on business and human rights whose scope of application considers transnational and domestic companies at the same level. Such provision would allow companies such as Hacking Team to be held accountable for providing services known to promote Human Rights abuses through state surveillance[52].

In light of all of the above, the signing organizations propose the following:

---

[48] Marczak, Bill, Scott-Railton John, Mckune ,Sarah, Razzak, Bahr and Deibert Ron. (September 18, 2018) *Hide and Seek; Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. The Citizen Lab. Available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[49] Tamari, Mariana. (November, 2018) *Em dezembro, sem saber, estaremos "dando close" para drones sentinelas.* Carta Capital. Available at: https://old01.cartacapital.com.br/blogs/intervozes/em-dezembro-sem-saber-estaremos-201cdando-close201d-para-drones-sentinelas

[50] United Nations Human Rights Council. *UN Guiding Principles on Business and Human Rights*. Available at: https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf

[51] United Nations Human Rights Council. *Open-ended intergovernmental working group on transnational corporations and other business enterprises with respect to human rights.* Available at: https://www.ohchr.org/en/hrbodies/hrc/wgtranscorp/pages/igwgontnc.aspx

[52] Oribhabor, Isedua. Micek, Peter. (January, 2019). *Four years to a first draft: slow progress toward treaty to bind companies.* Available at: https://www.accessnow.org/four-years-to-a-first-draft-slow-progress-toward-treaty-to-bind-companies/

1. Recommendations

a. To States

- Implement the appropriate regulatory framework to guarantee the transparency and accountability in the acquisition of surveillance technology.
- Implement the appropriate legislative framework to regulate and impose limits on the State usage of surveillance technology, which must include the establishment of necessary safeguards against abuse including:
    - Specific regulation on the use of surveillance tools like hacking, malware, drones as well as biometric technologies, which incorporates the principles of necessity and proportionality.
    - Independent judicial authorization and oversight mechanisms.
    - Regulations that ensure that the use of private surveillance technology is auditable by oversight bodies.
    - Transparency regarding the general surveillance capabilities of the State and meaningful information regarding the scope and extent of the use of private surveillance technology.
    - Ensure that individuals that are targeted with private surveillance technologies are eventually notified and have access to a remedy.
- Guarantee the existence of independent, impartial oversight bodies, endowed with the necessary powers to effectively audit, investigate and prosecute any abuse in the usage of surveillance technologies by State actors, this includes having absolute access to any information, installation or equipment necessary to carry out their functions;
- Adopt human rights due diligence measures in their acquisition of surveillance technologies in order to assess and monitor potential Human Rights abuses and/or violations offered by the deployment of such technologies.
- Monitor and impose appropriate penalties and guarantee the enforcement of those towards companies that deploy private surveillance technologies for their own business with the purpose of violating human and socio-environmental rights.

b. To companies that commercialize and deploy private surveillance technology

- Avoid causing or contributing to adverse human rights impacts from the deployment of the technologies they sell, and address such impacts when they occur;
- Seek to prevent or mitigate adverse human rights impacts that are directly linked to the deployment of the surveillance technologies they sell, even if they have not contributed to those impacts.

- Acknowledge their responsibility and role given the type of technology they provide and the consequences thereof, no matter their size, operational context, ownership and structure.
- Companies shall be only allowed to deploy surveillance technology tools if in partnership with public authorities, in accordance with necessary and proportionate principles, as well as with transparency and accountability measures and safeguards.
- Establish policies and processes that include:
    - A policy commitment to meet their responsibility to respect human rights, including conducting their own investigation of any alleged misuse of their products or services and terminating any contract whenever that happens to be the case;
    - A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights;
    - The availability of effective cooperation mechanisms with respect to any investigation into the acquisition or deployment of their products and services;
    - Remediation mechanisms for any adverse human rights impacts they cause or to which they contribute.

***

The signing organizations belong to “Al Sur”, a group of organizations from Latin America that aims at strengthening human rights in the digital environment.

This document has been signed on February 15th, 2019 by the following organizations:

- Asociación por los Derechos Civiles (ADC). Argentina. (adcdigital.org.ar)
- Coding Rights. Brazil. (codingrights.org)
- Derechos Digitales. América Latina. (derechosdigitales.org)
- Fundación Karisma. Colombia. (karisma.org.co)
- Hiperderecho. Peru. (hiperderecho.org)
- Instituto Brasileiro de Defesa do Consumidor (IDEC). Brazil. (idec.org.br)
- IPANDETEC. Panama. (ipandetec.org)
- Red en Defensa de los Derechos Digitales (R3D). México. (r3d.mx)
- TEDIC. Paraguay. (tedic.org)