The Surveillance Industry and Human Rights

Derechos Digitales' submission for the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Expression[1]

I. Introduction

The following report is a summary of the findings of Derechos Digitales (DD) with regards to the advancements in the acquisition and use of surveillance technologies, mostly by States, within the Latin American region. Although they are not intended to provide a complete view of the subject in Latin America, it is meant to provide some insights, as developed by DD's team, about the legal issues on surveillance industries, including its applicable regulatory frameworks. It is our understanding that the practice of surveillance creates a market of intrusive technologies, with governments and technology vendors as interested parties, and with the population under constant threat of being subject to intrusive measures, well beyond legitimate aims or without legal authority.

II. Regional context

In Latin America, state entities have begun to acquire different surveillance technologies, such as high definition cameras for deployment in public spaces, facial recognition systems, biometric scanners, unmanned aerial vehicles or "drones," surveillance balloons, malware, IMSI catchers, among other technologies. The excuse is often the need to ensure public safety, or the efficiency of policing systems.

However, these technologies are increasingly invasive, and can adversely affect fundamental rights. There have been plenty of calls from civil society organisations, as well as human rights defenders and journalists, raising alarm around the dangers arising from surveillance technologies, especially given Latin American history of political instability and authoritarian practices by governments. In this scenario, surveillance vendors do hold a responsibility as providers of invasive technologies by states. Legal frameworks to prevent an abusive exercise of investigative powers by the authorities are needed, in full compliance with international human rights law by both states and companies.

Just a few of the surveillance technology firms known to operate in Latin America are:

1) **Gamma International:** At the beginning of 2014, an initial report from Citizen Lab detected the presence of FinFisher, a surveillance malware sold exclusively to governments to intercept mobile communications, in countries as Mexico and Panama. A report from 2015 confirmed the malware's presence in Mexico, Venezuela and Paraguay.[2]
2) **Hacking Team:** The massive emails' leak from the Italian company Hacking Team, shed a light on the sales made by this surveillance firm in countries as Brazil, Chile, Colombia, Ecuador, Honduras, Mexico and Panama. "Remote Control System", Hacking Team's key product, is a malicious software presented to the user as a genuine and harmless software but when executed gives the attacker remote access to the infected device for both computers

[1] This report was prepared by María Paz Canales and J. Carlos Lara in February 2019, and was based on previous works by the authors, as well as Sebastián Becker, Marco Correa, and Paz Peña.

[2] Citizen Lab (2015). Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

or smartphones.[3] Hacking Team claims to have understanding of the "potential for abuse of the surveillance technologies" and asserts it is complying with international standards including the Wassenaar Arrangement protocols,[4] avoiding restrictions by arranging coöperation with states through intermediaries.

3) **M.L.M. Protection**: Israeli surveillance firm who sold long-range interception technology in 2010 to the government of Panama, enabling it to tap into computers and cellphones from a distance and record almost any content, including text messages and communications sent via applications such as WhatsApp and Blackberry Messenger.
4) **Digitro Tecnología Ltda.:** Brazilian company that sold a communications surveillance software named El Guardián (The Guardian) to the Uruguayan government. It is a system designed to monitor several networks, allowing up to 30 people to work simultaneously on mobile phones, landlines and emails.[5] Digitro also provided services in Brazil, under admission by the Brazilian Federal Police has admitted that they use the software to monitor social media.[6]
5) **The NSO Group**: an Israeli company that sells tools to governments to intervene in mobile phones, such as the "Pegasus" spyware, which exploits phone vulnerabilities to track its user and operate its camera. In 2016, links sent to exploit such vulnerabilities were sent to people working on public health issues.[7] The Mexican government had admitted in 2012 that it had signed a USD 20 million agreement with the NSO Group.

III. Surveillance practice: principles for lawful intrusion

Normative standards for lawful surveillance must consider international human rights law standards and principles, as well as the experience gathered in jurisprudence and principles developed by multiple stakeholders, including civil society organisations.[8] The application of such rules, however, must extend not only to communications surveillance, metadata retention or policing activities, but to those new practices that involve hacking, bodily surveillance, biometric data gathering, and any future form of data collection mediated by technology. These principles include:

1. **Legality**: basis in explicit legal authority for the development, acquisition, deployment, and use of intrusive surveillance technologies, as well as for its development and importation or exportation. Process, purposes, measures, requirements, probable cause, possible targets, and institutional authority must be stated by law.
2. **Necessity:** limitation of surveillance activities to what is strictly needed for a legitimate objective. Mere availability of low cost surveillance technology, or its offer by a vendor, does not justify acquisition or deployment.

[3] Gisela Pérez de Acha (2015). Hacking Team: malware para la vigilancia en América Latina. https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
[4] Privacy International (2015). Briefing for the Italian Government on Hacking Team https://privacyinternational.atavist.com/hackingteamsurveillanceexports
[5] Global Information Society Watch (2014). Penumbra: Surveillance, security and public information in Uruguay. https://www.giswatch.org/en/country-report/communications-surveillance/uruguay#_ftn11
[6] Convergencia Digital (2013). Exército usou software Guardião para monitorar redes sociais. http://wap.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34302&sid=11#.U5ZMmS9htb0
[7] CitizenLab (2017). Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links, https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/
[8] See, for instance, Necessary & Proportionate: International Principles on the Application of Human Rights to Communication Surveillance: https://necessaryandproportionate.org/es/necesarios-proporcionados

3. **Adequacy:** surveillance measures must be appropriate for the legitimate aim, and when no alternative means that are less restrictive of human rights are available for that purpose.
4. **Proportionality:** surveillance measures must be preceded by an analysis of the existence or likelihood of a crime or threat, that intrusion might very likely allow to gather relevant evidence, that less invasive measures are not available or would be useless, that no other information will be kept, that only relevant authorities will have access, that no other use or transfer will occur, and that fundamental rights will not be affected in their essence.
5. **Due process:** legal procedures allowing surveillance must be strictly regulated by law, for only legally stated causes, consistently applied, controlled by a judicial authority before surveillance takes place. Notification is required as soon as possible without affecting the investigation.
6. **Recourse:** oversight and accountability mechanisms must be implemented. Control of measures should reside in an independent authority different from those carrying out surveillance. Supervision must exist when surveillance is authorised for the first time, during its execution, and after it has ended. Recourse should be available even if no notice has been given.
7. **Transparency:** acquisition and use of surveillance technologies must include public disclosure of available technologies and statistics on their use. Usage policies must be made public, including purposes and security measures involved.
8. **Human rights impact assessment:** any private or public entity considering or carrying out the development or acquisition of surveillance technologies must be legally required to perform a prior human rights impact assessment, involving experts in technology, social sciences, fundamental rights, among others. Benefits, costs, impacts, and mitigating measures must be considered too.
9. **Democratic discussion:** acquisition, deployment and use of surveillance technologies must be subject to democratic control, extending to the legal tools and procedures that allow invasions on privacy. Participation processes must be open when local authorities aim to acquire or implement surveillance technologies.
10. **International cooperation guarantees:** cross-border data transfers for the purposes of investigation must be governed by transparent international cooperation mechanisms, fully respecting due process. Transfers between intelligence agencies, if allowed, must be strictly regulated and subject to independent judicial control.

IV. Standards for surveillance: recommendations for legal reform

DD has proposed the following standards for legal reform in Chile and Latin America more broadly[9].

1. Criminal investigation

- All activity of state surveillance must be carried out and controlled exclusively by competent investigation and prosecution entities specifically mandated and regulated by law, specifying their objectives, purposes and authorised activities.
- All authorities in charge of oversight of surveillance measures must be independent from those carrying out surveillance, and must be created and regulated by law, including the procedural mechanisms of control.

[9] Full recommendations available in Spanish here https://www.derechosdigitales.org/wp-content/uploads/propuesta-estandares-legales-vigilancia-chile.pdf

- Jurisdiction between criminal investigation and intelligence activities must be clearly separated by law. Communications between systems must be exceptional and subject to strict control by an independent judicial authority.
- Legal surveillance measures must be restrictively listed by law. All intrusive measures must be clearly and strictly regulated, with no implicit powers to go beyond the legally allowed activities.
- Use of legal surveillance mechanisms must not only show compliance with formal legal requirements, but also with substantive requirements consistent with constitutional rights and international human rights law.
- The admissibility of an intrusive measure must be qualified with regards to the seriousness of the facts investigated. The law must limit the persons affected by the measure, keeping them closely related to the facts.
- All measures must be limited in time, to terms set by law, as the minimum necessary for the goals of the investigation.
- All procedures to collect, examine, use and store information for investigation must be set by law, restricting access and safeguarding their integrity.
- Prosecution and investigation entities must have publicly available and clear protocols about their surveillance activities.
- Private entities in charge of information and/or communications services that can be subject to requests of data from authorities must have publicly available protocols about their procedure to safeguard their clients' interests and their cooperation with authorities.
- Each request for judicial authorisation to deploy or use surveillance mechanisms must, at the very least, thoroughly be preceded by a study the necessity of the measure, from a legal as well as an investigative perspective, and be requested in writing or with written support, specifying the investigated facts, the probable cause, the necessity of the measure, the information sought, the technical measures and their targets, their procedural protocols to collect and maintain information, and the measures to safeguard the rights of the defence and/or the investigated subjects.
- Each request for judicial authorisation to deploy or use surveillance measures must be accompanied by reporting mechanisms for the authorising authority, as well as control measure for the compliance of protocols, and collection of data for statistical reporting.
- The independent judicial authority in charge of controlling surveillance measures must, at the very least, prior to authorisation, verify the legal admissibility of the measures, as well as their proportionality, necessity, adequacy, technological viability, and the rights of those affected. The decision must be reasoned, based on the analysis of the available information, and setting the limits of the measure, as well as control and reporting mechanisms, and the conditions for the notification of those affected.
- All persons affected by surveillance measures must be given written notification about having been subjected to surveillance, including copies of the request and authorisation, with full information about the details of the surveillance activities, and the chance to seek redress.
- In the case of interception of private communications, all requests must analyse the necessity and proportionality of the measure, specifically identify the targeted persons and communication channels affected and their relation to the investigated facts, identify the entities that will carry out the interception, and the technologies that will be used. The use of malware must be explicitly forbidden, both by law and in any ruling on the request. No direct access must be allowed as a general rule by telecommunication companies.

- In the case of metadata, DD's research shows a current high level of informality to request and hand over communications information in Latin America. All requests for metadata should be sufficiently justified in similar terms than communications interception, including special consideration for the storage and use of the information. No legal mandates for a minimum term of bulk metadata retention should be enacted or enforced. Telecommunication companies must have clear, publicly available protocols on the cooperation mechanisms with authorities, expressing the need for specific judicial authorisation and the measures to safeguard the integrity and confidentiality of the information, as well as its timely destruction.
- In the case of stored information and electronic messages, including email, any request and any authorisation must be reasoned and separate from those pertaining interception of communications in transit.
- In the case of the seizure of devices and information storage units, and their examination, any request and any authorisation must be reasoned and separate from those pertaining interception of communications in transit or stored in servers. The use of tools for forced access, exploitation of vulnerabilities, or forced decryption of access controls or information, must be forbidden by law, and not allowed within legal prosecution. Investigation entities must provide detailed information about the techniques to obtain information from seized devices, without compromising the security and integrity of the devices or the stored information.

2. *Intelligence activities*

- The entities allowed to present requests of authorisation for surveillance practices for intelligence purposes must be clearly defined by law. Internal controls must be clearly set. Strict control of the measures through courts of law must be set by law, including requirements for detail and clarity with regards with authorised measures, and documentation of investigation leading to them.
- It is necessary to completely separate in law and practice the activities of intelligence from those of criminal investigation, to prevent exchange of information unless explicitly allowed by law and authorised by a court of law.
- External control from democratic institutions is necessary. Transparency mechanisms about intelligence activities deployed and their results must be provided to external control institutions, and the public without compromising information or after some time has lapsed.
- Mechanisms to obtain information must be clear, especially those involving technological means and which may affect information systems, as well as their circumstances of admissibility. Closely followed protocols and chains of custody, under external supervision and properly documented, is required. Balance of rights considerations must be required, including considerations of the aforementioned principles and rights.

3. *Prevention, policing of public spaces, and bodily surveillance*

Technology vendors have provided governments as well as private actors with tools that collect highly detailed information not only from communications, but also from their physical actions. The most pressing challenges in the region appear with relation to surveillance in public and open

spaces, and by the increased use of biometric indicators, including fingerprints, body scans, and facial recognition technologies.[10]

- In general, the development, acquisition, deployment and use of surveillance technology in open spaces for prevention purposes must be explicitly authorised by law, including explicit mention of those allowed to develop, acquire, deploy or use such technologies, the conditions for such use, and the authorities carrying out such surveillance. The law must specify the legitimate aims in a democratic society that can be invoked to implement such technologies, by which entities, and under which conditions.
- A general framework set by law, applicable to distance physical surveillance, is useful to provide uniform criteria in the acquisition, deployment, development and use of surveillance technologies in public spaces, regardless of special additional rules set for certain specific technologies when they might be especially intrusive, such as aerial equipment with video recording capabilities. There must be application of similar rules to public and private actors to prevent unlawful effects on fundamental rights.
- General data protection rules must still be applied, especially those concerning sensitive and biometric information, thus requiring additional safeguard mechanisms for data subjects.
- A human rights impact assessment must be conducted to determine the necessity, proportionality, adequacy, and the justification for surveillance and data collection measures that involve registering bodily data, as well as detailing the mitigation and risk prevention measures. Acquisition and usage of bodily surveillance measures that involve biometric records should not be adopted for public policy goals that do not require it, such as transportation, access to public benefits, or video surveillance. Mere availability of low cost technologies is not justification enough to acquire or use it.
- Transparency controls must be put in place, as well as participatory mechanisms for citizens for accountability. Surveillance in open spaces must be implemented with clear warnings, as well as usage policies, and procedures for examination, storage, security, erasure of, and access to collected information.
- External controls by an independent body must be established, as well as procedures for access to information, destruction of unnecessary collected information, and redress mechanisms.

4. Surveillance technology controls

- **Transparency and accountability in acquisition.** Law should provide a clear, specific framework with regards to which state agencies can develop, acquire or purchase technologies for their use in surveillance activities, and under which conditions. Independent oversight, public transparency and accountability mechanisms must be included. Human rights impact assessments, as well as capacity building for involved personnel, are required as well, and mechanisms to investigate abuse and terminate existing contractual, commercial or labour relationships.

  Transparent, public procurement processes must be the only legally available way to acquire such technology from private or foreign vendors. Transparency obligations must include timely information about adjudication, reducing the application of secrecy to the minimum. Vendors must comply with probity and commitment with human rights in every front of

[10] See Marianne Díaz (2018). El cuerpo como dato. https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

operation, and be excluded when there is a history of provision of technology to violate democratic principles and human rights.

- **Information security.** Given the nature of information collected by data intensive systems and surveillance mechanisms, vulnerabilities can allow malicious actors as much information as trusted data fiduciaries or the state. Security mechanisms over collected data must be put in place for both state entities and as requirements for any system acquired by the states or developed for surveillance purposes.
  The protection of legally collected data must be subject to legal obligations that include:
  - establishing measures to safeguard the integrity of data and the protection of the security of the systems that collect and process data,
  - implementing technical and organisational measures to prevent access to information by any person beyond those especially and explicitly authorised,
  - protecting data, through adequate technical and organisational measures, against accidental or illegal destruction by third parties, accidental loss or alteration, illegal retention, and illegal access, processing or disclosure by third parties.
- **Limitations on metadata retention and collection**. Communications data can be extremely intrusive. Legal frameworks must clearly identify metadata as personal data, protected as such. Access, retention and use of metadata must be only allowed exceptionally by law, passing the necessity, adequacy and proportionality tests pursuing a legitimate aim. Objective criteria to limit access to communications data and their use for prevention, detection or prosecution of severe crimes. Legal mandates for retention, if they exist, should be limited in scope and time, with obligations regarding the security in the storage of such data, access mechanisms, transfers, and conditions for deletion. Access must be subject to judicial authorisation.

V. Final comments

Even the Wassenaar Arrangement provides guidelines to limit the export of dual-use technologies, we consider relevant not exclusively focus the control of procurement and use of surveillance technologies to export and import controls. From Latin America perspective those voluntary regimes have attractive regarding what they can advance on transparency that allows civil society organisations track the acquisition of such technologies, but do not provide a proper framework to access to concrete information regarding the local use of imported or domestically developed technologies or initiate legal actions against their inappropriate use. That is why DD effort has devoted mainly to work jointly with other organisation in the region to foster a dialogue and provide insight in the appropriated national standards that should be implemented in accordance with human rights international framework.

Regarding the focus of the consultation in surveillance dual technologies, for Latin America in particular, and global south more broadly, it is necessary a more comprehensive approach that not only covers the malware development and distribution, but also other technologies as forensic technologies, deep package inspection technologies, or network management technologies that can be easily repurposed for surveillance objective. On the same line, there is a need to approach to the private provision of surveillance technologies that also covers bodily surveillance produced through the use of biometric technologies and technologies as HD cameras and drones. Standards should be developed to ask private companies a more strict exercise of human rights impact assessment previous to promote the acquisition and sell those technologies to governments in our region.