The right to privacy in the digital age

Response to the request for inputs by the OHCHR

Introduction

Derechos Digitales América Latina is pleased to respond to this call for input from the Office of the United Nations High Commissioner for Human Rights on "the right to privacy in the digital age".

The respondents are aware that the subject of privacy in the digital age covers vast areas of knowledge and policy. As members of civil society located and operating in different Latin American countries, the respondents understand the need for raised awareness in a group of highly contested matters that are outlined below, as recent developments in legislation, case law, and practice concerning the right to privacy in the digital age in our region.

In our view, the continuous growth of data-driven industries, as an integral part of the expansion of information and communication technologies, in our region has not been properly accompanied by sufficient safeguards for privacy in public policy, in law, and in practice. This has allowed for a landscape where citizens are subject to constant and increasing risk on their right to privacy, risks enabled by digital technologies well beyond the use digital communications alone. They represent a worrying trend in Latin America, where the shadow of past authoritarianism meets the present political unrest and a persistent public safety discourse that emboldens state actors to deploy surveillance technologies, while having a negative impact in not only privacy, but other rights enabled by it, such as freedom of expression, freedom of association and freedom of movement.

In this submission, we intend to highlight a few key areas of current issues in the field of privacy in Latin America, showing examples of concerns as well as possible action points for States, in the hope that these will be reflected in the report.

Communications surveillance in Latin America

Surveillance of digital devices by hacking is an important trend in Latin America. In recent years, news about surveillance of digital communications have spread with different emphases and a wide array of victims. In general, it is public institutions, mostly governmental at a national or local level, acquiring and often deploying digital surveillance tools, including the use of malware to infect devices and elude encryption mechanisms, often without a criminal investigation or a court order in place. This form of interception is highly intrusive and goes well beyond access to communications, potentially involving all forms of activity of a person using that device. For that reason, this represents a particularly severe threat to human rights.

In Mexico, malicious software known as "Pegasus", provided by the security company NSO Group, was used by state actors to intercept the communications of activists, journalists and government critics.[1] In Honduras, the government allegedly acquired malicious software to intercept private messages, just before the general elections at the beginning of 2018, right around the time where nationwide protests occurred and were met with violent repression.[2] Many other countries, as it was revealed in 2015, had also acquired malware to control and surveille digital devices, from Italian vendor Hacking Team.[3] Colombia, Panama and Venezuela are allegedly users of FinFisher to intercept mobile communications as well.[4]

Former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Frank La Rue, observed that "*[i]n order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous*".[5] The surveillance schemes sought by malware mechanisms affect the security and the privacy of the communications of the people affected by it, while their legally doubtful acquisition threatens the protection of the privacy of all individuals within a country.

Recommendation: States should enact rules for communication surveillance that comply with the requirements for justified interferences with the right to privacy,[6] including the principles of legality, legitimate aim, necessity and proportionality. States should recognise that communications surveillance through the use of hacking tools represents a highly invasive activity that also endangers security, and exclusively rely on it exceptionally for criminal investigation purposes. States should take steps in order to enhance the transparency, accountability and participation in the process of acquiring communication surveillance technologies. We urge the High Commissioner to recommend these principles to governments.

Mandatory retention of communications data

Retention of communications data, or metadata, continues as part of regulatory

[1] Perlroth, N., "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families". *The New York Times*, 19 June 2017, https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html.
[2] Lakhani, N., "UK sold spyware to Honduras just before crackdown on election protesters". *The Guardian,* 8 February 2018, https://www.theguardian.com/world/2018/feb/08/uk-sold-spyware-to-honduras-just-before-crackdown-on-election-protesters
[3] Pérez de Acha, G. (2016), *Hacking Team: Malware para la vigilancia en América Latina*, https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
[4] Fundación Karisma (2015), "Cuando el Estado Hackea. Análisis de la legitimidad del uso de herramientas de Hacking en Colombia", https://karisma.org.co/wp-content/uploads/2015/12/CUANDO-EL-ESTADO-HACKEA-D.pdf
[5] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, UN Doc. A/HRC/23/40, 17 April 2013.
[6] General Comment No. 16 of the Human Rights Committee.

frameworks in Latin America, where telecommunications companies are required to retain information from all their subscribers for a period of time. Existing frameworks have not changed in Latin America, and in fact, there have been attempts at creating new mandates or extending the existing ones. This is a threat to privacy at a mass scale that governments need to address.

Examples vary in the region.[7] In Colombia, Law No. 1621 requires retaining the user's communication history, the technical identification data of the subscribers that are part of the communication, and geolocation data, for a period of five years. In Brazil, telecommunications agency, ANATEL, requires ISPs to retain connection records for a period of one year, a requirement ratified by Law No. 12,965 / 24 ("Marco Civil de Internet"). In Peru, Legislative Decree No. 1182 of 2015 established a mandate to retain data "derived from telecommunications" for three years, without sufficient specification. In Mexico, Federal Telecommunications and Broadcasting Law obliges companies providing telecommunications services to conserve a broad array of metadata of their users' communications for two years. In Chile, criminal procedure law dictates that ISPs must maintain an updated list of their authorised ranges of IP addresses, as well as registration of IP numbers and their connections, for a minimum of one year, an obligation that was almost expanded via presidential decree in 2017 but failed constitutional control. In Venezuela, Administrative Measure No. 171 from telecommunications authority CNT requires ISPs the retention of metadata, eluding congressional debate on the subject.[8]

The processing of metadata has been acknowledged as an invasion on the right to privacy by the Human Rights Council, when it acknowledged that "*metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications*".[9] Also, in many of these examples, by statute or by practice, retention is provided for criminal prosecution entities to access the data, often without judicial review, giving the State enormous power over its innocent citizens. As expressed by Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye, "*[a] State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint*".[10] These regulatory schemes represent an invasion on the privacy of citizens at a mass scale.

[7] Díaz, M. (2017a), *Data Retention and Registration of Mobile Phones: Chile in the Latin American Context*, https://www.derechosdigitales.org/wp-content/uploads/Data-Retention-and-Registration-of-Mobile-Phones-.pdf

[8] Díaz, M. (2017b), "Sin lugar dónde esconderse: retención de datos de telefonía en Venezuela", https://www.derechosdigitales.org/11932/sin-lugar-donde-esconderse-retencion-de-datos-de-telefonia-en-venezuela/

[9] UN Human Rights Council, *Resolution on the right to privacy in the digital age*, A/HRC/RES/34/7.

[10] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/29/32, 22 May 2015, para. 55.

Recommendation: States should recognise that retention and processing of communications data represents an invasion of privacy, and refrain from establishing or expanding metadata retention mandates. States should outlaw all investigation mechanisms that involve massive data retention. States should establish clear, fair and transparent practices of data retention and access to communications data by prosecution and investigation entities, to ensure due process. We urge the High Commissioner to recommend governments to phase out communication data retention mandates and refrain from establishing new mandates.

Bodily surveillance and biometric information collection

The use of surveillance technologies over the movement of people has grown enormously, adding in recent years the use of digital technologies. Government entities in Argentina, Brazil and Chile have acquired unmanned aerial vehicles or "drones" to surveille and follow people in cities, sometimes including facial recognition technology, without proper safeguards against the surveillance inside private spaces, as well as rejecting acknowledgement of a sphere of privacy in public spaces.[11] At the same time, it is a serious threat to the exercise of the rights of freedom of association and expression, while the incorporation of digital technologies, including facial recognition, helps on the construction of massive databases without oversight in their use.

In a related development, the indiscriminate collection of biometric information has become commonplace in Latin America, with State and private actors deploying such technology for the declared purpose of identification or verification, for facial recognition in public spaces, or even as a requirement for access to basic goods and services. In Venezuela, the acquisition of groceries and medicines requires registration of an identity document including personal data as well as fingerprints;[12] in Brazil, a new national identification system would consolidate information databases including biometrics;[13] throughout Latin America,[14] the collection and processing of biometric data by public institutions and private actors remains a largely unchallenged practice that is not accompanied by data protection regulation. As result, there are not sufficient safeguards to prevent abuse, data breaches, or profiling based on biometric information, risking both the privacy of individuals as well as their security.

Recommendation: States should enact rules for surveillance in public spaces that

[11] Fundación Datos Protegidos (2018), *Drones en Chile: Un análisis de los discursos, industria y los derechos humanos*, https://datosprotegidos.org/wp-content/uploads/2018/02/Informe-Drones-espa%C3%B1ol.pdf
[12] Díaz, M. (2015), "Your fingerprint for a kilogram of flour: biometric and privacy in Venezuela", https://www.digitalrightslac.net/en/tu-huella-digital-por-un-kilo-de-harina-biometrica-y-privacidad-en-venezuela/
[13] Varon, Joana y Rená, Paulo (2015). "Brasil anuncia proyecto para identificación única con la biometría. ¿Cómo está el tema en América Latina?". Disponible en: https://antivigilancia.org/es/2015/07/1430/
[14] Varon, Joana y Rená, Paulo (2015). "Brasil anuncia proyecto para identificación única con la biometría. ¿Cómo está el tema en América Latina?". Disponible en: https://antivigilancia.org/es/2015/07/1430/

comply with the requirements for justified interferences with the right to privacy subject to judicial oversight, including safeguards for the sanctity of home and against the collection of biometric information from public spaces. States should recognise that the collection of biometric data needs strong safeguards, limiting its use to the minimum necessary, and setting strong legal and technical safeguards for its processing. States should take steps in order to enhance the transparency, accountability and participation in the process of acquiring technologies that collect information from physical characteristics. We urge the High Commissioner to recommend these principles to governments.

Data protection and automation: the data-driven economy

Latin America is currently facing the challenges of a growing data-driven economy, but with severe limitations in its capacity to address some of its risk. The use of data processing technologies that include algorithmic decision-making and machine learning, for purposes of profiling or segmenting, as it has happened in the private sector for many years, and with the public sector increasingly as a client of such technologies.

The risks of discrimination and profiling have been part of discussions in the global North in the last few decades. In Latin America, because of lacklustre or non-existent data protection frameworks in many countries in the region, these technologies can thrive, as personal information is widely available, with an extreme level of opacity over its collection and processing. And as a consequence, the risks of discrimination, social control, and unfair decisions made by machines, are enhanced. From targeted advertising and credit scoring, to public policy decisions on public safety, health and housing, citizens in Latin America are threatened in their capacity to learn how decisions that impact their lives are taken and to be able of conducting themselves freely without interference by machines.

One key area where algorithmic decision-making has been making advances in Latin America is predictive policing. In Brazil, CrimeRadar is being used in Rio de Janeiro,[15] while in Chile the police announced the acquisition of predictive software from the University of Chile.[16] These models are based on past data, thus reinforcing notions about what places are considered dangerous or crime-ridden, reinforcing discrimination based on their place of origin or altering their prospects in labour, insurance, housing, etcetera. The huge public availability of different sources of personal data, and the linking between databases, impact not only the right of privacy, but also their equal treatment and access to goods and services from public and private actors.

The Human Rights Council has recognised that "automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect

[15] CrimeRadar, https://igarape.org.br/en/apps/crimeradar/
[16] "Carabineros usará el primer software capaz de predecir dónde ocurrirán delitos", *La Tercera,* May 19 2017, http://www2.latercera.com/noticia/carabineros-usara-primer-software-capaz-predecir-donde-ocurriran-delitos/

the enjoyment of human rights, including economic, social and cultural rights".[17] Governments in Latin America need to address the absence of legal tools to exert control over personal data, to audit and demand explanation of algorithms, to restrict the use of machine made decisions in sensitive fields, or to oppose discriminatory decisions made by machines.

Recommendation: States should officially acknowledge the effect of algorithmic decision-making and profiling on the privacy and autonomy of individuals, as well as its risks of discrimination and reinforcement of biases. States should integrate a view of the risks of automated decisions when regulating personal data, limiting the automated decision-making. States should provide legal tools to oppose decisions made by machines, audit their decision-making processes, and reject or revert unfair decisions made with support from automation. We urge the High Commissioner to take into account these recommendations for States.

International transfers of personal information

The data-driven economy happens online at a global scale, and national borders are, for the most part, ignored by private actors for the purposes of collecting and processing personal data, which can be stored and processed anywhere in the world. This happens both with regards to the internet and the constant collection of personal data as enabled by business models and devices, as well as in the transfer of personal information between companies with different levels of integration located in different countries.[18] Naturally, although there may be a national framework to protect the rights of an individual or a group, the same may not be true about the places towards where the information is transferred. A complex global market involving internet companies and data brokers in different jurisdictions, makes tracking personal data nearly impossible. The loss of control over data thus becomes a loss of control over key aspects of one's right to privacy. Users in Latin America, in many cases without strong protections for personal data, have very little to no control once it leaves their borders.

Governments, as well, have the tendency to expect access to data stored worldwide. Brazilian courts have demanded access to WhatsApp communications disregarding its storing situation, based on their interpretation of the Marco Civil de Internet.[19] Chilean prosecution entities have used the mutual legal assistance tools to obtain data from Twitter

[17] Human Rights Council resolution on the right to privacy in the digital age, UN doc. A/HRC/RES/34/7.
[18] *"Fondo estadounidense adquiere I-Med, la empresa que almacena las huellas digitales de usuarios de la salud en Chile"*, El Dínamo, January 3, 2018, https://www.eldinamo.cl/nacional/2018/01/03/fondo-estadounidense-adquiere-empresa-que-almacena-las-huellas-digitales-de-usuarios-de-la-salud-chilenos/
[19] Abreu, J., "From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", *Columbia Journal of Transnational Law*, October 2016, http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/

in the United States, without sufficient fulfilment of the MLAT requirements.[20] Legal initiatives like the CLOUD Act in the U.S. would allow for all kinds of access to information from abroad. Moreover, opaque practices like communications surveillance and direct data exchange between companies situated in different countries, render moot all minimum level data protection requirement for international transfers of personal information, as was the case with the revelations about the Five Eyes collaboration between Australia, Canada, New Zealand, the United Kingdom and the United States.

This loss of control over international data transfers is often addressed through international or regional standards (outside law enforcement cooperation), such as the requirement for an adequate level of data protection for countries trading with the European Union, or soft instruments such as the APEC Cross-border Privacy Enforcement Arrangement (CPEA) or the OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Information.[21] But there is no such scheme that covers Latin America, where many countries have limited constitutional and legal protection over privacy and personal data without enforcement agencies many times, and where only a couple of countries (Argentina and Uruguay) have been recognised as having an adequate level of protection for exchanges with the EU. What this entails is vulnerability in the face of the digital economy, and an unequal standing for citizens of different regions of the world, with Latin Americans' rights severely under protected.

The negotiation of international trade agreements goes in the same direction. Chile, Mexico and Peru became part of the CPTPP, an agreement with other 8 nations around the Pacific Ocean, which has its own rules for cross-border data transfers (Article 14.11). The States parties fail to include substantive requirements to protect personal data or privacy, strong prohibitions on data localisation requirements or data transfer limitations (with limited exceptions). Thus, a model that favours commerce over privacy has been severely reinforced in our region through this type of agreements.[22]

Recommendation: States should fulfil their international commitment regarding protection of the right to privacy in trade negotiations that involve personal data transfers to enhance e-commerce. States should collaborate in the search for common solutions to cross-border data transfers that allow for the maximum level of protection for personal information. We urge the High Commissioner to highlight to the States the need for stronger privacy protections in trade negotiations concerning developing countries that allow promoting aligned internal reforms to better protect the right to privacy in those countries.

[20] Álvarez, D., "On the parody on Twitter: lessons to learn", *Digital Rights LAC,* July 17, 2013, https://www.digitalrightslac.net/en/sobre-la-parodia-en-twitter-lecciones-que-aprender/
[21] Cannataci, J. et al (2016), *Privacy, free expression and transparency: Redefining their new boundaries in the digital age*, UNESCO, http://unesdoc.unesco.org/images/0024/002466/246610E.pdf
[22] Greenleaf, G. (2016), "Free Trade Agreements and Data Privacy: Future Perils of Faustian Bargains". UNSW Law Research Paper No. 2016-08, https://ssrn.com/abstract=2732386