The right to privacy in Latin America in the face of digital technologies

Derechos Digitales' contribution to the report by the United Nations High Commissioner for Human Rights on the right to privacy in the digital age at the 51th session of the Human Rights Council

About Derechos Digitales

Derechos Digitales is a non-governmental and non-profit organisation, founded in 2005, with a Latin American scope. It has consultative status with ECOSOC and its headquarters are in Santiago de Chile. We are an organisation dedicated to defending and promoting human rights in the digital environment. Our actions are focused on analysing the impact of technologies on fundamental rights and influencing the public and private sector to promote social change around the respect and dignity of all people. Previously, Derechos Digitales has contributed to the reports on privacy in the digital age of this Office, sharing a Latin American vision on relevant issues related to privacy and digital technologies.

Introduction

This report seeks to contribute to documenting and systematising the Latin American experience on the exercise of the right to privacy in the digital age. In this report we present three trends in which privacy is violated through digital technologies in the last several years: the impact on privacy due to the massive collection and processing of personal data, targeted and massive surveillance, and the importance of encryption in communications to preserve privacy and security.

We consider that, in its interdependent nature, the violation of the right to privacy has as a consequence the violation of other human rights such as freedom of expression, freedom of association and peaceful assembly, equality and a dignified life. Additionally, because of the nature of personal data processing by states, in attempted fulfilment of its duties, privacy impacts can be conducive to differentiated or discriminatory effects on large portions of the populations that are more frequently subject to state control through data collection and processing.

The documentation supporting this report has been gathered by Derechos Digitales from our work individually and in alliances with other civil society organisations and academic institutions in the region as well as from other trusted sources in the region.

1. Personal data protection and surveillance during the COVID-19 pandemic

In Latin America, countries such as Argentina, Brazil, Chile, Ecuador, Mexico, Peru and Uruguay have legal frameworks to protect personal data, while countries such as Bolivia and

Venezuela do not yet have adequate legislation.[1] Despite considerable progress in legislation, the reality in the region is characterised by governments that implement actions to collect, use and transfer personal, sensitive and biometric data that violate the privacy of citizens.

In the wake of the Covid-19 pandemic, Latin America experienced a wave of implementation of new technologies, in the form of mobile digital applications and other forms of data processing, to track and monitor the evolution of the pandemic; however, these became a tool for the mass collection of personal and sensitive data that violated the privacy of the population and encouraged the surveillance of citizens.

A study by the Al Sur consortium analysed the implementation of 16 systems for monitoring the pandemic in the region by public entities, and identified that there were few protections for the control of personal data in most platforms. In its findings, there was little clarity about which institutions were accessing the data, what were the conditions under which the data was delivered, and what would happen to all of it.[2] In addition to these concerns, the report identified a regional trend towards the massive collection of personal data in these applications beyond its necessity, as in some cases collected information included more than identification, and included geospatial data or real-time location and access to device databases, allowing for surveillance beyond health measures.

Another study by Derechos Digitales,[3] reinforced that the technologies to monitor the pandemic made a massive collection of data, but it also identified that, at least, three countries (Argentina, Bolivia and Brazil) had personal data breaches, which puts the privacy of the affected people at risk. This allows us to see that there were no adequate procedures for the protection of personal and sensitive data by governments, and that safeguards were not in place before the attempts to tackle the pandemic.

Another project implemented in four Latin American countries,[4] identified that governments implemented technologies in the context of the pandemic without studies that anticipated the impact of the use of these technologies on human rights. This shows that there was no analysis that supported the criteria of proportionality, necessity and legality. The study also revealed that Latin American governments have implemented technologies for monitoring the pandemic that, in addition to being population surveillance technologies, are also collectors of personal data that operate under the negligence of the States to comply with the respect for the processing of personal and sensitive data.[5] Derechos Digitales together with its partners in the project "*Sonríe, te estamos vigilando*" made visible the lack of transparency and accountability practices and standards with which governments implemented data collection through these applications. This opacity was especially reflected

[1] Bordachar M. (2022). ¿Cómo y quiénes cuidan nuestros datos? Legislaciones vigentes en países Latinoamericanos. Derechos Digitales. Available at (in Spanish): https://www.derechosdigitales.org/17759/dia-de-la-proteccion-de-los-datos-personales/

[2] Venturini, J. Canales, M.P. *et al.* (2021). Informe Observatorio Covid-19 del Consorcio Al Sur: Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia. Al Sur. Available at: https://www.alsur.lat/sites/default/files/2021-06/Informe%20Observatorio%20Covid-19%20del%20Consorcio%20Al%20Sur(2).pdf

[3] Hernández, L. (2021). Uso de Tecnologías para el combate de la pandemia. Datos personales en América Latina. GNI Network. Available at: https://globalnetworkinitiative.org/wp-content/uploads/2021/11/COVID19-LAC-SPA.pdf.

[4] The countries were: Chile, Colombia, Brazil and El Salvador.

[5] For more information about the project: https://www.estamosvigilando-cejil.org/recursos/

in the agreements signed by the governments and the private companies that when they are asked for public information, they classify it as "reserved information".

In 2021, a group of civil society organisations, including Derechos Digitales, participated in a public hearing before the Inter-American Commission on Human Rights (IACHR).[6] In this hearing, civil society organisations highlighted the implementation of surveillance technologies under the discourse of public security, monitoring of the Covid-19 health pandemic, observation of borders and access to public services, without proper transparency and accountability.

In summary, in most of the cases analysed by civil society, studies showed that there was no adequate planning or a comprehensive public health strategy on the use of technologies to combat the pandemic. The lack of appropriate links between legitimate public health objectives and data processing efforts has meant a normalisation of data collection even beyond its necessity, raising concerns about the handling of information by states.

2. State surveillance as a threat to privacy

The use of digital communication tools has augmented the risk of state surveillance of its citizens, including both massive and targeted surveillance that negatively impact the right to privacy. Frequent victims of state surveillance include the media, civil society and opposition groups, through the use of digital technologies and tools such as artificial intelligence, biometrics, facial recognition, mass data collection systems, communications intervention technologies, among others. State surveillance can be a direct violation of the right to privacy if it does not comply with requirements of legality, necessity and proportionality, as it would represent an interference in the personal and private life of citizens. This in turn has an impact on other human rights such as freedom of expression and the right to peaceful assembly.

In the aforementioned hearing before the IACHR in 2021, civil society organisations highlighted the consequences of surveillance for human rights, including the right to privacy. The organisations asked that the IACHR establish standards and recommendations to limit the acquisition, development and use of surveillance technologies and, if it is necessary, that they be implemented under the principles of proportionality, necessity and legality.[7]

Digital technologies have facilitated the exercise of state surveillance both in a targeted and in a massive way. Targeted surveillance is aimed at specific persons or groups who may put government interests at stake, and mass surveillance has a broader scope, by monitoring the general public through, for example, the installation of systems with facial recognition in public spaces. In both cases, technologies allow both the surveillance of individuals and of their communications and devices.

---

[6] The participating organisations were: Derechos Digitales, R3D, Artículo 19 México y Centroamérica,CEJIL, Fundación para la Libertad de Prensa, Fundación Karisma. The hearing can be viewed here: https://www.youtube.com/watch?v=IdkYQIpBhoE&t=725s

[7] *Ibid.*

2.1. *Targeted surveillance and the use of malware in Latin America*

In Latin America, selective state surveillance is becoming a trend implemented by governments as a tool to violate the privacy of journalists, human rights defenders, the media, organised civil society and dissident groups that document and report cases of corruption, violence and human rights violations. In other words, the right to privacy is often violated as a consequence of the legitimate exercise of the right to freedom of expression and access to information.

Targeted surveillance is one more tool that governments in Latin America have used to deteriorate democracy in their countries and install political regimes with authoritarian overtones. The case of Nicaragua is an example that illustrates the implementation of a legal framework that violates civil and political rights,[8] added to actions of surveillance and harassment offline and online (under the purchase of surveillance equipment)[9] to activists, opponents of the political party in power and the media create a hostile environment for citizens and undermine the guarantee of human rights such as privacy, personal integrity, free expression and peaceful assembly, among others.

In the case of digital communications and devices, the trend in Latin America is the illegal use of surveillance malware, which affects the integrity of communication systems for surveillance purposes. A 2016 report by Derechos Digitales showed that several Latin American governments acquired the Remote Control System (RCS) software of the Italian company Hacking Team, which operated by accessing private communications and capturing information hosted on infected devices.[10] We identified that the narrative to acquire selective surveillance technologies is generated under the discourse of public security and national security, has allowed governments to implement surveillance actions illegally, having a negative impact on the human rights of the targets of this practice.

The role of government institutions in matters of public security and national intelligence to acquire surveillance technologies is striking, because they classify activists and journalists as a target to pursue. In the case of Hacking Team, its technology was bought by institutions such as the National Intelligence Police of Colombia, the Federal Police of Brazil, the Intelligence Secretariat of Ecuador or the National Directorate of Investigation and Intelligence of Honduras.

This case was followed years by the scandal brought by the revelation of acquisition of the Pegasus malware, from the Israeili company NSO Group, in Mexico and El Salvador, as well as its illegal use against activists and journalists. In Mexico, the malware was acquired by three institutions: the Ministry of National Defence, the Attorney General's Office and the

[8] See for example: CIDH. Nicaragua: Concentración del poder y debilitamiento del Estado de Derecho. Available at: https://www.oas.org/es/cidh/informes/pdfs/2021_Nicaragua-ES.pdf. CIDH. A CIDH condena a manipulação do direito penal e a falta de garantias em processos de pessoas presas políticas na Nicarágua. Available at: https://www.oas.org/pt/CIDH/jsForm/?File=/pt/cidh/prensa/notas/2022/027.asp

[9] Bow, J. C (2018). Ortega espía con tecnología israelí. Available at: https://www.confidencial.com.ni/politica/ortega-espia-con-tecnologia-israeli/

[10] Pérez, G. (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

Centre for Research and National Security. In that case, activists and journalists[11] who investigated cases of federal government corruption and human rights violations were monitored.[12] In El Salvador, around 35 people from organised civil society and the media were spied on, through the use of the Israeli software. The victims had been[13] investigating the administration of President Nayib Bukele, and its alleged negotiations with organised crime in favour of electoral support.[14]-[15]-[16]

In Brazil, even in the absence of proper legislation and safeguards, the Ministry of Justice and Public Security has attempted to buy different types of spyware. The Ministry was also questioned after a secret dossier was identified with data from more than 500 members of the public administration identified as "anti-fascists".[17]

The private sector plays a fundamental role as a supplier of surveillance technologies. Companies such as NSO Group have stated that technology such as Pegasus is only sold to governments, while the company Elite by Cargo, a supplier of surveillance technologies in Mexico, recently declared that it provides equipment to seven local governments and tools such as false telephone antennas, signal blockers and software to intercept WhatsApp,[18] going as far as admitting to have supported a mayor to have illegal access to the iCloud, Hotmail and Twitter accounts of a political figure in Mexico.[19]

Derechos Digitales is concerned about the invasion of privacy and intimacy experienced by journalists and human rights defenders through targeted surveillance technologies, because the risks are serious, especially when the victim does not know that they have been illegally

---

[11] Artículo 19, R3D, SocialTic. (2017). Gobierno espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México. Available at (in Spanish): https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf

[12] Comisión Nacional de los Derechos Humanos (2022). Recomendación General no. 47/2022. Available at: https://www.cndh.org.mx/sites/default/files/documentos/2022-05/RecGral_47.pdf

[13] Derechos Digitales (2022). Casos de espionaje con Pegasus en El Salvador: una nueva estocada al derecho a la libertad de expresión. Available at: https://www.derechosdigitales.org/17689; Oliva, X. (2022). Periodistas de GatoEncerrado y de otros medios fueron espiados con Pegasus en El Salvador. Available at: https://gatoencerrado.news/2022/01/13/periodistas-de-gatoencerrado-y-de-otros-medios-fueron-espiados-con-pegasus-en-el-salvador/

[14] Access Now (2022). Pegasus attacks in El Salvador: spyware used to target journalists. Available at: https://www.accessnow.org/pegasus-el-salvador-spyware-targets-journalists/

[15] Comisión Interamericana de Derechos Humanos - CIDH (2022). Audiencia pública: La situación de los derechos humanos en el contexto de la vigilancia cibernética en El Salvador. Available at: https://www.youtube.com/watch?v=E77H2_4SSPk

[16] Martínez, C (2022). Collapsed Government Talks with MS-13 Sparked Record Homicides in El Salvador, Audios Reveal. El Faro. Available at: https://elfaro.net/en/202205/el_salvador/26177/Collapsed-Government-Talks-with-MS-13-Sparked-Record-Homicides-in-El-Salvador-Audios-Reveal.htm

[17] Association for Progressive Communications (APC), Artigo 19 Brasil e América do Sul, Derechos Digitales & Intervozes (2022). Joint stakeholder contribution to the 41st session period of the Universal Periodic Review - Brazil. Available at: https://www.derechosdigitales.org/wp-content/uploads/UPR_Brazil_eng-logoPT.pdf

[18] R3D (2022). Empresario se declara culpable de vender equipo de espionaje en México a sabiendas de su uso ilegal. Available at: https://r3d.mx/2022/02/17/empresario-se-declara-culpable-de-vender-equipo-de-espionaje-en-mexico-a-sabiendas-de-su-uso-ilegal/

[19] Guillé, F. (2022). Espionaje en México: empresario admite vender equipos que gobiernos niegan haber comprado. Available at: https://serendipia.digital/datos-y-mas/espionaje-en-mexico-venta-de-equipos-de-espionaje-a-gobiernos-estatales

monitored. We believe that it is necessary to create local legal frameworks that limit the acquisition and use of surveillance technologies, as well as that international human rights organisations, such as the present Office, build international standards under which governments use these technologies in accordance with full respect of the right to privacy and free expression.

2.2. *Mass surveillance: biometrics and facial recognition systems*

In Latin America, massive state surveillance has been developed under narratives of public security, access to social assistance and public health services, especially in the context of the health pandemic, as shown in section 1. Through the massive collection of personal data from the population and the use of technologies such as facial recognition systems, initiatives that violate the right to privacy of citizens have been identified in practically all the countries of the region.

An ongoing trend in the region is the physical surveillance of citizens through advanced digital technologies. Civil society organisations in the region have documented the use of biometric databases to implement mass surveillance systems such as facial recognition. Biometrics works through databases of physical and behavioural traits that allow the authentication and identification of a person, in order to match between what is captured and what already exists in biometric databases.[20] In Latin America, such biometric data is obtained from various sources, such as mandatory identity documents or electoral databases.

The public security narrative has led countries to implement technologies with facial recognition capabilities, especially in public spaces such as streets and public parks. According to the governments, installing these systems makes it possible to keep public order and safety. However, facial recognition systems, biometrics and artificial intelligence acting together allow the identification of people and the monitoring of their actions in real time, information that can be stored and infer and predict future behaviour of a person.[21]

An investigation carried out by Al Sur studied 38 facial recognition initiatives with an emphasis on those used for mass surveillance in Latin America in the last three years. One of the results of this analysis is the identification of the violation of different human rights. On the one hand, the use of these technologies implies collecting personal and sensitive data, such as biometric data, without consent, so their rights to the protection of personal data and privacy are compromised.[22] This research also made it clear that the ability to predict behaviour of citizens can violate the right to privacy, freedom of expression, association, anonymity and peaceful assembly, because it can allow the profiling of participants in social protests, which promotes the criminalization of protest.

Other problems arise from facial recognition, such as the discrimination of historically vulnerable groups such as women, dark-skinned people or trans people, which has brought

[20] Díaz, M (2018). El cuerpo como dato. Available at: https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf
[21] Venturini, J; Garay, V. (2022). Facial recognition in Latin America: trends in the implementation of a perverse technology. Available at: https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_EN_Final.pdf
[22] Idem.

consequences for the presumption of innocence when the failure of the identification in facial recognition systems leads to prosecution of innocent people. Thus, automated facial recognition reproduces and reinforces historical biases against marginalised groups.

Access to personal and biometric databases is necessary for this kind of surveillance, for which governments and the private sector have created a series of initiatives that harm people's privacy. In Brazil, agreements were signed to share data between government agencies and the banking sector.[23] In Mexico, an attempt was made to create a National Register of Mobile Telephony Users (PANAUT) including biometric information.[24] In Colombia, public elections take place under a biometric registry of candidates and voters.[25] In Venezuela, access to food or medicine is conditioned based on a biometric data record.[26] These initiatives are risky in countries where personal data protection legislation is ineffective or nonexistent, creating new sources of information to facilitate surveillance.

Civil society organisations have promoted advocacy actions to limit state surveillance, for example, legal actions that put a stop to the use of these technologies through the courts. Currently, two emblematic judicial cases have been carried out in Brazil[27] and Argentina,[28] where the collection and use of biometric data from citizens has been suspended by interim orders, as well as the suspension of facial recognition systems. However, other technologies are still being used, such as predictive policing through databases with unreliable and inaccurate data,[29] or the use of technologies such as drones to monitor spaces such as borders,[30] among many others.

---

[23] Idec (2022). Idec questiona ANPD sobre acordo que libera dados dos cidadãos aos bancos. Available at: https://idec.org.br/noticia/idec-questiona-anpd-sobre-acordo-que-libera-dados-dos-cidadaos-aos-bancosMinistério Público Federal (2022). Notícia de Fato nº 1.26.000.000383/2022-78. Despacho nº 2271/2022. Available at: https://www.telesintese.com.br/idec-quer-acao-da-anpd-contra-uso-de-dados-dos-cidadaos-pelos-bancos/DESPACHO-2271-de-2022.pdf

[24] Souza, M. R. (2022). #NoAlPadrón: México frente a una abusiva reglamentación para el uso de celulares. Available at: https://www.derechosdigitales.org/17995/noalpadron-mexico-frente-a-una-abusiva-reglamentacion-para-el-uso-de-celulares/

[25] Hernández, L. R (2021). Inscripción de precandidatos se realizará por biometría facial, anticipa la Registraduría. Available at: https://www.rcnradio.com/politica/inscripcion-de-precandidatos-se-realizara-por-biometria-facial-anticipa-la-registraduria

[26] Venturini, J; Díaz, M. Sistemas de identificación y protección social en Venezuela y Bolivia: impactos de género y otras formas de discriminación. Available at:https://www.derechosdigitales.org/wp-content/uploads/sistemas-de-Identificacion_ES.pdf

[27] Arcoverde, L. (2022). Justiça de SP determina que Metrô interrompa implantação de sistema de reconhecimento facial. Available at: https://g1.globo.com/sp/sao-paulo/noticia/2022/03/22/justica-de-sp-determina-que-metro-interrompa-implantacao-de-sistema-de-reconhecimento-facial.ghtml

[28] Silva, I. (2022). Siempre seremos prófugos. Available at: https://www.derechosdigitales.org/18439/siempre-seremos-profugos/

[29] Buschmann, J (2022). Chile: Urban crime prediction system: algorithmic production of surveillance and control zones in the city. Available at: https://www.derechosdigitales.org/wp-content/uploads/03_Informe-Chile-Urban-Crime-Prediction-System_ES_28042022.pdf

[30] Carrillo, E., Meira, M. Secaf, H., Zanatta, R. La integración invisible: un estudio sobre el Centro Integrado de Operaciones de Frontera. TEDIC and Data Privacy Brasil. Available at: https://www.tedic.org/wp-content/uploads/2022/02/CIOFTEDICDPrivacyfinalespanol21022022.pdf

2.3. *New legislative efforts to facilitate state surveillance*

Although the interception of communications is technologically feasible, it is only legally permissible under the requirements recognised in international human rights law and standards, including the principles of (i) legality, that refers to the establishment of legal frameworks that express and regulate state surveillance, including its legitimate purposes and means; (ii) necessity, that implies the measure is justified by the lack of alternatives in order to achieve its objective; and (iii) proportionality, which means that there must be a balance between the purpose of surveillance and its impact on the right to privacy.[31]

Although the aforementioned cases often do not comply with these requirements, it is alarming to see that some Latin American governments are seeking to legalise abusive surveillance practices in their legal frameworks. In El Salvador, reforms to the Code of Criminal Procedure were approved by the National Assembly a week after the Pegasus revelations. The reform created the figure of "digital undercover agent" to access citizen communications without the need of a court order, which allows surveillance without justification.[32] A similar figure was lobbied for by the government in Chile, with the prosecution of cybercrime as the excuse,[33] along with attempted efforts to expand Chile's questionable metadata retention mandate and request information without judicial authorisation,[34] though it ultimately failed to pass. In Brazil, a reform to the Code of Criminal Procedure could allow the use of intrusive spyware by law enforcement agencies in spite of expert recommendations that such systems fail to comply with existing human rights standards.[35]

Similar trends at the regulatory level have also been observed when it comes to the adoption of facial recognition systems, including as a way to respond to the increasing judicial questions on their adoption. In addition to a law adopted in Buenos Aires,[36] and a failed attempt in the same direction in São Paulo, Brazil is currently discussing the adoption of a generic bill on artificial intelligence that, besides several other problems, risks creating legal uncertainty and authorising the adoption of such systems at the national level, ignoring all recommendations on the contrary by several international organisations and experts.[37]

---

[31] Becker, S. Canales, M. Lara, J. (2018). La construcción de estándares legales para la vigilancia en América Latina. Derechos Digitales. Available at: https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-I.pdf

[32] Derechos Digitales (2022). Las reformas legales en El Salvador: un gran retroceso en los derechos humanos y el Estado democrático. Available at: https://www.derechosdigitales.org/17840/

[33] Derechos Digitales (2022), El regreso de los delatores en el proyecto de ley de delitos informáticos. Available at: https://www.derechosdigitales.org/14890/

[34] ACTI (2022). ACTI, ONG Derechos Digitales, ALAI, U. de Chile alertan contra Proyecto de Ley que amenaza libertad de expresión en internet. Available at: https://acti.cl/acti-ong-derechos-digitales-alai-u-de-chile-alertan-contra-proyecto-de-ley-que-amenaza-libertad-de-expresion-en-internet/

[35] https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner

[36] Ucciferri, L. (2020). Avanza la regulación del reconocimiento facial en la Legislatura porteña. ADC. Available at: https://adc.org.ar/2020/09/18/avanza-la-regulacion-del-reconocimiento-facial-en-la-legislatura-portena/

[37] A non-official English translation of such bills can be found at: https://www.derechosdigitales.org/wp-content/uploads/Brazil-Bill-No-5051-of-2019-EN.pdf

3. Encryption as a privacy tool

In digital environments, security becomes essential so that the population can exercise their right to privacy and intimacy. Security becomes a more important issue when governments practice surveillance of their citizens and violate digital rights as a systematic practice. The use of tools to protect information and individual communications becomes a necessity. Encryption of communications and of stored information is one such tool. It consists of an "encoding process that prevents confidential information and personal data from being read without consent".[38] Encryption is essential for the transfer of data and information via the internet to be carried out safely and confidentially. In addition, the use of encryption is a factor that strengthens the exercise of rights such as anonymity and freedom of expression in all contexts[39], but especially in those political regimes that promote surveillance of their population.

It has been recommended that government, private and social actions promote encryption within their digital security strategies and policies as a tool to increase trust in communications. However, governments have resisted promoting this practice. This happens due to the false dichotomy between security and privacy,[40] since governments have understood its protection as an obstacle to access communications for purposes of national security or criminal investigations.[41] States' reluctance notwithstanding, civil society organisations increasingly promote the use of this tool, including through the recently created Alliance for Encryption in Latin America and the Caribbean (AC-LAC), a multi-stakeholder consortium that seeks to promote encryption in communications and jointly react to threats to privacy and security.[42]

Encryption is not only resisted as an obstacle for investigation, but also controversial because of the criminalisation of human rights defenders and digital security experts who promote its use. Two worrying examples: in Ecuador, the case of Ola Bini, and in Argentina, the case of Javier Smaldone, both started in 2019.[43] Both these cases have shown the inability of governments to understand the importance of technologies that protect citizen privacy, with a growing stigmatisation of these experts as criminals, when their work has focused on informing and training different actors to live a safer experience in online spaces.

---

https://www.derechosdigitales.org/wp-content/uploads/Brazil-Bill-Law-of-No-21-of-2020-EN.pdf
https://www.derechosdigitales.org/wp-content/uploads/Brazil-Bill-Law-of-No-872-of-2021-EN.pdf

[38] Alianza por el Cifrado en Latinoamérica y Caribe, AC-LAC. ¿De qué hablamos cuando hablamos de cifrado? Available at: https://ac-lac.org/wp-content/uploads/2021/10/aclac-infografía-ok.pdf

[39] ISOC (2016). EncryptionAn Internet Society Public Policy Briefing. Available at: https://www.internetsociety.org/wp-content/uploads/2020/07/PolicyBrief-Encryption.pdf

[40] ISOC (2016). EncryptionAn Internet Society Public Policy Briefing. Available at: https://www.internetsociety.org/wp-content/uploads/2020/07/PolicyBrief-Encryption.pdf

[41] Pereira, A., Rodrigues, G. Vieira, V. Percepciones sobre el cifrado y investigaciones criminales: mapeo y análisis. IRIS-BR. Available at: https://irisbh.com.br/wp-content/uploads/2021/08/Percepciones-sobre-el-cifrado-y-investigaciones-criminales-mapeo-y-analisis-IRIS.pdf

[42] AC-LAC. La AC-LAC se anuncia y propone unir esfuerzos en la región para defender el Cifrado y crear capacidades y conocimiento en torno al tema. Available at: https://ac-lac.org/wp-content/uploads/2021/10/alianza_archivo.pdf

[43] Derechos Digitales (2019). Declaración para la protección de las personas defensoras de los derechos digitales. Available at: https://www.derechosdigitales.org/14065/

***

All of the above is but a brief overview of the challenges to the right to privacy in Latin America in the context of digital communications, and the domino effect that threats to privacy and security present to all other human rights in the region, especially those of activists and journalists, and those of historically marginalised groups. Thus, the promotion of human rights standards for governments and private companies is a crucial necessity in Latin America.

We welcome the opportunity to contribute to the call for inputs, and are happy to receive any comments or questions from your Office on the work of Derechos Digitales on the right to privacy, personal data protection frameworks, and the development of digital technologies in Latin America. We can be reached at ia@derechosdigitales.org.