AI Sur's Submission to the Global Digital Compact: perspectives from Latin America

April, 2023

I. About Al Sur

Al Sur is a consortium of 11 organizations of civil society and academia in Latin America working towards strengthening human rights in the region's digital environment.[1] Its main purpose is to build a space in which Latin American civil society can deepen their understanding of critical aspects, emerging trends and opportunities related to digital technologies and act in a coordinated and strategic manner to influence decision-making from a perspective that is sensitive to the diversity of gender, race, ethnicity and class.

II. About this submission

Latin American countries are affected by persistent inequalities that continue in the digital era and have even greater effects on vulnerable populations. If those are not taken into account within decision-making related to digital and internet governance, technology might deepen such inequalities instead of being instrumental to promote change and achieve the Sustainable Development Goals (SDGs).

The Global Digital Compact (GDC) is a key opportunity to generate a global digital agenda that takes into account the inequities and challenges that affect Latin America as well as the knowledge and experiences from the region. As part of a Global South consortium, Al Sur organizations are aware that the problems related to digital technologies have differentiated impacts in our societies. Such problems and impacts need to be considered within the formulation of a GDC.

Al Sur's submission includes contributions on the following suggested topics: apply human rights online, connect all people to the internet including schools, protect data, and promote regulation of artificial intelligence. The contributions were drafted after a series of collective meetings and joint action building from the experience of the eleven aforementioned members working on human rights and technology issues. The contribution summarizes six years of trajectory and joint reflection on the challenges, realities, lessons learned and proposals systematized in more than 20 collective publications available in English, Portuguese and Spanish.[2]

[1] Asociación por los Derechos Civiles, ADC, Argentina; Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Universidad de Palermo, CELE, Argentina; Coding Rights, Brasil; Derechos Digitales, América Latina; Fundación Karisma, Colombia; Hiperderecho, Perú; Instituto Brasileiro de Defesa do Consumidor, Brasil; Instituto Panameño de Derecho y Nuevas Tecnologías, Panamá; InternetLab, Brasil; Red en Defensa de los Derechos Digitales, México; Tedic, Paraguay. More info: https://www.alsur.lat/quienes-somos

[2] Available at: https://www.alsur.lat/en/reports.

III. Inputs by topic

1. Apply human rights online

At a time of accelerated growth of internet connectivity and an increasingly intensive use of digital technologies – including within the public sector pushed by the isolation measures adopted during the COVID-19 pandemic –, compliance with and protection of human rights in digital environments is one of the greatest challenges for national, regional and global agendas.

Greater commitments are urgent to assure that policies and practices related to the digital sphere incorporate decades of advances in the recognition of human rights standards which have been updated and reinforced considering the particularities of such specific context. The Global Digital Compact has a key role in this regard, to influence stakeholders to assume a greater commitment and responsibility regarding the recognition of human rights online at the individual and collective levels.

From this perspective, this contribution focuses on the rights to freedom of expression and privacy as key enabling rights online.

1.a Freedom of expression

Access to the internet is essential to the exercise of the right to freedom of expression, including access to information, and to a series of related fundamental rights. Besides persistent digital divides, freedom of expression online continues to be limited in various forms in Latin America.[3] Restrictions are both direct and indirect: on the one hand with rules and practices that impose censorship to legitimate content or with internet disruptions, for instance. On the other with the spread of online violence, hate and the use of surveillance technologies to target journalists and human rights defenders, as identified in several Latin American countries (see 1.b), and as key drivers of self-censorship.

Internet disruptions have been reported in several Latin American countries, particularly in the context of protests as identified in recent cases in Colombia and Ecuador.[4] Beyond full national internet shutdowns, the interruption of the operation of specific services or at specific regions has raised concerns over the manner in which information flows can be controlled by states and private entities. Such incidents affecting internet infrastructure are not usually easy to detect but imply concrete impacts to affected groups, such as in the case of the blocking of a website with

[3] See: https://www.oas.org/es/cidh/expresion/informes/IA2021ESP.pdf

[4] APC and Derechos Digitales, "Internet shutdowns and human rights" at https://www.derechosdigitales.org/wp-content/uploads/internet_shutdowns_and_human_rights_ohchr_submission_2022-1.pdf.

information on sexual and reproductive rights in Brazil.[5] Besides affecting legitimate content in a number of cases, they are often a result of interpretations or norms that are not in line with international standards on freedom of expression.

Online gender based violence (OGBV) has been a key concern in the region with female journalists, activists and political figures as a priority target for online harassment and attacks in clear attempts to silence their voices and discourage their possibility to participate in public discussions taking place online. It is important to recall at the same time that while online forms of political gender based violence expand previous and offline violence, their impact goes beyond the online environment, as recognized by the MESECVI and UN Women[6] ".

Recommendations for the Global Digital Compact

- Concrete measures and monitoring mechanisms should be put in place to eradicate all forms of violence against journalists and human rights defenders, including within online environments or with assistance of digital technologies including spyware.
- Limitations to freedom of expression online should follow the same standards as offline limitations and, therefore, be established by law and comply with the conditions necessary for their application according to the three-part test: they must be appropriate, necessary and proportionate.
- Global, regional and local decision-making processes regarding defining concepts that may potentially restrict freedom of expression online should include wide multi-stakeholder participation processes.
    - The GDC should create mechanisms for coordinated dialogue that include the different instances trying to advance concepts, standards and frameworks on the matter –including efforts to fight online gender based violence, desinformation and others at the UN level–, and foster leaders and participants of such initiatives to engage in existing multi-stakeholder spaces such as the Internet Governance Forum (IGF) and its regional and national processes (NRIs).
    - All UN bodies involved in decision-making processes that might have implications for freedom of expression online should consider existing human rights standards, frameworks and criteria, including the three-part test. The Special Rapporteur on Freedom of Expression should be involved and able to review any proposals that might affect freedom of expression online originating from any UN body.
- Online platform providers should include mechanisms to account for cultural and contextual diversity in their content moderation policies and practices and adopt concrete measures to

[5] Coding Rights. (2019, 29 October). On the blocking of pro-choice websites: Women on Waves and Women on Web. Available at: https://medium.com/codingrights/on-the-blocking-of-pro-choice-websites-women-on-waves-and-women-on-web-505ed6f17b63; Braga, N. (2019, 12 December). NET, Claro e Vivo bloqueiam acesso a site com informações sobre aborto seguro. The Intercept. https://theintercept.com/2019/12/12/net-claro-e-vivo-bloqueiam-site-aborto-seguro/

[6] MESECVI and UN Women (2022) Cyberviolence and harassment against women and girls within the Belem Do Para Convention. https://lac.unwomen.org/es/digital-library/publications/2022/04/ciberviolencia-y-ciberacoso-contra-las-mujeres-y-ninas-en-el-marco-de-la-convencion-belem-do-para

protect users from violence, particularly OGBV, by providing proper tools for reporting, quick response and remedy for victims, notification and defense opportunity to alleged perpetrators in order to correct eventual mistakes, as well as publishing periodic transparency reports that indicate prevalence and actions adopted. Zero tolerance policies against OGBV should be adopted and specifically stated on platforms terms of use and no content related to OGBV should be promoted by platforms recommendation algorithms.

- High level standards and supervision mechanisms should be established to guarantee network neutrality and that States and private technology companies respect the free flow of information online.
- Full or partial internet disruptions pose serious challenges to the exercise of a wide range of rights and should be avoided. Any measure that restricts people's ability to fully connect to the internet should be strictly justified through the principles of proportionality and necessity.
- Anonymous and pseudonymous discourses should be protected as key mechanisms for the exercise of freedom of expression online.

1.b Surveillance

In the digital age, the right to privacy has become a gateway to the protection of other rights[7] and therefore requires strong protection as "a necessary precondition for the protection of fundamental values, including liberty, dignity, equality", and "an essential element for democratic societies".[8] The right to privacy can be restricted only in "a carefully circumscribed manner". Interference with the right to privacy is permissible under international human rights law as long as it is not arbitrary or unlawful. Thus, their use must be justified on the basis of effectiveness in the pursuit of a legitimate aim and strict compliance with the principles of legality, necessity and proportionality.

State surveillance has a considerable impact on the exercise of human rights as it can lead to violations of the right to privacy and the right to freedom of expression, as well as allow the use of the information collected for illegitimate and dangerous purposes, including discrimination, persecution, criminalization and violence against people, causing threats to the rights to integrity, life and personal freedom. The UN Human Rights Committee's General Comment 16 on Article 17 of the ICCPR has already stated that the arbitrary collection of personal information by governments constitutes a highly intrusive act that "violates the rights to privacy and freedom of expression and may contradict the principles of a democratic society".[9] Additionally, it may lead to 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.[10] As the UN Special

[7] UN. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, May 20, 2015. Available at: https://www.undocs.org/es/A/HRC/29/32

[8] UN. Report of the Special Rapporteur on the right to privacy, A/HRC/40/63, October 16, 2019. Available at: https://undocs.org/es/A/HRC/40/63

[9] UN - General Comment 16. Human Rights Committee. Art. 17 right to privacy. 32nd session U.N. DOC. HRI/GEN/1/ REV

[10] 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

Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression 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".[11]

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 around the world and within Latin America, often without adequate safeguards in place, resulting in several cases of abuse, particularly against human rights defenders, journalists and activists. This increase is also reflected in the use of these technologies in public policies to address a wide range of social challenges including public security, border control, monitoring of social protests, access to public services, and recently as a way to combat the pandemic.[12] This is done invoking extremely broad purposes such as security or public health, without any analysis of the role of the technology or prior or subsequent evaluations of their impact on fundamental rights[13] which makes it impossible to determine whether the restriction of rights was justified according to the benefit or purpose for which the technology was implemented. There is also a lack of accountability, control mechanisms and tools, which undermines the right of access to justice.

Focusing on Latin America, several investigations have shown the prevalence and usage of targeted surveillance tools, including malware and spyware, against activists and advocates, journalists, and human rights defenders[14] and Al Sur has produced evidence on different surveillance tools used by public authorities. For instance, it has shown that facial recognition systems have advanced with excessive opacity and little commitment from public authorities to ensure minimum conditions in their deployment in order to mitigate the impact on the exercise of fundamental rights.[15]

The exercise of illegal surveillance practices has deepened with the rise of the surveillance industry and the intrusive and sophisticated nature of the technologies used which is especially worrisome

---

[11]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

[12] See: https://www.estamosvigilando-cejil.org/recursos/

[13] See: https://www.estamosvigilando-cejil.org/blog/analisis-final-de-las-respuestas-a-las-solicitudes-de-acceso-a-la-informacion-publica-sobre-el-uso-de-tecnologias-con-capacidad-de-vigilancia-en-el-salvador-2/

[14] See, for instance: AP News, "Press groups: Spyware again used against Mexican activists", 18 April 2023, at: https://apnews.com/article/mexico-pegasus-spyware-activists-press-freedom-army-76477e1d4e3e09250e20aa4896b1f9e1, EFF, "Uncle Sow: Dark Caracal in Latin America", 10 February 2023, at: https://www.eff.org/deeplinks/2023/02/uncle-sow-dark-caracal-latin-america, Access Now, "Pegasus attacks in El Salvador: spyware used to target journalists and activist", 13 January 2022, at: https://www.accessnow.org/press-release/pegasus-el-salvador-spyware-targets-journalists/

[15]See: https://estudio.reconocimientofacial.info/ and Facial recognition in Latin America: trends in the implementation of a perverse technology. Available at: https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia

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.[16] 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".[17]

A history of abuses and deficient regulation on surveillance, particularly when it comes to safeguards, aggravates the risks posed by such technologies to the exercise of fundamental rights. Most attempts to regulate biometric identification technologies in Latin America seem to be more concerned with validating their implementation than with balancing their purpose with respect for human rights, in clear contradiction with their international commitments. Therefore, while specific regulation could be beneficial to strengthen controls and remedy, this will only be possible when its formulation considers a focus on preventing impact and risks to the exercise of fundamental rights, including notably privacy and non-discrimination.

Procurement of advanced surveillance tools by States has thus become a source of concern, as the industry of spyware and malware tools, among others, has risen taking advantage of the lack of proper legal frameworks and democratic oversight, leading to calls for limiting the sale, transfer and use of surveillance tools.[18] In this regard, it is crucial to take into account the recommendations of the United Nations High Commissioner for Human Rights on the need to control the production and sale of surveillance systems that do not respect human rights, as well as to call for a moratorium on those that do not meet the basic criteria.[19]

As some of Alsur organizations have stated in a recent thematic hearing before the IACHR,[20] although there are clear standards on the subject and both the universal and interamerican systems have recognized the risk that surveillance technologies pose to human rights, given the enormous and rapid growth of these technologies and the lack of information and control, these standards are insufficient to prevent impacts. There is a pressing need to develop standards to regulate the acquisition, development and implementation of technologies with surveillance capabilities with a focus on prevention, especially considering that the evaluation of rights violations is always carried out after they have occurred and in many cases this prevents the situation from being remedied.[21]

---

[16] See: https://www.alsur.lat/sites/default/files/2020-04/Al%20Sur%20-%20The%20Surveillance%20Industry%20and%20Human%20Rights_.pdf

[17] See: https://www.alsur.lat/sites/default/files/2020-04/Al%20Sur%20-%20The%20Surveillance%20Industry%20and%20Human%20Rights_.pdf

[18] UN General Assembly, Human Rights Council (28 May, 2019). Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/41/35. Available at: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session41/Documents/A_HRC_41_35.docx

[19] UN News. Urgent action needed over artificial intelligence risks to human rights. Available at: https://news.un.org/en/story/2021/09/1099972

[20] See_ https://youtu.be/IdkYQIpBhoE

[21] See: https://www.estamosvigilando-cejil.org/recursos/.

Recommendations for the Global Digital Compact

- Supervise States compliance to their international human rights commitments with regards to the acquisition and deployment of surveillance technologies emphasizing the need to comply with the principles of necessity, legality and proportionality through case by case analysis.
- Guide and supervise the adoption of human rights based normative frameworks to limit the State's use of surveillance technologies with specific safeguards against abuses, according to the principles of necessity and proportionality and existing obligations regarding access to information and transparency. Such frameworks should include an obligation to apply a moratorium when technologies – such as hacking tools, malware, drones as well as biometric technologies – don't comply with basic human rights criteria.
- Support the strengthening of judicial and oversight institutions and mechanisms, emphasizing on the need of prior judicial authorization for any intrusions to the right to privacy, explicitly guaranteeing the right to an effective remedy, as well as mechanisms of transparency and accountability of States. Support the development of the necessary capacities (financial, human, technical and knowledge) and 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.
- Transparency should guide any State action regarding its general surveillance capabilities, including regarding the scope and extent of the use of private surveillance technologies and safeguard measures implemented to avoid abuses.
- Mandate the adoption of human rights due diligence measures in the acquisition of surveillance technologies in order to assess and monitor potential human rights abuses and/or violations offered by the deployment of such technologies, applying a moratorium on technologies that don't meet the basic criteria.
- Guarantee that mechanisms and standards are in place to assure that the surveillance technology industry complies with their duty to respect and protect human rights, no matter their size, operational context, ownership and structure, as well to avoid causing or contributing to adverse human rights impacts from the deployment of their systems, and address such impacts whenever they occur.
- Stimulate the adoption of mechanisms to prevent and mitigate adverse human rights impacts, as well as to monitor abuses, within the surveillance technologies' industry.

2. Connect all people to the internet

The connectivity challenge in Latin America is still an undeniable reality. To date, less than 50% of the population in Latin America and the Caribbean has fixed broadband connectivity, and only 9.9% have high-quality fiber at home. When thinking about rural-urban connectivity gaps, four out of ten Latin Americans living in rural areas have connectivity options vis a vis 71% of the population in urban areas.[22] Connectivity gaps are a reflection of the inequity that afflicts the region. The link between poverty and inequality has its share in this problem, but there are other disparities that we must acknowledge including that the digital divide also affects more women populations and geographically or socially isolated groups.[23]

To address these challenges and ensure universal access to telecommunication services, States must combine different regulatory initiatives to guarantee the principles of availability, affordability and accessibility, as established by the International Telecommunication Union (ITU)[24]. For this, telecommunication administrations have increasingly adopted Universal Service Funds (USF) as a funding mechanism that is typically funded via some form of contribution from telecommunication service providers.[25] This said, States must protect the nature of these funds. I.e., in Paraguay, there is documentation that such funds have been used to acquire facial recognition cameras to be deployed in the capital instead of actually being applied to expand connectivity to all.[26]

Beyond internet access' key role in the exercise of fundamental rights including freedom of expression (see section 1.a), connectivity becomes each day more a necessity for the fulfillment of States obligation to guarantee the exercise of economic, social and cultural rights.[27] For this to occur, connectivity public policies must go beyond the mere connection objective and adopt a social justice and human rights approach.

Although in some countries of the region there are roadmaps in place to reduce the connectivity gap, they focus mostly on maintaining and strengthening the commercial activity of large operators. This cannot respond to the full diversity of contexts. For instance, the poor infrastructure for rural areas and the often low purchasing power of the people tend to prevent big operators from investing

---

[22] World Bank, 'Low digital access holds back Latin America and the Caribbean. How can this problem be solved?', 12 August 2021, https://blogs.worldbank.org/es/latinamerica/el-escaso-acceso-digital-frena-america-latina-y-el-caribe-como-solucionar-este.

[23] Al Sur, Expanding Internet Connectivity.A Report for the ITU CWG-Internet Open Consultation. Available at: https://www.alsur.lat/sites/default/files/2021-01/Al%20Sur_%20ITU-Expanding%20Internet%20Connectivity.pdf.

[24] International Telecommunication Union, 'Universal Service Fund and Digital Inclusion for All', 2013, https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.SERV_FUND-2013-PDF-E.pdf.

[25] International Telecommunication Union.

[26] TEDIC, 'Biometría y video-vigilancia: La enajenación continua de nuestros derechos [Parte 1]', *TEDIC* (blog), 11 July 2018, https://www.tedic.org/biometria-y-video-vigilancia-parte1/.

[27] ALSUR, 'Regional Report on Technology, Big Data and Cyber-Surveillance', 2018, https://www.alsur.lat/sites/default/files/2020-04/informe%20regional%20sobre%20Tecnolog%C3%ADa%2C%20Big%20Data%20y%20Cibervigilancia.pdf.

in such areas.[28] Consequently, increasing connectivity is not only a matter of expanding coverage, it also requires focusing strategies to reduce inequalities and the search for equal opportunities. Betting on market solutions exclusively foregoes the chance to create other approaches. Solutions that incorporate community networks and local providers should be considered, as both options ensure links to communities and a high degree of contextual awareness.

It is worth noting that schools are essential to include when thinking about connectivity strategies. The COVID-19 pandemic demonstrated the need to connect schools: State actions to strengthen access to the internet in schools are necessary. The Committee on the Rights of the Child has recently published General Comment No. 25, which considers the protection of children in the digital environment to be fundamental.[29] This document points out that States must mobilize, allocate and use resources to ensure children's rights in the digital environment, including connectivity (Paragraph 28).[30] The document also points out that States parties "should not intentionally obstruct or allow other actors to obstruct [...] mobile telephone networks or Internet connectivity in any geographical area [...] in a manner that may have the effect of hindering children's access to information and communication"(Paragraph 54).[31] Finally, the document states that standards for digital educational technologies should ensure that the use of such technologies is ethical and appropriate for educational purposes and does not expose children to violence, discrimination, misuse of their personal data, commercial exploitation or other infringements of their rights, such as the use of digital technologies to document their activities and share this information with their parents or caregivers without children's consent (Paragraph 103)[32].

Transversal to all the above is the State's duty to ensure net neutrality. Currently, zero rating provisions in multiple Latin American markets are a situation that needs to be reflected upon and with the final goal of securing diverse access to the internet in the region that allows local innovation to thrive. States must adopt a focus that provides full and universal access to the internet, rather than concentrating efforts on allowing partial access mediated by operator preferences[33]. Such approach must also be adopted in schools, and avoid plans that only grant access to State digital educational resources[34] since it would limit children's ability to access diverse information.

---

[28] ALSUR, 'Expanding Internet Connectivity', 2020, https://www.alsur.lat/reporte/ampliando-conectividad-internet-0.

[29] MERCOSUR Institute of Public Policies and Human Rights, 'Public Policies against School Bullying and Cyberbullying in MERCOSUR', 2022, https://www.ippdh.mercosur.int/wp-content/uploads/2022/12/Politicas-p%C3%BAblicas-contra-el-acoso-escolar-y-el-ciberacoso-en-el-MERCOSUR.pdf.

[30] Committee on the Rights of the Child, 'General Comment No. 25 on Children's Rights in Relation to the Digital Environment', 2021, https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFO6kx0VqQk6dNAzTPSRNx0myCaUSrDC%2F0d3UDPTV4y05%2B9GME0qMZvh9UPKTXcO12.

[31] Committee on the Rights of the Child.

[32] Committee on the Rights of the Child.

[33] Laura Mora et al., 'How Is Internet Access Contracted in Latin America?', 2016, https://www.tedic.org/wp-content/uploads/2016/06/Informe-ISOC-Final-jun-27.pdf.

[34] Maricarmen Sequera Buzarquis, 'Virtual education and Internet infrastructure in Paraguay', *TEDIC* (blog), 27 April 2020, https://www.tedic.org/la-educacion-virtual-y-la-infraestructura-de-internet-en-paraguay/.

Moreover, full and meaningful connectivity requires considering explicitly the problems faced by people with disabilities (PWD). From a human rights perspective, disability is associated with the idea that it is social and cultural barriers that prevent people from fully exercising their rights. This approach is known as the social model and implies a paradigm shift, in which disability is no longer understood as an individual attribute but rather the result of an environment that imposes barriers and gives rise to exclusion. Disability is, thus, a condition that can disappear if such barriers are removed. The approach was incorporated by the International Convention on the Rights of Persons with Disabilities (2006).[35]

The Convention includes accessibility in its Article No. 9 and states that it means ensuring access for persons with disabilities to their physical surroundings, transport, information and communication services and technologies on an equal basis with others, as well as other public facilities, in urban and rural areas. Although access and accessibility are closely related in the online sphere, there is a difference between connectivity and web accessibility that should be highlighted. The former refers to internet access, meaning the possibility to log into a network through a device. The latter refers to specific environments, such as websites, platforms, or applications being developed with criteria that enable access to the greatest diversity and number of people possible, in both, their programming and design, regardless of their technical skills and types of equipment. Research carried out in some Latin American countries showed that states and companies should increase their efforts to provide web accessibility by developing accessible products and services for PWD.[36]

Recommendations for the Global Digital Compact

- The GDC should acknowledge that providing connectivity for all is part of States' obligations to guarantee the exercise of civil and political, as well as economic, social and cultural rights, and provide that connectivity policies should be implemented considering a human rights framework and a gender-based and social justice perspective. Affirmative actions should be adopted to overcome gender digital divides.
- The GDC should foster the adoption of different regulatory initiatives to guarantee the principles of availability, affordability and accessibility when it comes to connectivity policies and assure that specific measures are implement to overcome urban-rural and gender divides, respecting the self-determination of groups potentially affected by infrastructure deployment and international commitments with prior consultation in case of indigenous areas.
- Policies to advance connectivity for all must combine market-based with community-oriented solutions, especially in rural areas, which includes measures to

[35] Convention on the Rights of Persons with Disabilities, 2006 https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities

[36] Asociación por los Derechos Civiles (ADC), "Persons with disabilities and access to information and communication services", 2019. Available at: https://adc.org.ar/en/reports/persons-with-disabilities-and-access-to-information-and-communication-services/

facilitate access to spectrum by community and locally based internet service providers, including the broad review of electromagnetic spectrum licensing criteria.

- Universal Service Funds should be activated to achieve internet access for all, including schools, prioritizing remote or marginalized areas. Supervision, transparency and accountability mechanisms should be in place to avoid misuse, including with periodic participatory evaluation.
- The GDC should recognize network neutrality as key to achieve connectivity for all and offer explicit guidance regarding for States to limit zero-rating agreements, as well as any other measures that prevent full and meaningful access to the internet as an enabler for the exercise of a number of fundamental rights.
- The GDC must include provisions that encourage States to develop digital literacy policies that considers urban-rural disparities and adopt a gender perspective. More importantly, such policies must not contribute to the already dominant position of Global North tech companies, and must consider open source educational resources when developing such plans.
- The GDC should make explicit that providing connectivity for all includes adopting specific measures to allow people with disabilities (PWD) to fully take advantage of the internet. This includes creating incentives to include PWD in the technology industry, but also adapting existing efforts of digital literacy to account for the needs of PWD, fostering the adoption of legal and technical standards for the development of hardware and software that are accessible, and the review of intellectual property legislation that may prevent the implementation of such standards and in general to allow for access and interaction with all forms of digital content.

3. Protect data

The development and advancement of digital technologies has depended on the massive collection, use and storage of personal data. Since a broader use of social media platforms, the Internet of Things (IoT) and today with Artificial Intelligence (AI), this reliance on personal data processing has been increasing at an accelerated pace.

However, the regulation and data protection frameworks implemented by the States have not kept that pace, even with the most developed countries still lagging behind. Moreover, progress towards strong personal data protection legislation has come into tension with the implementation of surveillance technologies, such as facial recognition systems and the use of spyware for State security purposes. These technologies, in addition to affecting privacy, also have implications for the use of public space by restricting free movement, freedom of association and freedom of expression.

Discussions on data protection frameworks and the rejection of the implementation of harmful technologies also take place in a relationship of unequal power between the owners of the data with respect to the States and companies. While the former have few claiming instruments and must necessarily use platforms and the Internet to access information, communicate and carry out several of their activities, the latter take advantage of these needs.

At the same time, it is also important to mention the power imbalances at the international level. While citizens of countries in the Global North enjoy stronger data and privacy protection frameworks, even extraterritorially, citizens of the global South are subject to greater abuses by companies and States. Civil society organizations, for instance, have reported how the personal data of migrants at the borders of countries in the Global North are collected without proper safeguards and how their conditions are often invisibilized in regulatory discussions at national and international levels.[37] Similarly, technology companies take advantage of legislative and regulatory loopholes to collect personal data from countries in the global South for commercial purposes and the development of their technologies, including the training of Artificial Intelligence models – deepening geopolitical inequalities.

The discussion on international instruments for the fight against cybercrime is also a matter of concern. We have observed the setback that the adoption of the new Protocol to the Convention on Cybercrime of Budapest may imply for personal data, since access to subscriber data without sufficient safeguards may reveal sensitive information about people's online activity and may put activists, human rights defenders, political dissidents and journalists at risk. At a time of discussion of a new international convention to combat cybercrime, data protection at the international level must be adequately safeguarded.

Without strong international instruments to balance these power relations, the interest of security

[37] See, for instance: https://www.accessnow.org/press-release/joint-statement-ai-act-people-on-the-move/.

and economic exploitation of data will prevail to the detriment of individual and collective rights, especially those of people from countries where due regulation does not yet exist.

Finally, considerations about the protection of personal information that might be used to identify persons that wish to remain anonymous needs to be considered. Accessing private information like IP addresses and other online identifiers for the purpose of identifying anonymous online activity can reveal a good deal about individuals' lives—including sensitive details of their interests, beliefs, relations, and intimate lifestyle—and thus such access should be subject to solid protections. As subscriber information is critical to identifying users and can reveal people's activities, expressions, relations, and movements, it can be the tip of the iceberg, revealing a detailed profile about someone. The lack of proper safeguards when disclosing subscriber information puts activists, human rights defenders, dissidents, journalists, and everyday people at risk. Subscriber data, when combined with content or traffic data that is already in the State's possession or can be easily obtained, linked or referenced, can be used to identify specific people involved in expressive activities, their location, and other sensitive information and therefore needs to be protected in a more proactive way.

Recommendations for the Global Digital Compact

- The adoption of robust legislation on personal data protection and access to information should be fostered, as well as standards to balance fundamental rights to privacy, freedom of expression and access to information.
- There is a need to rethink the idea of "informed consent" combining it with other data protection principles in the face of the emergence of new technologies based on data processing. Consent should not be used as a carte blanche and data protection principles such as purpose limitation and data minimization should be considered minimum standards that cannot be waived or revoked at the moment of giving consent.
- Public and private data controllers must follow obligations of loyalty, care and confidentiality, including the prohibition to use the personal data for purposes unknown or different from those motivated for its collection without prior notification and meaningful consent by data subjects and the possibility for them to deny such uses. This is especially relevant regarding biometric data, given its inalienable nature and the potential for enabling mass surveillance.
- States must have independent data protection authorities with due capacities to inspect, monitor and sanction violations by both private and public entities. These authorities must have sufficient human, operational, technical, knowledge and financial resources to be able to effectively monitor compliance. Likewise, their independence and autonomy must be guaranteed so that their actions are guided by the law and not by the influences of interested parties.
- The acquisition and deployment of technologies by the public sector, as well as the digitalization of public services, should be guided by the principles of transparency, legality,

necessity and proportionality and a broad, robust and comprehensive human rights perspective that considers economic, social, cultural and environmental rights.[38]

- The use of big data on public policies at global, regional, national or local levels, including within the UN bodies, should follow strict human rights and data protection principles and should not be implemented if there are risks of abuse, if they involve processing of sensitive data or if they may limit access to essential public services. It is advisable not to dismantle current developments in favor of the right to privacy and data protection for the sole purpose of enabling the implementation of big data policy. On the contrary, these protections should be maintained, strengthened and updated.
- As freedom of expression mandates indicate, the interception, collection and use of personal information must have a clear legal basis in order to protect the individual against arbitrary or abusive interference with his or her private interests. The law should establish limits on the nature, scope and duration of such measures, the reasons for ordering them, the authorities competent to authorize, execute and supervise them, and the legal mechanisms for challenging them.
- Legal surveillance of communications should be carried out only when necessary and proportional. There must be ways to control and monitor the use of these tools. Any excess should be sanctioned.
- States must establish specific controls for access to databases and their use for the identification of individuals, for example, under judicial authorization in criminal cases, which in turn must be based on certain more serious crimes.
- States must adopt legislative, administrative and other measures with high standards for the protection of personal data and human rights in general; specifically, in relation to cross-border criminal investigations. Criminal procedural safeguards must be respected, including the provision of prior judicial authorization for access to subscriber data, the establishment or preservation of strong privacy safeguards and increased levels of privacy protection, etc. The UN should foster the highest protection standards on this matter and guide implementation by member States.
- Service providers should train their employees and develop robust security protocols. They should also be trained in human rights impact assessment, checking the legality, proportionality and local context of cross-border direct cooperation requests.

[38] Facial recognition in Latin America: trends in the implementation of a perverse technology. Available at: https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia

4. Promote the regulation of artificial intelligence

Artificial Intelligence (AI) characteristics such as high complexity, autonomous behavior, the need for large amounts of data to operate and opacity can negatively affect several fundamental rights such as privacy, freedom of expression, access to justice, among others. The impacts on human rights in the use of AI have already been acknowledged in various resolutions at the international level. The recent UN Human Rights Council Resolution A/HRC/RES/48/4 on the right to privacy in the digital age[39] has delineated some of the risks of adopting AI for the exercise of human rights, which occur "primarily when [AI] is employed for identification, tracking, profiling, facial recognition, behavioral prediction, and for establishing scores for individuals."[40] The Resolution establishes that States must respect human rights when it comes to implementing such systems and adopt preventive measures and remedies for violations and abuses of the right to privacy, especially of women, children, and people in vulnerable conditions.

In a similar vein, the report by the UN High Commissioner for Human Rights, Michelle Bachelet, points to the serious risks to privacy posed by the use of AI tools.[41] According to Bachelet, profiling, the automation of decision-making and machine learning technologies have a major impact on the right to privacy and several other associated rights in at least four specific sectors: police forces and investigations, national security, criminal justice, and border controls. According to the former High Commissioner, these systems add further opacity that prevents true State accountability for violations in areas that have historically suffered from a lack of transparency. The use of AI in remote biometric recognition (facial and emotion recognition) is also severely criticized by the report, as it impairs "people's ability to live their lives unobserved and resulting in a direct negative effect on the exercise of the rights to freedom of expression, peaceful assembly and association, and freedom of movement.

In Latin America, there is an alarming trend of increasing use of AI systems- in many cases used in sensitive areas of public policy such as to provide State services without proper public debate or specific rules limiting their use, having serious impacts on the exercise of human rights.[42] The implementation of automated facial recognition technology in public spaces has also increased in the region with little safeguards and transparency considerations, thus allowing for the continuous and ubiquitous re-identification and de-anonymisation of citizens and subjecting them to constant surveillance.[43]

---

[39] A/HRC/RES/48/4. Available at: https://undocs.org/A/HRC/RES/48/4

[40] A/HRC/RES/48/4. Available at: https://undocs.org/A/HRC/RES/48/4

[41] A/HRC/48/31. Available at: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx

[42] This is the case of the Horus Project for the prediction of adolescent pregnancy and school dropout implemented in Argentina and in the process of expansion to other countries in the region, including Brazil. See: Peña, Paz & Varon, Joana. Case study: Plataforma Tecnológica de Intervención Social / Projecto Horus - Argentina and Brazil. Available at: https://notmy.ai/news/case-study-plataforma-tecnologica-de-intervencion-social-argentina-and-brazil/

[43] See: https://estudio.reconocimientofacial.info/ and Facial recognition in Latin America: trends in the implementation of a perverse technology. Available at:

Although the developments related to the implementation of AI were dominated by private initiatives, the public sector already plays an important role in encouraging the use of AI technologies either from a regulatory perspective with the development of AI strategies that incentives their development and deployment,[44] or from an implementation perspective by directly acquiring, developing or adopting them.[45] In many cases, this incentive comes at the expense of States' international human rights obligations and best practices in terms of transparency, oversight and public accountability.[46] The adoption of these systems by States often foregoes transparent bidding processes, and public-private alliances are based on agreements with companies, without adequate guarantees that the necessary measures have been taken to mitigate and remedy any violations of fundamental rights or that less harmful options have been considered to address a given issue. Furthermore, neither in the case of private or own system developments, there are no sufficiently implemented transparency and review measures for automated decisions[47].

Research conducted by Derechos Digitales on the use of these systems to provide State services, such as those linked to social interventions in Chile, justice administration in Colombia, job allocation in Brazil, and public health management in Uruguay, shows that most initiatives process personal information, including sensitive information, without sufficient guarantees for data subjects, including in terms of meaningful consent. In this context, they are forced into relationships with actors widely unknown to them in order to exercise social and economic rights such as social security, the right to work, the right to healthcare, and access to justice.[48]

Considering the issues outlined, there is a pressing need for a human rights based regulation of the development and implementation of AI systems as a regulatory approach is essential to strengthen the coercive capacity needed to address concrete violations derived from the implementation of AI systems.[49] While our analysis shows that data privacy laws are often the main source of control to prevent abuses, they are still not sufficiently mature in most countries to be applied to such complex contexts and sometimes they fall short in offering specific protections against the impacts of AI.

---

https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia.

[44] See: https://www.derechosdigitales.org/wp-content/uploads/DD-Call-for-input-OHCHR-privacy-in-the-digital-age.pdf

[45] Venturini, Jamila; Velasco, Patricio. Decisões automatizadas na gestão pública na América Latina - Uma abordagem comparativa da sua aplicação no Brasil, Chile, Colômbia e Uruguai. Derechos Digitales, 2021. Available at: https://www.derechosdigitales.org/wp-content/uploads/08_Informe-Comparado- PT_180222.pdf

[46] See: Souza, Michel R. Artificial intelligence 2021: important developments in the international legal framework. Available at: https://www.derechosdigitales.org/17675/artificial-intelligence-2021-important-developments-in-the-international-legal-framework/

[47] Available at: https://covid.alsur.lat/pt/

[48] Available at: https://www.derechosdigitales.org/wp-content/uploads/DD-Call-for-input-OHCHR-privacy-in-the-digital-age.pdf

[49] See:: Canales, Maria Paz. What do we talk about when we talk about AI? Algorithmic decision- making in Latin America. Em: Latin America in a Glimpse. Derechos Digitales, 2020. Available at: https://www.derechosdigitales.org/wp-content/uploads/glimpse-2019-4-eng.pdf

UNESCO Recommendation on Ethics and AI,[50] approved by its 193 member states, is a key reference in advancing contextually-sensitive regulation on AI and further agreements on the matter should be built from such a basis.

Recommendations for the Global Digital Compact

- Reinforce all stakeholders' obligation to respect human rights within the development and deployment of AI systems, expressly emphasizing that the promotion of non-discrimination and diversity must be addressed throughout the entire life cycle of IA systems, from their design to their implementation and evaluation. Such obligation should include the need to respect the principles of legality, necessity and proportionality and provisions mandating the conduct of human rights impact assessments prior to the development, acquisition or deployment of AI systems should be advanced considering particular regional contexts. Assessments should consider a holistic and integrated conception of human rights, taking into consideration the economic, social, cultural, and environmental rights and paying special attention to the potential impacts on vulnerable groups and individuals, including women, children and adolescents, persons with disabilities, and the elderly, as well as potential structural impacts on the increase of pre-existing inequalities.
- Encourage effective multi-stakeholder and multidisciplinary participation in decision-making during the full life-cycle of AI systems, including their design, development, acquisition, deployment, evaluation and monitoring, as well as the production of human rights impact assessments, through specific recommendations, as well specific considerations regarding the need for affirmative actions to guarantee inclusion of historically marginalized groups in decision-making processes. Considering persisting digital divides, offline mechanisms should be considered to complement online access to information and consultation processes.
- Encourage and guide the establishment of monitoring and control mechanisms: Develop standards for periodic mechanisms for evaluation, monitoring and accountability throughout the IA life cycle. It's important to incorporate sustained external evaluations in the different stages of implementing the public policy, to foster the detection and correction of errors, particularly as regards emerging situations that have not been contemplated in the design stages.
- In relation to the principles of transparency and publicity, clear obligations must be established regarding the publication reporting and evaluation mechanisms implemented by providers, which must include information about identified risks/abuses, transparency about who are the actors involved, how the system is developed, what data are used, among other important aspects; planned mitigation or remediation measures, as well as concrete justifications for the continuation or discontinuation of ongoing initiatives.

[50] Available at: https://www.unesco.org/es/legal-affairs/recommendation-ethics-artificial-intelligence?TSPD_101_R0=080713870fab20007beacf3e8f33f18d52aa7b2e816794305061bf5bdee3a5765371e3cf9866e08b086bb9d86d1430002c870150ac49cedbd4fb98c8fd0b1011bafcd7a84b937f19baa70b54312c66d13149eca18f2e9de8339fa0ef8e6bb57d

- UN and intergovernmental bodies should observe such all above recommendations and adopt specific participation, human rights impact assessments and accountability mechanisms regarding their own processes for standard development, financial support mechanisms and direct development, acquisition and deployment of AI systems.
- Encourage collaboration between more advanced economies and those in regions such as Latin America to foster development of skills, breach knowledge gaps, enhance local industry, and focus growth on the equal satisfaction of human necessities from an inclusive, human-centric and rights-respecting perspective. Discourage development of technologies that create risks for human rights, such as surveillance technologies.