DERECHOS DIGITALES
América Latina

A Latin American perspective on the use of AI systems by the State

Derechos Digitales' contribution to the upcoming report by the United Nations High Commissioner for Human Rights on the right to privacy in the digital age

About Derechos Digitales

Derechos Digitales is an independent non-profit organisation, founded in 2005, with main offices in Santiago de Chile. Our aim is the defence and promotion of fundamental rights in the digital environment in all of Latin America, using advocacy tools among policymakers, private companies and the general public to promote social change around the respect and dignity of all people. Derechos Digitales has contributed to previous reports on privacy in the digital age, and has also conducted research on human issues raised by artificial intelligence (AI) systems and technologies. From our policy analysis, research, an advocacy work, we submit for your consideration the following.

1. Specific impacts on the enjoyment of the right to privacy caused by the use of artificial intelligence

In Latin America, the developments related to the implementation of AI technologies come mainly from private initiatives, either from transnational corporations based in the global north or local articulations of relevant actors, including universities and research centres. The factors that promote the implementation of AI technologies are mainly related to the articulation between the notion of development and the role of technologies to favor an "efficient" supply chain of various goods and services.

The promises articulated by this type of technologies are built mainly around the capabilities of advanced data processing, and most of the time there is no clear diagnosis that critically justifies their need. Even leading to institutional development proposals being articulated around the implementation of technologies rather than question their adequacy.[1]

Thus, the deployment of AI technologies seeks to find its legitimacy and recognition under the promise of the efficiency that technological solutions can offer. This favours the interests of the promoters of this type of solutions, usually private actors, who offer technological alternatives that promise contributions on addressing the institutional development gaps that can be observed in Latin America.

[1] Valderrama, M. (2020) Chile: Sistema alerta niñez, available at: https://ia.derechosdigitales.org/wp-content/uploads/2021/03/CPC_informe_Chile.pdf

The data collection and analysis facilitated by AI systems is a powerful tool of meaning-making[2], ordering knowledge about the world and focusing our collective attention to the purposes served by the system implementers, being those State actors or the companies that offer those technologies to States. And more often than not there is a negative feedback loop between those two related to the incentive of the private sector to provide for solutions that allow governments to reduce the political frictions of inaction in key policy areas such as determining access to social welfare, the resolution of judicial conflicts, healthcare services provision or employment matching.

The challenges that AI technologies pose for the exercise of the right to privacy have two different sides. On the one hand, the research and development of AI systems normally requires the collection and processing of large amounts of data, including personal data. Therefore, the availability of personal information for the development of AI systems that will be used to classify or make decisions impacting citizens, will become a source of concern from the perspective of the right to privacy. This is the case for most AI and other algorithmic decision-making systems in Latin America, as analysed by Derechos Digitales.[3] The lack of attention to limit data collection to what is proportionate and adequate for a system's goals, puts us with a landscape in which governments of the region are more focused in massive collection of data through different interactions, even for processes or services that would otherwise not require it, in order to accumulate and exploit that information later through new systems.

Secondly, the use of AI itself presents serious risks for its capacity to further process personal information, including sensitive data. AI systems can optimise data processing given their speed, the scale of its capacities (i.e., the use of gigantic data sets), and their capabilities to process without supervision, all of which improve efficiency at the expense of human participation. This turns previously human-operated systems in public administration into dark holes where it is almost impossible for citizens to determine in which moment and by which part of the system processing there have been mistakes or problems with inputs that lead to harmful impacts to them.

The use of AI can be aimed to defeat the exercise of personal autonomy. AI can be used to identify and to monitor individuals, both online and offline. Tracking systems can follow an individual through different online communications, and AI can be used to re-identify and de-anonymise them based on this tracking. The use of facial recognition systems can compromise anonymity in public spaces, while also collecting further biometric information for the purposes of surveillance by tracking individuals physically. These systems have been multiplying recently in many cities Latin America, as reported by Derechos Digitales.[4]

Finally, AI systems can infer information from the available data that they have on individuals. From this, AI systems can be used to profile individuals, by classifying and ranking their constructed profiles, which can be used to make decisions about citizens. More alarmingly, this profiling can be used to infer health conditions, emotions, personal

[2] Maciej Kuziemski, Gianluca Misuraca, AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings, Telecommunications Policy, Volume 44, Issue 6, 2020,101976, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2020.101976.

[3] "Decisiones automatizadas en la función pública en América Latina", available at: https://ia.derechosdigitales.org/wp-content/uploads/2021/03/CPC_informeComparado.pdf

[4] See https://www.reconocimientofacial.info.

relations, sexual orientation, and other personal information that would not be otherwise shared with the entities operating AI systems. And this profiling and inference can be used to predict, adding negative impacts on personal autonomy and with it civil and political rights, but also expose individuals and groups to discrimination in the exercise of their economic and social rights.

There is research, particularly in global north countries, on the ability of AI technologies to reproduce and exalt biases that potentially articulate arbitrary discrimination mechanisms based on criteria such as gender, age or skin colour[5]. In addition to such issues, it is important to note that, when evaluating the application of such technologies by States, not only the potential emergence of such forms of discrimination is worrying, but also the institutional weakness of the State in the countries of the region. This results in institutional blindness when considering, for example, marginalised and vulnerable groups (on the basis of age, geographic location, ethnic origin, gender, among others) that are "invisible" when the State acts and designs its policies.

Based on research by Derechos Digitales,[6] it is not yet possible to identify intended mechanisms of discrimination in the application of AI technologies for public functions in Latin America. However, the lack of technical and regulatory safeguards allows such errors to be the result of the system deployment, a risk of high probability considering the low level of evaluation and public auditing of the technologies implemented.

Derechos Digitales has led research to identify 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. The research found direct links between private information, including sensitive information, as part of the information that is processed for the exercise of the rights to social security, the right to work, the right to healthcare, and access to justice. Therefore, collection and automated processing of information becomes an integral part of that provision of services and exercise of rights. In our analysis,[7] national data privacy laws are often the main source of control to prevent abuse, however, still in many countries such protections are weak or do not exist. The protection and promotion of the right to privacy in the digital age requires making sure that systems that process personal data as part of automated decision-making processes, on which the exercise of rights depends, be subject to strict privacy-enhancing rules.

Also, as it has been tracked by Derechos Digitales,[8] the Latin American region has grown in its use of automated facial recognition technology implementations in public spaces, thus allowing for the continuous and ubiquitous re-identification and de-anonymisation of citizens and subjecting them to constant surveillance. This application of ever-improving AI technology has not been implemented with sufficient safeguards for fundamental rights, negatively affecting the exercise of the right to protest, including negative impacts on freedom of movement, freedom of expression, and freedom of peaceful assembly. Only a

[5] Zuiderveen, F. (2018). Discrimination, intelligence and algorithmic decision-making. Directorate General of Democracy, Council of Europe.

[6] See Inteligencia Artificial e Inclusión en América Latina. Case Studies, https://ia.derechosdigitales.org/en/casos/

[7] "Decisiones automatizadas en la función pública en América Latina", https://ia.derechosdigitales.org/wp-content/uploads/2021/03/CPC_informeComparado.pdf

[8] See https://www.reconocimientofacial.info.

recent judicial ruling put a stop to such a system in São Paulo's public transport,[9] while implementation continues in Brazil and many other countries in the region.

It is important to note that these developments often involve economic interests in the public procurement and deployment of these technologies under efficiency narratives. Many of these systems are provided by private vendors to public entities, disproportionately promoting the alleged benefits but without proper consideration for the need to promote privacy-preserving technologies or accompany them with improvements on the currently limited data protection laws. Wrong incentives can thus be the source of wrong AI implementation where better data controls should be in place. The asymmetry of information between public administration eager to quick solutions to long term institutional problems of efficiency in public policies, and private companies eager to expand the market for their technologies, make a wrongful match to provide better scrutiny of the limitations and risks of the technologies offered.

2. Legislative and regulatory frameworks

Several Latin American countries are attempting to adopt principles and guidelines for the use of AI, following global trends. Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico and Peru have adhered to the OECD Principles on Artificial Intelligence.[10] However, recent research[11] has shown an underrepresentation of global south perspectives in global debates around AI and ethics, which are influential on policy debates on the matter, resulting in frameworks that may not be adequate for the region.

Despite such gaps, some countries have already developed AI national strategies, such as Argentina, Colombia and Uruguay, while others are in the phase of drafting theirs, like Brazil, Chile and Mexico. Although most initiatives declare to be open to respond to ethical concerns in AI, the reality is that they more often respond to market pressures to guarantee legal environments that can foster the adoption of AI products and services. Argentina, Mexico and Uruguay have adopted Council of Europe's Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data. These can be considered regional leaders when it comes to data protection, with relatively updated national laws and strong enforcement institutions. Other countries still have limited data protection frameworks when it comes to international standards and best practices in the matter or face limitations on the institutional capacities of their oversight bodies, such as Brazil, Chile, Colombia and Mexico. Brazil, Ecuador and Panama have only recently adopted their general data protection frameworks, while Bolivia, despite having fragmented provisions on privacy and data protection, is still in an early stage of discussing the approval of a unified norm.

Some positive innovations are observed, like the provision on the review of automated decisions, present in the Brazilian data protection framework, and also under discussion to update current legislation in Argentina and Chile. Such a mechanism, initially accounting for a *human* review of automated decisions, is inspired by the European General Data

[9] https://www.biometricupdate.com/202105/face-biometrics-systems-shut-down-in-washington-dc-and-sao-paulo-brazil

[10] See https://www.oecd.org/going-digital/ai/principles/

[11] See https://www.nature.com/articles/s42256-019-0088-2

Protection Regulation (GDPR), but the human element was finally vetoed by the Brazilian federal government in the final version of the law.

At the same time, DD research on the concrete applications of automated decision systems by governments in Brazil, Chile, Colombia and Uruguay, showed that data protection frameworks were limited, particularly due to the wide exceptions on the demand for consent in the public sector. In practice, this makes it harder for citizens to be properly informed on new forms of treatment of their data, including sensitive data. Such weak informed consent mechanisms imply the impossibility of reviewing decisions made by publicly implemented automated systems.

In some cases, the COVID-19 pandemic has been used to weaken existing guarantees. In Brazil, the Executive used its power to expand its surveillance capacities by authorizing the unification of a large number of databases, against existing data protection legislation.[12] The fact that States already collect and store indefinitely an enormous amount of data from citizens cannot represent a general authorisation for uses beyond their stated purpose. But what we witness in Latin America is that purpose limitation is usually defeated by broad exceptions in favor of public administration. There is an urgent need for updated data protection provisions for stronger consent when involving automated systems and derived uses of previously collected data for new purposes, particularly when treatment involves sharing it with third (public or private) parties.

Our research emphasises the current shortcomings in the legal frameworks in the Latin American region regarding transparency and participation mechanisms, as well as citizen supervision. This is a fatal loophole, for systems that may impact privacy and autonomy, but also put citizens at risk of discrimination when applied to control access to State programs and services.[13] AI systems can result in the exclusion of groups from accessing public spaces and programmes, deepening pre-existing inequalities.[14] As mentioned, Latin America has seen a surge in facial recognition deployment without any space for consultation, any prior human rights impact assessment, and with no mechanisms for monitoring and evaluation that can justify expenditure and risks. But while we agree with the proposal of a global ban on facial recognition systems, other AI systems may result equally harmful.

3. Other safeguards and measures to prevent violations of privacy when using AI, and address and remedy them

Faced with the rapid advance of artificial intelligence technologies and the attempts to regulate this sector, we observe the emergence of various guides and orientations responding to the challenges involved in AI deployment. Research[15] has identified the existence of

[12] Coding Rights, Cadastro Base do Cidadão: A Megabases de dados, 2020, https://www.codingrights.org/docs/megabase.pdf

[13] See https://privacyinternational.org/news-analysis/4478/derechos-digitales-publish-report-id-systems-and-social-protection-venezuela-and

[14] See https://privacyinternational.org/news-analysis/3263/surveillance-and-social-control-how-technology-reinforces-structural-inequality

[15] Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nat Mach Intell 1, 389–399 (2019). https://doi.org/10.1038/s42256-019-0088-2

dozens of documents of principles and ethical frameworks related to artificial intelligence developed by public or private actors at the local or international level. However, we can point out at least two limitations in those documents. On the one hand, there is a marked absence in the debate of voices from the global south, and specifically from Latin America, which implies the lack of sensitivity of these proposals of the context of regional context, evolution and needs. On the other hand, the emphasis on ethical perspectives and privacy concerns seems to neglect the need to pay attention to broader international human rights standards.

Resistance to approaching the issue from a regulatory framework is additionally related to a perception of a “race of merits” from countries to show capacity for innovation, with the fear that clearer standards linked to human rights will discourage private investment, which would be directed elsewhere. This has had the direct consequence of Latin American governments directing their energy to create national AI strategies rather than regulatory frameworks for its development. Those instruments usually serve as diagnostic tools of capacities and strategic lines of action, which are attractive for private actors to engage, but rarely emphasise risk assessments or preparedness of public administrations and companies to maintain respect for human rights when implementing and managing these technologies.

Shortcomings in regulation and risk assessments are followed by an AI policy debate heavily skewed towards voluntary standards and self-governance, disregarding power imbalances and informational asymmetries. Broad concepts as “trustworthiness” and “fairness” are used to describe inherent qualities attributed to the proposed systems. But trustworthiness is rather a result than an intrinsic value, a product of reaching benchmarks and fulfilling expectations. It is the result of setting a governance structure for which the ethical considerations provide little concrete guide. In the same way, although “fairness in AI” has been in fashion, it is “equity” that better describes just outcomes from certain systems. Fairness as inherent value does little for explaining which efforts are required, and which stages of the life cycle of an AI system should be tested and evaluated for equity.

From our perspective, in all these guidance initiatives greater emphasis should be put on human dignity in relation to existing human rights instruments, standards and documentation from UN bodies. Besides, the individual and collective dimensions of human dignity should be considered, in the sense of self-determination of nations and groups. The deployment of AI systems modeled by global north companies and offered to global south governments challenges the ability to conduct rational and free decisions for exercising freedoms for individuals and groups.

The goal for States and companies many times is the opposite: to standardise measures and interactions. Therefore, those goals are the ones reflected in the ethical guidelines selected for ruling AI systems, and they provide insufficient safeguard and remedy for broader human rights impact. What we have found in our research is that the decision itself to implement and use AI should be subject to analysis under its impact to human dignity and self-determination, which are part of a political discussion that exceed proposed ethical frameworks. There must be room to refrain from using these technologies based on this analysis when their more likely result of implementation will cause more harm than good, and in that case they should be replaced by other types of measures.

In this evaluation, what usually escapes AI ethical frameworks is the question of *optimising for what*? Authorities should open a democratic debate with the community regarding the aims of the technical solutions, according to international human rights standards and their duty to promote and protect human.

Although the range of options can be wide, the motivations for AI system deployment can usually be grouped into two main variants: solutions that seek to address problems of efficiency and effectiveness in the use of public resources, and those that can be used as components to ensure the exercise of rights and the construction of social justice.[16] Those objectives are not incompatible, but they are not always considered together in public decision-making on the adoption of technology, nor clearly stated as points of evaluation by ethical guidelines. Usually those guidance start from a techno-solutionism standpoint, full of utopian optimism of the intrinsic value of the proposed technology and dazzled by its capacity and they attempt to mitigate rather than refrain from negative impacts.[17]

In this sense, since often the declared goal of many public sector's AI systems deployment is to improve the productivity and quality of services and moving from what it has been currently done to what could be valuable, from our perspective it will be useful to advance additional efforts from private companies and international cooperation entities to help governments (particularly in the global south) to assess the suitability of existing performance measurement tools, or develop new ones to effectively measure the contribution of AI systems to the problems they are intended to solve.[18] The move to social change driven by AI should not be forced or collectively embraced without concrete and clear evidence of how this new complexity layer of social systems will contribute to social justice and human rights. The burden of proof should be on technology developers, international cooperation promoters and government implementers, not civil society and academia.

To this end, what seems more urgent are frameworks for evaluating the potential impact of the use of AI in the public sector that are adapted to local realities and global south governments. From Derechos Digitales, we are currently working on the design of assessment tools that move in that direction for Latin American decision makers. We have chosen this practical approach to the subject, taking advantage of what has been already debated and the common trends in the principles identified that speak of human dignity, privacy, transparency, equity, responsibility, oversight, redress and democratic engagement, which are repeated through different standards, although with divergence in their interpretation.

***

We welcome any comments or questions on the work of Derechos Digitales on artificial intelligence, the right to privacy and the development of digital technologies in Latin America. We can be reached at ia@derechosdigitales.org

[16] What Do We Talk When We Talk About AI: Algorithmic Decision-Making in Latin America (2020) María Paz Canales, https://www.derechosdigitales.org/wp-content/uploads/glimpse-2019-4-eng.pdf

[17] See World Economic Forum, AI Procurement in a Box, 2020, https://www.weforum.org/reports/ai-procurement-in-a-box

[18] A useful attempt from a technical perspective has been done by the IADB and its initiative FAIr LAC. See González, Felipe; Ortiz, Teresa; Sánchez Ávalos, Roberto, IA Responsable: Manual técnico: Ciclo de vida de la inteligencia artificial, 2020, IADB, https://publications.iadb.org/es/ia-responsable-manual-tecnico-ciclo-de-vida-de-la-inteligencia-artificial