Public consultation

Ethics and Data Protection in Artificial Intelligence: continuing the debate. A contribution from Latin America & the Caribbean

The organizations signing this document are part of the consortium Al Sur, an organized group from civil society in Latin America that seeks to strengthen human rights in the digital environment. The public consultation[1] on "Ethics and Data Protection in Artificial Intelligence: continuing the debate" [2] promoted by the ICDPPC *(International Conference of Data Protection and Privacy Commissioners)* is a new opportunity for Global South and Latin American perspectives to be part of the debate around ethics and data protection in the context of Artificial Intelligence (AI).[3] We believe that the considerations in this document could complement in-depth and complexity some aspects of the ICDPPC declaration.

In this regard, we appreciate that the statement presented by ICDPPC recognizes that the development of AI increasingly threats respect for rights such as privacy and data protection and that its development must be complemented with ethical and human rights considerations. Responding to this greater challenge, it seems crucial that ICDPPC has detected the need for data protection and privacy authorities to work together with other human rights authorities in order to develop perspectives that respond to the complexity demanded by Artificial Intelligence systems.

And it is precisely in this context of recognizing the complexity of scenarios that Artificial Intelligence presents, in addition to the unequal distribution of power among all interested parties involved in the AI developments and outcomes, that the signatory organizations suggest considering the following aspects in some of the principles proposed by the ICDPPC.

- **Opting for the use of the international Human Rights framework to assess the effects of AI**

We celebrate the incorporation of the idea of ethics in a coordinated way with the concept of "privacy by design", which has gained popularity thanks to the General Regulation of Data Protection (GDPR) of the European Union. However, we are cautious about the generality of the concept "ethics by design" and, therefore, its potential danger of being a battlefield coveted by values of dominant cultures from the Global North that do not necessarily respond to cultural diversity. In this regard, we join the call of specialists such as Eileen Donahoe (Executive Director, Global Digital Policy Incubator, Stanford University) when she states that "**our existing human rights framework is an invaluable lens through which to assess the effects of AI on human beings and humanity**".[4]

Using the existing framework internationally agreed on human rights offers several advantages, among which it is found that in many countries -both in the North and the Global South- there is already advanced legislation on the matter, in addition to standards that have been developed by regional systems to protect fundamental rights. All this allows us to be better prepared to face AI's impact on the exercise of multiple rights of individuals and communities, such as the civil, political, economic, social, and cultural rights.

- **Explicit recognition of groups in a particular condition of vulnerability due to AI systems**

According to available evidence, today, it could be affirmed that -as the ICDPPC declaration recognizes- the use of Artificial Intelligence has an impact not only on individuals but also significantly on social groups. However, it seems fundamental to us an explicit acknowledgment in the declaration that there are "groups in a situation of special vulnerability" regarding the harmful effects on their human rights by AI systems.

In Latin America and the Caribbean we observe with concern several cases regarding this point: for example, the use of the PredPol Software by the Ministry of the Interior of Uruguay in order to identify sections of the city where crimes are most likely to be committed has been questioned by local and international organizations as these tools "tend to replicate the biases of training data and the historical power dynamics between law enforcement and minority or underprivileged populations and that they are used to justify police presence in marginalized areas".[5] Similar criticisms have had systems that aim to automatically predict adolescent pregnancies in the province of Salta, Argentina,[6] as well as the recently launched system to predict social vulnerability risks in childhood and adolescence in Chile.[7]

The explicit recognition of the situation of vulnerability of certain social groups, on the one hand, makes more evident the need for both companies and policymakers to take a contextual look at the effects of AI in each of their countries and, on the other, to allow to the same data protection authorities to compare and understand the effects on the most vulnerable communities of our societies.

- **The responsibilities of the States should be explicit when they use AI systems to facilitate public policies.**

Likewise, we believe States should be explicit in the caring of human rights whenever an AI system is purchased, designed and/or implemented to define its public policies, as they are the main guarantors of the strengthening of these rights. This is particularly relevant because, as we have seen in the previous point of this document, human rights are undermined when many of these systems end up automating discriminatory policies towards, particularly vulnerable populations.

In Latin America, this is especially problematic due to little or no transparency concerning how data has been collected and the explicit authorization of data holders (or their legal representatives) for secondary data uses, like those implemented in many AI systems. Likewise, in a regional context of relative normative weakness respecting personal data protection standards and authorities in charge of making this protection effective, the database purification or the possibility of the affected citizen to complain about the outcomes of AI is rather scarce or null.

- **Recognize tensions that AI introduces to the traditional data protection system and, from that point, advance in agreed solutions.**

As stated in the statement, the information must be delivered in a timely and intelligible way to individuals when they interact directly with an AI system or when they provide personal data to be processed by such systems. However, we believe that these solutions are based on a vision about the freedom of the individuals that do not consider their inequality of power, knowledge, and resources. If we incorporate these last elements into the analysis, we can realize that the decision capacity of people is strongly limited. That is why we consider it fundamental to make explicit at least two aspects that should complement the traditional approach on the topic in the context of AI:

The uncertainty of the principle of purpose: For authors like Zeynep Tufekci,[8] companies cannot inform us about the risks we accept, not necessarily because they are acting in bad faith, but because computational methods are increasingly powerful -such as machine learning- and they work like a "black box," that is, not even those who have access to code and data could know the consequences that a system has on our privacy. In this sense, fundamental matters such as the principle of the purpose of data collection may end up compromised.

The difficulty of informed consent: Besides, since the operation of this type of system is highly complex even for their own developers, it seems unfair that individuals bear the responsibility of informing themselves and understanding matters as arid as its impact on their human rights. In this context, it is important to recognize that traditional forms of data protection, such as informed consent by users no longer have the same supposed efficacy in complex systems such as AI. Moreover, informed consent can be used as an excuse to legitimize the impact on privacy and data protection. Therefore, obligations to respect rights must be fulfilled regardless a consent is obtained. In the same way that happens in other areas where inequality of position between parties has been recognized (labor law, consumer law, among others), consent must be considered as a requirement that joins other duties and not as something that replaces them.

With this background, it is important to recognize traditional data protection systems weak points, and therefore commit ourselves to advance in agreed mechanisms that allow strengthening the supervision of AI systems, set boundaries with respect to our human rights, and implement mechanisms of public transparency.

- **Be explicit on the activities assumed by authorities supervising AI systems**.

Consistent with what was stated in the previous point, we recognize the vital importance that authorities have today supervising AI, as they are the engine to promote accountability of all relevant stakeholders in these systems. Thus, we believe it is very important to be explicit regarding three aspects of the work by State supervisor authorities:

- It is important that these authorities (whether data protection authorities or similar) have powers authorized by law and, therefore, with a consistent budget and trained human resources, in order to address the complex study scenarios that AI demands in the protection of Human Rights.

- Likewise, the authority's independence must be expressly guaranteed.
- Responding to the complexity of the AI scenarios and the inequality of budgets regarding accountability -especially between North and Global South- transparent cooperation mechanisms must be established among authorities, academia, private sector, and civil society in order to facilitate the discussion on evidence and impacts.

States that use AI systems to define their public policies, in any of their areas, should also have mechanisms for transparency, auditing and accountability -by independent committees- from the development of the system concept, its tendering, databases used to feed the system and its development and implementation over time.

- **Point out the oligopolistic forces of the market and its effect on AI**

Although the statement acknowledges "the potential risks induced by the current trend of market concentration in the field of artificial intelligence", we believe it is fundamental to recognize and expressly ensure the balance of power of all parties involved in the systems of Artificial Intelligence and, in particular, to be explicit about the risks people could face due to the dominant position that a handful of companies have reached offering digital services (which are mainly powered by data from their users) such as Facebook, Google, Amazon, among others.

In order to improve its effectiveness, AI needs large amounts of data- It is worrisome the domain level that these companies currently have in the market regarding the exploitation of the personal data of their users. This domain, which escapes traditional logic of evaluation by competition rules as their services offers are diverse; it is aggravated by the participation of such companies in multiple vertically integrated markets, as well as by the public recognition that some of them share personal data of their users with other companies.[9]

Likewise, whether it is already difficult for countries in the Global North to achieve a certain level of accountability by these companies, the task becomes even more difficult for countries in the Global South that often lack a strong institutional framework in terms of competition and consumer protection. We urge ICDPPC to explicitly recognize this market reality regarding companies developing and/or implementing IA and therefore be able to create special control and accountability mechanisms for this type of oligopolies in Artificial Intelligence.

- **Security in AI systems and their outcomes**

The adoption of digital security mechanisms according to human rights standards is a matter of the utmost importance. In this sense, we understand that adopting a rights perspective to define "digital security" implies that the center of analysis shouldn't be concepts such as "national interest," "national security," "economic interest," or similar. On the contrary, digital security should focus on the ability of people to interact with technology in a way that is beneficial for their needs and preferences, and without disproportionately exposing them to risks of controlling their autonomy and identity.

The first aspect of digital security in AI systems is related to the fact that actors must incorporate practices that guarantee integrity, confidentiality, and availability of the system, to avoid

malicious interference in the system feeding data and its decision making, or the deviation from the original purpose of its use.

In addition, they must ensure that people who can be impacted by AI decisions are provided with the necessary tools to critically understand and analyze it and determine if their use could contribute or harm their life situation. In this sense, it cannot be ignored that millions of people in Latin America and the Caribbean - and in the rest of the world - live in conditions of poverty and low educational level, and therefore their risk of marginalization could be increased by the application of AI. Moreover, they could even not be able to access information or understand the consequences of such systems. This social inequality must also be addressed by the ICDPPC as part of a real effort to ensure the safe use of AI.

:::

This document was signed on January 25, 2019 by the following organizations:

- Derechos Digitales. Latina America. (derechosdigitales.org)
- Asociación por los Derechos Civiles (ADC). Argentina. (adcdigital.org.ar)
- Hiperderecho. Peru. (hiperderecho.org)
- IPANDETEC. Panama. (ipandetec.org)
- Red en Defensa de los Derechos Digitales (R3D). México. (r3d.mx)
- TEDIC. Paraguay. (tedic.org)
- Fundación Karisma. Colombia. (karisma.org.co)
- Coding Rights. Brazil. (codingrights.org)
- Idec. Brazil. (idec.org.br)

[1] Public consultation – Ethics and Data Protection in Artificial Intelligence: Consultation extended until 15 February 2019. ICDPPC. October 31, 2018 https://icdppc.org/public-consultation-ethics-and-data-protection-in-artificial-intelligence-continuing-the-debate/
[2] Declaration on Ethics and Data Protection in Artificial Intelligence. ICDPPC. October 23, 2018 https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf
[3] For the purposes of this report, we refer to the full spectrum of different intelligences and data-based processes with the name of Artificial Intelligence or AI: from automated and algorithmic decision-making; to machine learning, including deep learning that mimics biological neural networks, among others.
[4] Human-Centered AI: Building Trust, Democracy, and Human Rights by Design. Donahoe, Eileen. 9 de julio del 2018. https://medium.com/stanfords-gdpi/human-centered-ai-building-trust-democracy-and-human-rights-by-design-2fc14a0b48af
[5] Ortiz Freuler, J. and Iglesias, C. (2018). Algorithms and Artificial Intelligence in Latin America: A Study of Implementation by Governments in Argentina and Uruguay, World Wide Web Foundation.

[6] Sobre la predicción automática de embarazos adolescentes. Laboratorio de Inteligencia Artificial Aplicada. https://liaa.dc.uba.ar/es/sobre-la-prediccion-automatica-de-embarazos-adolescentes/
[7] Expertos advierten riesgos en uso de big data para prevenir vulneraciones a niños. La Segunda. 14 de enero 2018. http://impresa.lasegunda.com/2019/01/14/A/SN3HIO68/all
[8] The Latest Data Privacy Debacle. Zeynep Tufekci. 30 de enero 2018. https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html
[9] Facebook Used People's Data to Favor Certain Partners and Punish Rivals, Documents Show. The New York Times. 5 de diciembre del 2018. https://www.nytimes.com/2018/12/05/technology/facebook-documents-uk-parliament.html?smid=tw-nytimes&smtyp=cur