March 13, 2020

Principles on Identification for Sustainable Development

Call for Consultation

Submission by Asociación por los Derechos Civiles[1]

We welcome the opportunity to submit comments under the Call for Consultation in regards to the World Bank's ID4D Principles. In the following report we will highlight our pressing concerns about the text of the Principles themselves, as well as on how these Principles are currently being deployed in existing systems. In this last case, we will base our analysis on the case study published by the World Bank titled "Argentina ID Case Study: The Evolution of Identification", the portrayal of this case by the Bank as an example on ID development is quite worrying, not only because of its lack of in-depth analysis on the nuances of the identification system in Argentina, but, more importantly for this consultation, because it doesn't even follow the very core philosophy behind the Principles.

About ADC

The Asociación por los Derechos Civiles (ADC)[2] is a non-governmental, independent and non-profit organization founded in 1995, based in Buenos Aires, Argentina. ADC's aim is to defend and promote the exercise of civil and fundamental rights in Argentina and Latin America, with a special focus on the needs of those in vulnerable situations due to their gender, nationality, religion, disability condition, or deprivation of liberty.

Over its 25 years, ADC raised strategic allegations of human rights violations, promoted legal and institutional reforms aimed at improving the quality of Argentinian democratic institutions and influenced positively in public policymaking processes. This activity has been recognised at a national and international level for its expertise and efficacy in the defense and promotion of civil rights and democratic values. ADC also has stood out in its fight for the promotion and defense of the founding principles of the Rule of Law.

Moreover, ADC has remained at the forefront of the human and civil rights defense in different political, social and cultural contexts, in both Argentina and Latin America. Thus,

---

[1] This briefing was written by Leandro Ucciferri, Ssr. Project Officer, ADC. lucciferri@adc.org.ar

[2] https://adc.org.ar

aware of the increasing digitalisation and the use of technology in the various public and private fields, ADC has undertaken the mission of understanding the impact of digital technologies on human rights.

Since 2014, ADC has been publishing research and analysis on the uses of biometric technologies and their intrinsic relationship with our bodies and identities. More recently, the focus was broadened in order to challenge and shed light on the narratives that are promoted by governments to justify the implementation of biometrics which has been increasingly related to the concept of "digital identity".[3]

ID4D Principles

The title of the Principles mention that their focus is set on "identification", but throughout the text we also encounter mentions to "identity". These concepts should be treated in accordance with their proper nuance, in order to avoid any misunderstanding as if they were synonyms. Identity is not only the "set of attributes that uniquely describes an individual or entity", but a more complex concept that sees its roots both on the socio-economic context as well as the sum of the experiences that a person encountered throughout their life, resulting in the characteristics that comprise aspects of their personality. In this regard, "identity" exceeds the notion of legal status.

In this context, we must also emphasise that identity shouldn't be seen as a merely bureaucratic issue to be dealt with, but focusing instead on the nuances that arise from the diversity of the population and that interplays with potential social, economic and cultural implications, especially considering the introduction of technology for the deployment of identification systems.

As the human rights organization Privacy International further explains: *"the design of any system that tries to lock [the concept of identity] down is going to fail in some way to fully recognise the magnificent diversity in human beings when it comes to identity. The change, the flux, the contextual richness of 'identity' is not easy to encompass in these digital*

---

[3] Some of the latest reports on these issues published by ADC include:
"The Identity We Can't Change" (2017): https://adc.org.ar/en/reports/the-identity-we-cant-change-sibios/

"Fintech: privacy challenges in the data economy" (2019): https://adc.org.ar/en/reports/fintech-privacy-challenges-in-the-data-economy/

"Tu yo digital – Descubriendo las narrativas sobre identidad y biometría en América Latina" (2019)
https://adc.org.ar/informes/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/

systems. That is the challenge of these systems – and, unfortunately, an imperfect design can have a legacy that goes on for generations."[4]

1. Ensuring a universal coverage for individuals from birth to death, free from discrimination.

4. Creating a platform that is interoperable and responsive to the needs of various users.

Although Principle 1 mentions universality and non-discrimination, there should be stronger wording to account for the risks of exclusion that arise from ID schemes. Particularly in the context of biometrics-based systems. As the technology industry promotes their own solutions and developments to governments that are eager to comply with the Sustainable Development Goals, there's an increasing risk that ID systems will be implemented without considerations on bias and how it may affect their own population. Biometrics, particularly facial recognition, can negatively impact women, the LGBTQI+ community, the elderly, and people with disabilities.

Moreover, in regards to the considerations that should be addressed concerning people with disabilities, particular attention must be brought amid the increasing development of online platforms and apps that are used as part of ID schemes. These tools should be developed from the ground up considering the use-cases of people with disabilities, in order to comply with accessibility standards.[5]

Accessibility standards should also be taken into account when developing the very platforms in which ID schemes will be based. Identification systems shouldn't discriminate on the basis of the individuals' capacity.

Regarding the aspects of interoperability in Principle 4, technical features that allow several databases to communicate or exchange information between each other shouldn't disregard the purpose for which the data was collected in the first place. We will further expand on this point in Principle 8.

5. Using open standards and ensuring vendor and technology neutrality.

---

[4] "Identity, discrimination, and the challenge of ID", Privacy International (2018): https://privacyinternational.org/long-read/2274/identity-discrimination-and-challenge-id

[5] One example of standards for web development are the Content Accessibility Guidelines provided by the W3C: https://www.w3.org/WAI/standards-guidelines/wcag/

Together with open standards, greater emphasis should be added on the need of independent security audits and the role of information security experts. No system is infallible, and in an increasingly digital world systems must be meticulously inspected and studied, particularly with consideration to socio-cultural contexts.

In this regard, systems are expected to be designed with digital security in mind both at the backend/infrastructure level, as well as on the frontend/user level. Independent and transparent audits of the technology on ID systems is essential for building trust and introducing further accountability. Digital security should be addressed as a continuos risk assessment, constantly evaluating potential consequences and vulnerability threats, as highlighted as well by the OECD.[6] The auditing processes should also include considerations on how ID systems can be abused by internal staff at government agencies or businesses.

When addressing vendor and technology neutrality, one cannot be oblivious of the lobbying power of the private sector and the close relationship that businesses build with government officials.

Regarding vendor "lock-in", it is worth illustrating with the situation in Argentina. For the development of the new Digital Identity System in 2017, the Ministry of Interior and the former Secretariat of Modernisation decided to acquire the facial recognition software to the same company with which the Ministry of Interior had contracted in the past for the rest of its infrastructure, in order to ensure maximum compatibility.[7]

"Just try again" can't be an official response when biometric systems fails to authenticate an identity, as one citizen reported being told after numerous attempts of using Argentina's Digital Identity System, implemented not only for governmental use cases (e.g. as the app "Mi Argentina" and AFIP, the tax revenue agency) but also to register for new fintech services run by private businesses.[8]

Identification systems shouldn't rely solely on one technology or solution (e.g. facial recognition, as in the case of Argentina's Digital Identity System), alternatives must be built into the core structures of these systems and schemes, not only as a way of upholding

---

[6] Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document, available at: https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

[7] Confirmed through a formal reply by the former Secretariat of Modernisation to ADC's freedom of information request in September 2018.

[8] Maximiliano Firtman, "No me gusta tu cara": ¿discriminan las aplicaciones?, La Nación, September 2019: https://www.lanacion.com.ar/tecnologia/no-me-gusta-tu-cara-discriminan-aplicaciones-nid2292711

technology neutrality, but also as a measure to mitigate bias and discrimination, while promoting accessibility.

6. Protecting user privacy and control through system design.

The incorporation of Privacy by design into Principle 6 is a good starting point, which must be considered together with the addition of privacy impact assessments, as a requirement for every stage of the research, development and implementation of ID schemes. These privacy impact assessments must also be revisited throughout the lifespan of the identification system.

Further clarification should be made when referring to "global norms" for data protection under "Proportionality and minimal disclosure". Taking into account the swift technological change that ID schemes have faced in recent years, the Principles should highlight standards and norms that are more adequate to the digital age.

In that regard, we can mention two bodies of data protection standards that have been developed to address the challenges of technology innovations. The modernized Convention for the protection of individuals with regard to the processing of personal data, known as Convention 108+, from the Council of Europe,[9] together with the Data Protection Standards for Ibero-American States, from the Ibero-American Data Protection Network.[10] These bodies offer a more comprehensive approach to privacy and data protection suitable to analyse how modern technological implementations of identification systems can interfere with fundamental rights.

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.

We believe privacy should play a crosswise role in identification schemes, as the fundamental right that enables the exercise and enjoyment of other rights.

In this regard, the concepts of consent and purpose, as addressed in data protection regulations, should be strongly highlighted in the Principles. This becomes even more important when taking into account the context of the countries where ID schemes are mandatory and essential for everyday life in order to function as a human being in a modern

[9] Convention for the protection of individuals with regard to the processing of personal data: https://www.coe.int/en/web/data-protection/convention108/modernised

[10] Estándares de protección de datos personales para los estados iberoamericanos: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

society. As individuals cannot escape that reality, it is urgent to incorporate considerations about how these systems can be turned against citizens, particularly vulnerable communities.

Moreover, we want to bring attention to the mention of “self-regulation” as a framework model. The private sector, especially the biometric industry, has played a key role in the push towards digitised identification systems adopted by governments. Businesses are the main players developing the solutions that are later on marketed to government officials in order to deploy digital identity schemes and modernise the infrastructure behind the systems. Sensitive aspects such as data protection, security, non-discrimination and bias can’t be left alone to be solved by the industry. On the contrary, these issues call for multiple stakeholder involvement in order to have as a comprehensive representation as possible.

In order to illustrate how Principle 8 can be loosely interpreted to analyse a current identification scheme, it is worth mentioning the case study published by the World Bank on Argentina together with key aspects that were not included in the report.

Even though Argentina was indeed one of the first countries in Latin America to establish civil registries, the national ID card as we know it today was born through an Executive Order dating to the military dictatorship of Juan Carlos Onganía in 1968.[11] In this context, the expressions used in the norm take on a new meaning. Its very title, "Identification, Registration and Classification of the Human Potential", reveals an aim of control rather than a mere recognition of legal identity. The lack of a democratic debate around the introduction of this identification scheme, which was not possible at the time given the political context, was increasingly left on the side given the prevalence of the ID number in the everyday life of Argentines.

Subsequent reforms of the identification system were carried out through Executive Decrees and Ministerial resolutions. The introduction of biometric technology and more recently the new Digital Identity System, were not discussed democratically, in an open, inclusive and transparent framework. On the contrary, they were decided unilaterally by public officials within the Executive Power.

Moreover, when addressing data protection safeguards, although the Argentine law is based on European standards, there are provisions within the legislations that allows too much discretion to the State when collecting, processing and sharing personal data.

---

[11] The Collecting State. A Study About Argentina and Citizen’s Personal Data, ADC (2014): https://adc.org.ar/wp-content/uploads/2019/06/003-A-the-collecting-state-09-2014.pdf

Articles 5.2.b and 11 of Law 25.326, provide exceptions that enable government agencies to not require the consent of individuals when collecting their data under the "exercise of functions of the State", as well as in the cases of transferring said data within State bodies.

Thanks to these provisions, what should be understood as an ID scheme that is required to carry out civic life in Argentine society, was expanded to other purposes. Such is the case of SIBIOS, a federal biometric database that can be accessed by multiple government agencies (particularly, police forces throughout the country), without court orders or warrants, without a justification of an imminent danger in an active judicial investigation, or even notifying the individual whose data was shared, with whom and for what.[12]

These policies cannot be understood as a "comprehensive legal and regulatory framework", as stated by the World Bank's case study, or even as in compliance with the very essence of the Principles in question.

Suggestions

1. Introduce further language to strengthen data protection on ID systems

Consent should be –as a minimum– freely given, informed and revocable. Consent should never be assumed or automatic.

Strong restrictions on data sharing purposes must be established specifically for ID systems, not only within private businesses, but also within State bodies and agencies. These limitations should be established by law and be transparent, so as to define really specific and connected use-cases, in order to avoid abuses and excessively broad interpretations for using the ID systems and its data in ways were their users didn't originally consented.

Individuals should have the right to not be subject of automated decisions that impacts their rights, either directly or indirectly. In these cases, human intervention must be introduced. Moreover, individuals should have a direct and transparent way of asking for an explanation about the decisions made about them and/or with their data, together with proper redress mechanisms to revisit decisions.

[12] For further information read "The Identity We Can't Change" (ADC, 2017).

2. Provide clarity about the meaning behind “comprehensive legal and regulatory frameworks”

In order to build proper legal and operational foundations to establish trust and accountability among the various stakeholders involved in ID systems, comprehensive legislations and regulations must be set.

On a very elemental level, this means that legislation must be debated and decided upon democratic standards. Governments should refrain from using and abusing unilateral decision-making channels to introduce new systems and technologies that present risks to fundamental rights.

Identifications systems, at their very core, must be built with a democratic perspective, involving an open, inclusive and transparent framework, where the parties that will be involved and affected can give shape to the outcome.

In our increasingly digital society, comprehensive legal frameworks that impact ID systems, directly or indirectly, include having specific legislations, not only for the ID systems themselves, but also for the technologies used, such as the case of biometrics and the use of biometric data.

3. Introduce Privacy Impact Assessments and Human Rights Impact Assessments

The introduction of Privacy Impact Assessments (PIA), or even more specifically Data Protection Impact Assessments (DPIA), serve as a baseline process for building and demonstrating compliance. As these assessments are scalable, they should be carried out throughout the different stages –creation, development and deployment– of ID systems, as well as periodically throughout the system’s life time.

The basic steps of a DPIA include:

a) providing a systematic description of the personal data processing. Including the nature, scope, context, purpose, functional description of the operations, assets in which personal data rely;
b) assess the necessity and proportionality. Are there specified, explicit and legitimate purposes, is the system adequate, relevant and limited to what is necessary data;
c) managing risks to the rights and freedoms of data subjects. Identifying the origin, nature, particularity and severity of the risks, as well as their consideration from the point of view of the data subject;
d) include interested parties, as Data Protection Officers and the views of data subjects.

For further details about this framework, there's the guidelines developed by the Article 29 Working Party.[13]

In addition, both businesses and governments should carry out broader Human Rights Impact Assessments (HRIA) when working on the development and deployment of ID schemes. For example, in order to identify potential bias and discrimination in algorithms used in the systems, and then taking measures to mitigate this risk.

Human Rights Impact Assessments are comprised of five phases:

I. Planning and scoping: activities, human rights context and stakeholders, developing terms of reference.
II. Data collection and baseline development: including the selection of indicators.
III. Analysing impacts: types of human rights impacts and assessing their severity.
IV. Impact mitigation and management: Actions to address impacts, monitoring and access to remedy.
V. Reporting and evaluation: Challenges and approaches.

The Danish Institute for Human Rights provides comprehensive and in-depth guidelines for each phase, in order to tailor and implement the framework for the specific context in which they are carried out.[14]

---

[13] Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[14] The Danish Institute for Human Rights, Human rights impact assessment guidance and toolbox, available at: https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox-0