The Mexican unique digital ID (CUID) proposal threatens human rights

Honorable Chamber of Senators of the Federal Legislative Power of Mexico,

The undersigned organizations express our concern regarding the draft General Population Law, and in particular regarding the mandatory "Unique Digital Identity Card" (CUID) project, which would be built using a centralized database compiling the biometric data of all Mexican citizens and all foreigners who are in Mexico.

The CUID seriously threatens human rights for the following reasons:

1. **There is no solid evidence of the usefulness of massive biometric identification systems**

   Biometric data is neither the only nor the most effective way to legally identify a person. It has been proven that this type of system entails errors or risks that decrease the fidelity of the identification, such as:

   - **Intrinsic recognition inaccuracies**: The technology available shows problems in correctly identifying people with darker complexions. In Mexico, where around 67% of the population self-classify their skin color as medium tones and 20% as dark tones, the system could have this problem, excluding millions of people from its use and potentially condemning it to disuse despite the high public spending.

- **Technology hoaxes:** The biometric identification system can fail. Technology can be deceived with the use of deepfakes (a technique that plausibly impersonates the identity of a person in a video, recreating facial characteristics, gestures, and sounds) and even copying fingerprints from photographs taken from social networks, which has generated security problems for years in Germany and identity theft in Peru. With the advancement of technology, biometric data can potentially lose its uniqueness.

- **Information leaks**: Once the data is leaked to third parties, a recurring problem, the collected biometric data can no longer be trusted, as it can be used by other people. Unlike a password, which can be easily changed, biometric data cannot be easily changed. In Estonia, after a security breach in the cryptographic keys of more than 750,000 digital identification cards, the government had to lock them and take drastic measures to restore the system; this would not have been possible if the flaw had compromised biometric data.

- **Social exclusion**: This biometric system presupposes that everyone can supply all the requested data, when sometimes the person simply may not have the required characteristics. An example of this are people who do not have fingerprints, which would leave them outside the identification system, and from different public bodies that guarantee access to other human rights, such as health, housing, etc.

2. The CUID database's centralized design presents a serious risk of data breach, and the consequences can be irreversible or very difficult to repair

These are the most important risks of collecting and processing biometric data in a national identification system.

- **High-value target:** Centralized systems are insecure, as they are a single point of attack that allows the disclosure of large and diverse personal information. The leakage and theft of data from a centralized system compromises people's entire lives. This risk was criticized during the judicial process that assessed the constitutionality of the integrated national identity management system in Kenya. According to expert Anand Venkatanarayanan, who testified before the Grand Court of the country, the centralized system is an archaic model since today decentralized models are preferred for greater security.

- **Impersonation:** When biometric data is leaked or stolen it is always possible for third parties to use it to impersonate other people. As stated in the Report of the United Nations High Commissioner for Human Rights (Resolution A/HRC/39/29), "*identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights.*" According to the CUID proposal, identity theft can prevent access to public and private services, including through the attribution of criminal actions.

The right to privacy and freedoms of movement and expression are guarantees that the Mexican State has undertaken to defend, and that this initiative directly threatens. The potential benefits of digital identification, which can also work without biometric data, do not compensate for or justify putting citizens in jeopardy. For these reasons, we strongly recommend the elimination of biometric data collection.

3. Mandatory registration for the CUID using biometric data will disproportionately affect vulnerable populations

Mandatory registration for CUID further exacerbates the risk of exclusion, profiling, and surveillance. This happens both when the law

makes it mandatory and when the identity document becomes the only means of identification to access services, making it *de facto* mandatory.

- **No consent:** If registration for the CUID is mandatory, as the current proposal requires, people will lose the freedom to decide whether or not they should put their rights at risk by providing biometric data. Making either the ID itself or collection of biometric data mandatory is in direct contradiction with the State's legal and political duty to protect human rights, since anyone who is unwilling or unable to comply would be completely excluded from society. It should be noted that this lack of consent was one of the points that led the Supreme Court of Jamaica to declare unconstitutional the first project to establish a National Digital Identification System. Currently, the new legislative proposal in Jamaica establishes that registration must be voluntary.

- **Exclusion from essential services:** If the registration is voluntary but the digital identification becomes the only means of accessing services, the most vulnerable populations will be those who are once again excluded. In India it was believed that, with the creation of the voluntary Aadhaar identification system, thousands of Indians could finally be identified and have access to social services. However, the opposite happened. Over time, the Aadhaar number has been linked to the provision of various private and public services, making it indispensable for living. The problem is that accessing this biometric identification is difficult in a country with huge social and technological differences. The consequences are so disastrous that there were people who starved to death simply because they did not have an identification card.

Mexico is among the 25% of the countries with the greatest social inequality in the world. Adding another factor of exclusion from social

and private services, especially for vulnerable groups, can have severe repercussions for the economy, health, and development of the country.

These risks are solved by allowing the coexistence of multiple identification systems, without the CUID prevailing over others, and above all, allowing the delivery of biometric data to be voluntary and not mandatory.

4. **The use of CUID as a condition for access to public and private services — particularly when combined with biometric data — allows for the massive and permanent monitoring of the population**

   Mexico has a long history of state surveillance, and we must carefully guard against the expansion of these practices that seriously harm human rights.

   - **Mass and targeted biometric surveillance:** The creation of a centralized database with biometric information will expand the government's surveillance capacity. Further, creating a unique digital identity card to access public transport services, legal processes (such as complaints or suits), and banking systems, among others, gives the State extraordinary power over its inhabitants. Especially in combination with existing surveillance tools that have a history of abuse, this database could be used both to monitor and restrict people's freedom of movement and association, as well as to persecute activists, journalists, representatives of the opposition, and minorities, among others.

   - **Temptation of expansion:** Due to the large amount of centralized data that contains information on people's day-to-day lives, this database is attractive for profiling people by analyzing their behavior patterns on an ongoing basis, even if the government isn't conducting that type of surveillance now. In Argentina, it has been

seen that from the creation of a centralized and biometric database, surveillance activities have increased, including the creation of the Federal System of Biometric Identification for Security fed by the civil registry database.

Diversifying identity documents by giving them each the same relevance reduces the chances of mass surveillance. Likewise, it is essential that criteria, rules and prohibitions are established for sharing personal data, including logs, that is, the record of activity in a system.

Recommendations

Considering the serious risks that the CUID project represents, it is essential to modify the draft in a way that makes it possible to consider alternative mechanisms that guarantee the right to legal identity without putting the privacy and security of more than 130 million people at risk in an unnecessary and potentially irreversible way, without generating an instrument for mass surveillance, and without putting conditions on access to services with disproportionate effects on vulnerable populations.

In particular, we recommend the following:

1. Do not include biometric data as part of the National Population Registry.
2. Determine that the CUID should rest on decentralized systems.
3. Establish that obtaining the CUID is optional.
4. Prevent making access to public or private services conditional on obtaining the CUID.
5. Prevent the collection, storage, or transfer of data that records the use of the CUID.

Signatories:

Access Now - Global
AfroLeadership - Africa
Arturo J. Carrillo - The George Washington University Law School, USA
Asociación por los Derechos Civiles (ADC) - Argentina
Centro Latam Digital - Latin America
Coding Rights - Brazil
Cooperativa Tierra Común - Mexico
Damian Loreti - Universidad de Buenos Aires, Argentina
Datos Protegidos - Chile
Datysoc, Laboratorio de Datos y Sociedad - Uruguay
Derechos Digitales - Latin America
Fundación Acceso - Central America
Fundación InternetBolivia.org - Bolivia
Gambia Cyber Security Alliance - Gambia
Instituto Brasileiro de Defesa do Consumidor (IDEC) - Brazil
Instituto para la Sociedad de la Información y Cuarta Revolución Industrial - Peru
Ipandetec - Central America
Laboratório de Políticas Públicas e Internet (LAPIN) - Brazil
Luchadoras - Mexico
Privacy International - Global
R3D: Red en Defensa de los Derechos Digitales - Mexico
SeguDigital - Mexico
Senegal ICT Users Association (ASUTIC) - Senegal
Sula Batsú - Costa Rica
Sursiendo, Comunicación y Cultura Digital - Mexico
TEDIC - Paraguay
The Civil Pole for Development and Human Rights - Tunisia