La cédula única de identidad digital incluida en la Ley General de Población amenaza los derechos humanos

Honorable Cámara de Senadores del Poder Legislativo Federal de los Estados Unidos Mexicanos,

Las organizaciones que suscribimos esta carta manifestamos nuestra preocupación acerca de la minuta que expide la Ley General de Población, en particular, respecto al proyecto "Cédula Única de Identidad Digital" (CUID), de carácter obligatorio, que pretende construirse sobre una base de datos centralizada que incluya los datos biométricos de todos los ciudadanos mexicanos y de todas las personas extranjeras que se encuentren en México.

A continuación se detallan las razones por las que la CUID amenaza gravemente los derechos humanos.

1. No existe evidencia sólida de la utilidad de los sistemas masivos de identificación biométrica

Los datos biométricos no son la única manera ni la más efectiva para identificar legalmente a una persona. Se ha comprobado que este tipo de sistemas conllevan errores o riesgos que disminuyen la fidelidad de la identificación, como son:

- **Imprecisiones intrínsecas de reconocimiento**: La tecnología con la que se dispone muestra problemas para identificar correctamente a

personas de tez más oscura. En México, donde alrededor de un 67% de la población autoclasifica su color de piel en tonos medios y un 20% en tonos oscuros, el sistema podría caer en este problema, excluyendo a millones de personas y potencialmente condenándolo al desuso, a pesar de haber incurrido en un gasto público elevado.

- **Engaños a la tecnología:** El sistema de identificación biométrico puede fallar. Es posible engañar a la tecnología con el uso de *deepfakes* (ultrafalsos, técnica que permite suplantar de manera plausible la identidad de una persona en un video, recreando las características faciales, gestos y sonidos) e incluso copiando huellas dactilares a partir de fotografías tomadas de redes sociales, lo que ha generado problemas de seguridad desde hace años en Alemania y de suplantación de identidad en Perú. Con el avance de la tecnología, los datos biométricos pueden potencialmente perder su singularidad.

- **Filtración de información:** Una vez que los datos se filtran a terceros, un problema recurrente, ya no se puede confiar en los datos biométricos recolectados, debido a que pueden ser utilizados por otras personas. A diferencia de una contraseña, que puede ser fácilmente cambiada, los datos biométricos son difíciles de modificar. En Estonia, tras una falla de seguridad en las llaves criptográficas de más de 750 mil tarjetas de identificación digital, el gobierno tuvo que bloquearlas y tomar medidas drásticas para restaurar el sistema; ello no habría sido posible si la falla hubiera comprometido datos biométricos.

- **Exclusión social:** Este tipo de sistemas apunta a que todas las personas pueden suministrar todos los datos solicitados, pero en ocasiones, la persona puede sencillamente no contar con las características requeridas. Ejemplo de ello son las personas que no tienen huellas dactilares, lo que las dejaría al margen del sistema de identificación y,

con ello, de diferentes instancias públicas que garantizan el acceso a otros derechos humanos, como la salud, la vivienda, etcétera.

2. El diseño centralizado de la base de datos de la CUID presenta un grave riesgo de vulneración de los datos, cuyas consecuencias pueden ser irreversibles o muy difíciles de reparar

Estos son los riesgos más importantes de recolectar y procesar datos biométricos en un sistema de identificación nacional.

- **Base de datos de gran valor para los atacantes:** Los sistemas centralizados son inseguros, ya que constituyen un único punto de ataque que permite la revelación de una cantidad grande y diversa de información personal. La filtración y robo de los datos de un sistema centralizado compromete la vida entera de las personas. Este riesgo fue criticado durante el proceso judicial que evaluó la constitucionalidad del sistema nacional integrado de administración de identidad en Kenia. De acuerdo con el experto Anand Venkatanarayanan, que testificó ante la Gran Corte del país, el sistema centralizado es un modelo arcaico, ya que hoy se prefieren los modelos descentralizados para mayor seguridad.

- **Suplantación de identidad:** Al momento de que los datos biométricos son filtrados o robados, siempre es posible que terceros los empleen para suplantar la identidad de otras personas. Como señala el Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (Resolución A/HRC/39/29) "(...) el robo de la identidad a través de los datos biométricos es muy difícil de reparar y puede afectar gravemente a los derechos de una persona". De acuerdo a la propuesta de creación del CUID, la suplantación de identidad puede impedir el acceso a servicios públicos y privados, incluyendo la atribución de acciones delictivas.

El derecho a la privacidad y las libertades de movimiento y de expresión son garantías que el Estado mexicano se ha comprometido a defender y que se ven directamente amenazadas con este tipo de iniciativas. Los potenciales beneficios de una identificación digital, que además puede funcionar sin datos biométricos, no compensan ni justifican la exposición de la ciudadanía a peligros. Por todo lo anterior, recomendamos fervientemente la eliminación de la recolección de datos biométricos.

3. La obligatoriedad del registro para el CUID usando datos biométricos afectará desproporcionadamente a poblaciones vulnerables

El registro obligatorio para obtener la CUID exacerba aún más el riesgo de exclusión, elaboración de perfiles y vigilancia. Esto sucede tanto cuando lo hacen obligatorio por ley, como cuando el documento de identidad se vuelve el único medio de identificación para acceder a servicios, volviéndolo de *facto* obligatorio.

- **Sin consentimiento:** Si el registro es obligatorio, como en el caso de México, las personas pierden la libertad de decidir si deben o no poner en riesgo sus derechos al entregar datos biométricos. La obligatoriedad del CUID o la recolección de datos biométricos contradice la obligación legal y política del Estado de proteger los derechos humanos, ya que si una persona se niega a entregarlos o no logra acceder a la identificación digital, quedaría completamente excluida de la sociedad. Cabe resaltar que este aspecto de falta de consentimiento fue uno de los puntos que llevó a la Corte Suprema de Jamaica a declarar inconstitucional el primer proyecto para instaurar un Sistema Nacional de Identificación Digital. Actualmente, la nueva propuesta legislativa en Jamaica establece que el registro debe ser voluntario.

- **Exclusión de servicios esenciales:** Si el registro es voluntario, pero la identificación digital se vuelve el único medio para acceder a servicios,

las poblaciones más vulnerables serán quienes se vean una vez más excluidas. En India se creyó que con la creación del sistema voluntario de identificación Aadhaar, miles de indios podrían por fin ser identificados y tener acceso a servicios sociales. Sin embargo, ocurrió todo lo contrario. Con el tiempo, el número Aadhaar ha sido vinculado a la prestación de diversos servicios privados y públicos, haciéndolo indispensable para vivir. El problema es que acceder a esta identificación biométrica es difícil en un país con abismales diferencias sociales y tecnológicas. Las consecuencias son tan desastrosas que hubo personas que murieron de hambre por el solo hecho de no contar con la tarjeta de identificación.

México se encuentra entre el 25% de los países con mayor inequidad social en el mundo. Agregar un factor de exclusión de grupos poblacionales a servicios sociales y privados puede tener severas repercusiones en la economía, salud y desarrollo del país.

Estos riesgos se solucionan permitiendo la coexistencia de múltiples sistemas de identificación, sin que la CUID prevalezca sobre otros y, sobre todo, permitiendo que la entrega de datos biométricos sea voluntaria y no obligatoria.

4. El uso de la CUID como condición para el acceso a servicios públicos y privados, particularmente al combinarlo con datos biométricos, permite el monitoreo masivo y permanente de la población

México tiene una larga historia de vigilancia estatal; como sociedad civil, debemos cuidadosamente resguardarnos contra la expansión de estas prácticas que dañan gravemente los derechos humanos.

- **Vigilancia biométrica masiva y dirigida:** La creación de una base de datos centralizada con información biométrica ampliará la capacidad de vigilancia del gobierno. Lo que es más: crear una cédula única digital

de identidad para acceder a servicios de transporte público, a procesos legales (como denuncias o demandas), a sistemas bancarios, entre otros, le brinda al Estado un poder extraordinario sobre sus habitantes. Esta base de datos podría utilizarse tanto para monitorear y restringir la libertad de movimiento y asociación de las personas, como para perseguir a activistas, periodistas, representantes de la oposición, minorías, entre otros, especialmente en combinación con las herramientas de vigilancia existentes que tienen un historial de abuso.

- **Tentación de expansión:** Debido a la gran cantidad de datos centralizados que contiene información del día a día de las personas, dicha base de datos es atractiva para realizar perfilamiento de personas mediante el análisis permanente de sus patrones de comportamiento, incluso si el gobierno no está llevando a cabo ese tipo de vigilancia ahora. En Argentina se ha visto que, a partir de la creación de una base de datos biométrica y centralizada, las actividades de vigilancia han aumentado, incluyendo la creación del Sistema Federal de Identificación Biométrica para la Seguridad que se alimenta de la base de datos de registro civil.

Diversificar los documentos de identidad, dándoles la misma relevancia, reduce las posibilidades de vigilancia masiva. Asimismo, es primordial que se establezcan criterios, reglas y prohibiciones para compartir datos personales, incluyendo el registro de actividad en un sistema (logs).

Recomendaciones

En vista de los graves riesgos que el proyecto de la CUID representa, resulta indispensable modificar la minuta de manera tal que sea posible contemplar mecanismos alternativos que permitan garantizar el derecho a la identidad legal sin poner en riesgo de manera innecesaria y

potencialmente irreversible la privacidad y seguridad de más de 130 millones de personas, sin generar un instrumento de vigilancia masiva de la población, y sin condicionar el acceso a servicios con efectos desproporcionados en poblaciones vulnerables.

En particular se recomienda lo siguiente:

1. No incluir datos biométricos como parte del Registro Nacional de Población.
2. Determinar que la CUID deba descansar sobre sistemas descentralizados.
3. Establecer que la obtención de la CUID sea opcional.
4. Impedir el condicionamiento del acceso a servicios públicos o privados a la obtención de la CUID.
5. Impedir la recolección, almacenamiento o transferencia de datos que registren el uso de la CUID.

Suscribimos:

Access Now - Global

AfroLeadership - Africa

Arturo J. Carrillo - The George Washington University Law School, EE.UU.

Asociación por los Derechos Civiles (ADC) - Argentina

Centro Latam Digital - América Latina

Coding Rights - Brasil

Cooperativa Tierra Común - México

Damian Loreti - Universidad de Buenos Aires, Argentina

Datos Protegidos - Chile

Datysoc, Laboratorio de Datos y Sociedad - Uruguay

Derechos Digitales - América Latina

Fundación Acceso - Centroamérica

Gambia Cyber Security Alliance - Gambia

Fundación InternetBolivia.org - Bolivia

Instituto Brasileiro de Defesa do Consumidor (IDEC) - Brasil

Instituto para la Sociedad de la Información y Cuarta Revolución Industrial - Perú

Ipandetec - Centroamérica

Laboratório de Políticas Públicas e Internet (LAPIN) - Brasil

Luchadoras - México

Privacy International - Global

R3D: Red en Defensa de los Derechos Digitales - México

SeguDigital - México

Senegal ICT Users Association (ASUTIC) - Senegal

Sula Batsú - Costa Rica

Sursiendo, Comunicación y Cultura Digital - México

TEDIC - Paraguay

The Civil Pole for Development and Human Rights - Túnez