

IDENTIDAD DIGITAL EN PARAGUAY: RIESGOS Y RECOMENDACIONES DESDE UNA PERSPECTIVA DE DERECHOS HUMANOS



IDENTIDAD DIGITAL EN PARAGUAY: RIESGOS Y RECOMENDACIONES DESDE UNA PERSPECTIVA DE DERECHOS HUMANOS

La presente publicación ha sido financiada por la Unión Europea. Su contenido es responsabilidad exclusiva de TEDIC y no refleja necesariamente los puntos de vista de la Unión Europea.



Financiado por
la Unión Europea

CON EL APOYO DE

La gente
cambia
el mundo

Diakonia

TEDIC
Tecnología
& Derechos
Humanos

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

IDENTIDAD DIGITAL EN PARAGUAY: RIESGOS Y RECOMENDACIONES DESDE UNA PERSPECTIVA DE DERECHOS HUMANOS

ABRIL DE 2024

AUTORÍA

Eduardo Carrillo

Leonardo Gómez Berniga

COMUNICACIÓN

Araceli Ramírez

DIAGRAMACIÓN

Horacio Oteiza



Esta obra está disponible bajo licencia Creative

Commons Attribution 4.0 Internacional (CC BY SA 4.0)

<https://creativecommons.org/licenses/by-sa/4.0/deed.es>

TABLA DE CONTENIDO

INTRODUCCIÓN	5
1. CONTEXTO GLOBAL	6
1.1. Biometría: Riesgos y preocupaciones	6
2. CONTEXTO NACIONAL	7
3. ANÁLISIS DE LA LEY N° 7177/2023	9
3.1. Colisión legislativa	9
3.2. Protección de datos	10
4. CONCLUSIÓN Y RECOMENDACIONES	12

INTRODUCCIÓN

Con la promulgación de la Ley N° 7177/2023, Paraguay se une al creciente número de países que adoptan formatos digitales para documentos de portación obligatoria, como la cédula de identidad y la licencia de conducir. Esta tendencia plantea importantes desafíos en el ejercicio de la privacidad y otros derechos fundamentales.

Desde TEDIC, venimos advirtiendo sobre los riesgos de implementar políticas públicas con un componente digital sin integrar en su desarrollo e implementación evaluaciones de impacto en materia de derechos humanos¹. En este artículo, ofrecemos una síntesis de nuestras principales preocupaciones, así como algunas recomendaciones de pasos a seguir en el marco de la implementación de esta política.

1 Asamblea General (ONU). El derecho a la privacidad en la era digital. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. A/HRC/39/29. 2018. <https://documents.un.org/doc/undoc/gen/g18/239/61/pdf/g1823961.pdf>

1. CONTEXTO GLOBAL

Aunque la identidad digital promete eficiencia y conveniencia, su implementación a nivel mundial ha revelado riesgos significativos para la privacidad y la seguridad de los datos personales.

En México, más de 20 organizaciones nacionales e internacionales se posicionaron contra la implementación obligatoria de la Cédula Única de Identidad Digital (CUID) ya que su implementación no contemplaba mecanismos para garantizar el derecho a la identidad legal y para evitar poner bajo significativo riesgo la privacidad y seguridad de más de 130 millones de personas. Así también, no se contemplaban mecanismos para evitar la vigilancia masiva y todavía más, se planteaba condicionar el acceso a servicios públicos a condición de la tenencia y uso de la Cédula Digital, lo que implicaría impactos desproporcionales en poblaciones vulnerables.

En India, la implementación del sistema biométrico Aadhaar, vulneró la privacidad de la población y ocasionó restricciones masivas a servicios y beneficios estatales, profundizando la exclusión social.

Jamaica, país que también implementó un sistema similar a Aadhaar, tuvo que adecuar su marco normativo de protección de datos antes. Sin embargo, su implementación evidenció que se retenían más de 16 datos personales sin claro manejo del consentimiento.

Otros casos documentados también en Túnez, Estonia, Marruecos, Perú, entre otros, ilustran las complejidades y desafíos que enfrentan los países al adoptar tecnologías de identidad digital. Estos ejemplos resaltan la necesidad de un enfoque equilibrado que proteja los derechos humanos de las personas. Para Paraguay, es esencial estudiar estas experiencias internacionales, para desarrollar un marco legal y operativo que garantice tanto la eficiencia tecnológica como la protección integral de los derechos fundamentales de la ciudadanía en el contexto del uso y promoción de la cédula digital.

1.1. BIOMETRÍA: RIESGOS Y PREOCUPACIONES

La organización Privacy International (PI) define los datos biométricos como «métodos automatizados que pueden reconocer de manera precisa a una persona basándose en sus características físicas o de comportamiento». A su vez, PI también indica que “las tecnologías biométricas abarcan una amplia gama, incluyendo el reconocimiento de huellas dactilares, de palma, facial, de patrones de venas, del iris, de voz y otras manifestaciones corporales como el ADN y la dinámica del tecleo, entre otros».

En tal sentido, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha indicado que es “preocupante que algunos Estados hayan emprendido enormes proyectos basados en datos biométricos sin contar con las garantías jurídicas y procesales necesarias” y, a su vez, ha recomendado a los Estados que “velen por que los sistemas que emplean un gran volumen de datos, incluidos los que implican la recopilación y conservación de datos biométricos, solo se utilicen cuando los Estados puedan demostrar que son necesarios y proporcionales para lograr un fin legítimo”.

El ex Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue², junto con Navi Pillay³, ex Alto Comisionado de la ONU para los Derechos Humanos, han manifestado su inquietud respecto a las infracciones del derecho a la privacidad causadas por la inadecuada protección en el uso de tecnologías biométricas.

Martin Scheinin, quien fue Relator Especial de la ONU sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, advierte sobre los riesgos asociados con el almacenamiento de datos biométricos en bases de datos centralizadas en lugar de en documentos de identidad. Según Scheinin, esta práctica aumenta la vulnerabilidad de los individuos y la seguridad de la información, y podría conducir a un incremento significativo en las tasas de error a medida que se acumula más información biométrica⁴.

Desde Privacy International señalan cómo estos sistemas pueden conducir a la exclusión de servicios esenciales, el aumento del riesgo de robo de identidad y sistemas de vigilancia invasivos. Tal situación adquiere una dimensión todavía más delicada en contextos con un débil estado de derecho.

Por su parte, desde Access Now amplían su preocupación a los casos donde la implementación de sistemas de identidad digital centralizados pueden conducir a la vigilancia y el perfilado exhaustivo de las personas usuarias, violando la privacidad, además que generar exclusión en los casos que se establecen como obligatorios o con prácticas que atentan contra la autonomía y el consentimiento.

Los riesgos asociados con el uso de identificadores biométricos, como huellas dactilares y escaneos del iris, en los sistemas de identidad digital amplifican el daño ante posibles filtraciones, ya que a diferencia de las contraseñas, no se pueden cambiar fácilmente una vez comprometidos y, además, son irrecuperables.

Por otro lado, poblaciones históricamente marginadas, como personas refugiadas y personas transgénero, podrían verse sumamente afectadas por la obligatoriedad de inscribirse en programas de identidad digital que les fueren a identificarse de forma diferente a su identidad, planteando registros discriminatorios o digitalizando de forma violenta sus rasgos biométricos. Esto también podría llevar a forzar el consentimiento y la autonomía de las personas a cambio de acceder a servicios esenciales y derechos básicos atentando contra la dignidad humana.

2. CONTEXTO NACIONAL

En Paraguay, la implementación de la Ley N° 7177/2023 se está llevando a cabo en un ambiente donde prevalece un entusiasmo excesivo por las soluciones tecnológicas, a menudo denominado 'hype tecno-solucionista'. Este enfoque puede descuidar consideraciones críticas en términos de derechos y privacidad.

2 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40. ONU. Abril, 2013.

3 UN News Centre, UN rights chief urges protection for individuals revealing human rights violations. ONU.

4 Estas preocupaciones también ya habían sido publicadas ante el anuncio de la posible incorporación de registros biométricos para ejercer el voto en contextos electorales en Paraguay: <https://www.tedic.org/huella-dactilar-iris-y-reconocimiento-facial-identidad-que-no-se-puede-reimprimir/>

La emisión de la cédula de identidad civil en Paraguay está a cargo de la Policía Nacional, lo cuál genera una gran concentración de datos personales en una misma entidad a cargo de la persecución de delitos y crímenes en el país. La normativa paraguaya obliga a toda persona dentro del territorio nacional a portar la cédula y faculta a la Policía a demorar personas sin que exista indicios flagrantes de actuar ilícito.

Paraguay cuenta con históricas deudas en la consolidación de una democracia efectiva. La población paraguaya, según datos del Barómetro de las Américas del 2021, cuenta con altos niveles de insatisfacción a la democracia a la par que crecen los niveles de valoración positiva de las fuerzas militares en la opinión pública. Todavía más, existen datos que indican que al menos la mitad de la población, aceptaría un golpe de estado contrario al orden democrático.

Paraguay es el único país del Mercosur que no ha separado la emisión de documentos civiles de los órganos policiales³. La no separación entre el manejo civil y los mecanismos de seguridad establecen preocupaciones sobre el diseño del Estado.

Desde el 2018, con la ley de creación del Ministerio de Tecnologías de la Información y Comunicación (MITIC) y posteriores resoluciones, se dio cuerpo a la existencia de un “Portal Único de Gobierno y Trámites en línea”, que se instituyó como un indexador de soluciones de gobierno electrónico, apoyado por un sistema de intercambio de información con otras entidades.

Esta implementación creció en uso, incorporando la generación de documentaciones como certificados de nacimiento, antecedentes policiales y judiciales, constancia de libreta de vacunación, grado académico, entre otros. En octubre del 2023, se registraban más de 46.000 usuarios registrados. Además, según proyecciones, se busca digitalizar y simplificar 120 trámites en el marco de una agenda digital del Estado.

En setiembre del 2023, el Congreso Nacional sancionó la Ley N° 7177/2023, que valida el formato digital de los documentos de portación obligatoria, entrando en vigor en octubre de dicho año. El proyecto no tuvo mucha socialización ni audiencias para discutir sus implicancias. Sin embargo, presenta varios aspectos técnicos y jurídicos que requieren un análisis detallado.

La ley tiene como objetivo otorgar validez oficial al formato digital de los documentos de portación obligatoria, estableciendo la coexistencia de formatos digitales y físicos. La autoridad de aplicación será el MITIC, a través del Viceministerio de Tecnologías de la Información y Comunicación.

Los sujetos obligados bajo esta ley incluyen también a las autoridades emisoras de documentos. Concretamente:

- Cédula de identidad emitida por el Departamento de Identificaciones, dependiente de la Policía Nacional.
- Cédula verde vehicular emitida por la Dirección del Registro de Automotores, dependiente de la Corte Suprema de Justicia.
- Licencia de conducir vehicular y la habilitación vehicular emitidas por cada municipio correspondiente.

3. ANÁLISIS DE LA LEY N° 7177/2023

La ley en cuestión se encuentra en vigor, pero su aplicación práctica depende de una reglamentación adecuada que aún se encuentra pendiente. Esta ley establece un plazo de hasta dos años para la implementación y reglamentación, lo cual implica un período de transición y ajuste para todas las partes involucradas, situación que aún no ocurrió.

Considerando que el Gobierno Nacional buscó incorporar la implementación de esta política a su informe de logros de los 100 días de gobierno, habilitó el uso de la cédula de identidad y el registro de conducir digital sin que exista una reglamentación publicada por parte del MITIC. Esto se puede ver, por ejemplo, al verificar que la actual plataforma aún no cuenta con una política de privacidad ajustada al marco normativo y las especificidades de la cédula de identidad digital. Por tanto, tal rapidez en esta implementación plantea preocupaciones sobre la manera en la cual se acuerda la implementación de este tipo de políticas en un sistema democrático.

3.1. COLISIÓN LEGISLATIVA

La Ley N° 7177/2023 de Paraguay, que establece el formato digital de documentos de portación obligatoria, presenta importantes desafíos legales y éticos en términos de protección de derechos y privacidad. Esta legislación debe ser analizada detenidamente a la luz de las normativas internacionales de derechos humanos y protección de datos, como el Pacto Internacional de Derechos Civiles y Políticos (PIDCP, Artículo 17) y la Convención Americana sobre Derechos Humanos (CADH, Artículo 11). Ambos instrumentos, ratificados por Paraguay, protegen contra injerencias arbitrarias o ilegales en la vida privada, lo que es fundamental en la era de la identidad digital. **La necesidad de consentimiento informado y medidas de seguridad robustas para el manejo de datos personales es un pilar central de estas normativas.**

En el contexto internacional, la jurisprudencia sobre protección de datos personales y privacidad ha sido ampliamente desarrollada por entidades como el Tribunal Europeo de Derechos Humanos y la Corte Interamericana de Derechos Humanos (Corte IDH, en adelante). Aunque la Corte IDH no ha abordado específicamente los datos biométricos, sus decisiones han enfatizado consistentemente la importancia de proteger la privacidad y los datos personales. En este contexto, la Ley N° 7177/2023 debe implementar salvaguardas explícitas, incluyendo limitaciones en la recolección de datos biométricos, protección contra accesos no autorizados y procedimientos para asegurar la integridad y confidencialidad de estos datos. Asimismo, es crucial que se establezcan procedimientos claros y accesibles para que las personas puedan corregir o eliminar sus datos personales.

La Ley también debe ser evaluada **desde la perspectiva de la necesidad y proporcionalidad**. Según la Corte IDH, cualquier medida que afecte la privacidad debe ser necesaria en una sociedad democrática y proporcional al fin legítimo perseguido¹. Este principio es esencial para garantizar que los avances tecnológicos no socaven los derechos fundamentales.

La transparencia y el derecho de acceso a la información pública son aspectos cruciales en el manejo de datos personales. La legislación debe asegurar que las personas tengan acceso claro a la información sobre cómo se utilizan y almacenan sus datos y cómo pueden ejercer sus derechos para impugnar o rectificar esta información², algo no evidenciado en la implementación actual en Paraguay.

Además, la implementación de la Ley N° 7177/2023 ha generado preocupaciones específicas relacionadas con la presunción de inocencia, un derecho consagrado en el Artículo 16 de la Constitución Nacional de Paraguay. Juristas como Jorge Vasconcellos y José Casañas Levi han señalado que las detenciones aleatorias por no presentar documentos podrían constituir una violación de este principio fundamental. Dicha práctica, considerada un vestigio de épocas autoritarias, socava la presunción de inocencia y el orden constitucional, y podría ser interpretada como una forma de criminalización por la falta de documentación.

Incluso, esta ley genera aún más confusión jurídica al colisionar con la recientemente implementada Ley N° 7179/2023 de “Simplificación de Trámites Administrativos en Organismos y Entidades del Estado”, aun sin reglamentar. Su artículo 2° establece que:

«Ninguna entidad del Estado podrá exigir como requisito para gestiones o trámites administrativos la presentación de constancia, certificado u **otro documento que haya sido expedido por ella misma o que por su naturaleza debiera constar en sus archivos.**»

Esta situación pone de manifiesto la necesidad de armonizar las leyes para evitar contradicciones y garantizar el respeto a los derechos fundamentales.

La Ley N° 7177/2023, si bien representa un avance hacia la modernización digital en Paraguay, debe ser cuidadosamente equilibrada para proteger los derechos fundamentales de privacidad y protección de datos personales. La revisión y ajuste de la legislación son esenciales para alinearla con los estándares internacionales y la jurisprudencia relevante, y para garantizar que no se perpetúen prácticas autoritarias bajo el pretexto de la modernización tecnológica.

3.2. PROTECCIÓN DE DATOS

Un aspecto fundamental y sumamente deficiente en la discusión sobre la implementación de la identidad digital en Paraguay es la protección de datos personales. Paraguay aún no cuenta con un marco legal integral de protección de datos personales.

La ausencia de un marco normativo macro que establezca cuidados y debidos procesos en el tratamiento de datos personales, sumado a la ausencia o incluso superposición de reglamentaciones entre sistemas interoperativos vinculados a la identidad digital en los organismos públicos vinculados³, generan un escenario de incertidumbre frente a la protección que debe ser garantizada por el Estado Paraguayo.

En ese sentido, tanto la aplicación “Portal Paraguay”, desarrollada para sistemas operativos Android y el portal web de Identidad Electrónica dirigen a la misma política de privacidad⁴ y a los Términos y condiciones (TyC)⁵, a pesar de ser dos infraestructuras completamente diferentes.

En los TyC, el MITIC se desliga totalmente de la responsabilidad sobre las modificaciones, pérdidas o daños sufridos en el mantenimiento de la plataforma. Tampoco asume responsabilidad en fallas del sistema. Además de esto, se plantean situaciones que discrecionalmente atentan contra el consentimiento informado de la población usuaria, cómo “el derecho de actualizar y modificar en cualquier momento y de cualquier forma, de manera unilateral y sin previo aviso, las presentes condiciones de uso, políticas de privacidad y los contenidos de la página”⁶.

A su vez, la plataforma estatal reconoce ceder información sobre uso de la aplicación desde la web del ID Digital a Google Analytics⁷. Esto implica confiar la gestión de datos a una empresa extranjera, cuyo código es cerrado y no puede ser auditado en profundidad. La divulgación de información incluye detalles sensibles como:

- número de usuarios que acceden a la web,
- número de páginas vistas,
- frecuencia y repetición de las visitas, su duración,
- el navegador utilizado,
- el operador que presta el servicio,
- el idioma que utiliza,
- la ciudad a la que está asignada su dirección IP.

A pesar que la política de privacidad de estos TyC señale que no comparte sus datos con terceros con fines de marketing, se evidencia una falta de garantías que evite que un servicio privado como Google no utilice las cookies de las personas usuarias para realizar perfilamiento con fines publicitarios.

Por último, la política de privacidad invoca una ley derogada como la Ley N° 1682 “QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO” y sus normas complementarias y demás normativas de la República del Paraguay.

No solo se está hablando aquí del riesgo que implica implementar la identidad digital, sino que, desde el lanzamiento de la plataforma, no se ha establecido un marco robusto que garantice la seguridad de los datos personales de las personas usuarias. Esto refleja una aproximación deficiente que requiere una urgente revisión.

4. CONCLUSIÓN Y RECOMENDACIONES

La implementación de la cédula digital en Paraguay, en virtud de la Ley N° 7177/2023, se ha realizado en un contexto global donde los sistemas de identificación digital están siendo sometidos a un escrutinio intenso debido a sus implicaciones en la privacidad y los derechos fundamentales. La experiencia de países como México, India y Jamaica, donde la implementación de sistemas similares ha generado preocupaciones significativas ofrece lecciones valiosas que el Estado paraguayo no puede ignorar. En ese sentido, en el marco de la presente política así como otras en materia de identidad digital recomendamos los siguientes pasos:

1. **Evaluación de riesgos y protección de derechos:** Es crucial que el Estado paraguayo integre evaluaciones exhaustivas en materia de derechos humanos en el desarrollo e implementación de políticas públicas que involucren tecnología y tratamiento de datos personales. Tales evaluaciones deben abordar los riesgos de exclusión, vigilancia y explotación de datos a modo de mitigar de manera acorde posibles riesgos devenidos de la implementación de cualquier tipo de política.
2. **Transparencia y participación pública:** El proceso de implementación de la cédula digital debe ser transparente y participativo. Esto implica socializar el proyecto, impulsar políticas de transparencia para la auditoría y control de la implementación entre múltiples partes y asegurar que la población comprenda las implicancias de la nueva ley.
3. **Reglamentación adecuada y políticas de privacidad:** Antes de su implementación efectiva, es fundamental que exista una Ley Integral de protección de datos personales, y posteriormente, una reglamentación armonizada. La reglamentación debe incluir políticas claras sobre el uso, almacenamiento y acceso a los datos personales.
4. **Capacitación y concienciación:** Debe haber una inversión en la capacitación y sensibilización tanto de las personas encargadas de la implementación como de la población en general sobre los riesgos y beneficios de la cédula digital.
5. **Mecanismos de mitigación de daños:** Es esencial establecer mecanismos efectivos para abordar y remediar cualquier violación de derechos que pueda surgir como resultado de la implementación de la cédula digital. Tales mecanismos deben estar accesibles públicamente y para todas las personas usuarias del sistema.
6. **Acceso inclusivo y no discriminatorio:** La implementación de la cédula digital debe asegurar que no se excluya a ninguna parte de la población, prestando especial atención a grupos históricamente marginados, como personas indígenas y personas transgénero.
7. **Seguridad de datos biométricos:** Dada la naturaleza sensible de los datos biométricos, se deben tomar medidas robustas para proteger estos datos contra accesos no autorizados y/o filtraciones.
8. **Alineación con estándares internacionales:** La implementación debe alinearse con los estándares internacionales en materia de derechos humanos y protección de datos, tomando en cuenta las experiencias y mejores prácticas de otros países.

En conclusión, mientras Paraguay avanza hacia la digitalización, es imperativo que se tomen medidas para asegurar que esta transición no vulnere los derechos humanos. Esto implica no solo establecer un marco sólido de protección de datos sino también garantizar que la tecnología no sea utilizada como una herramienta para la restricción de libertades civiles. Es urgente que el Estado paraguayo aborde estas preocupaciones de manera integral, evitando un avance impulsado únicamente por el tecno-solucionismo, para proteger a su ciudadanía en un mundo cada vez más digitalizado.

