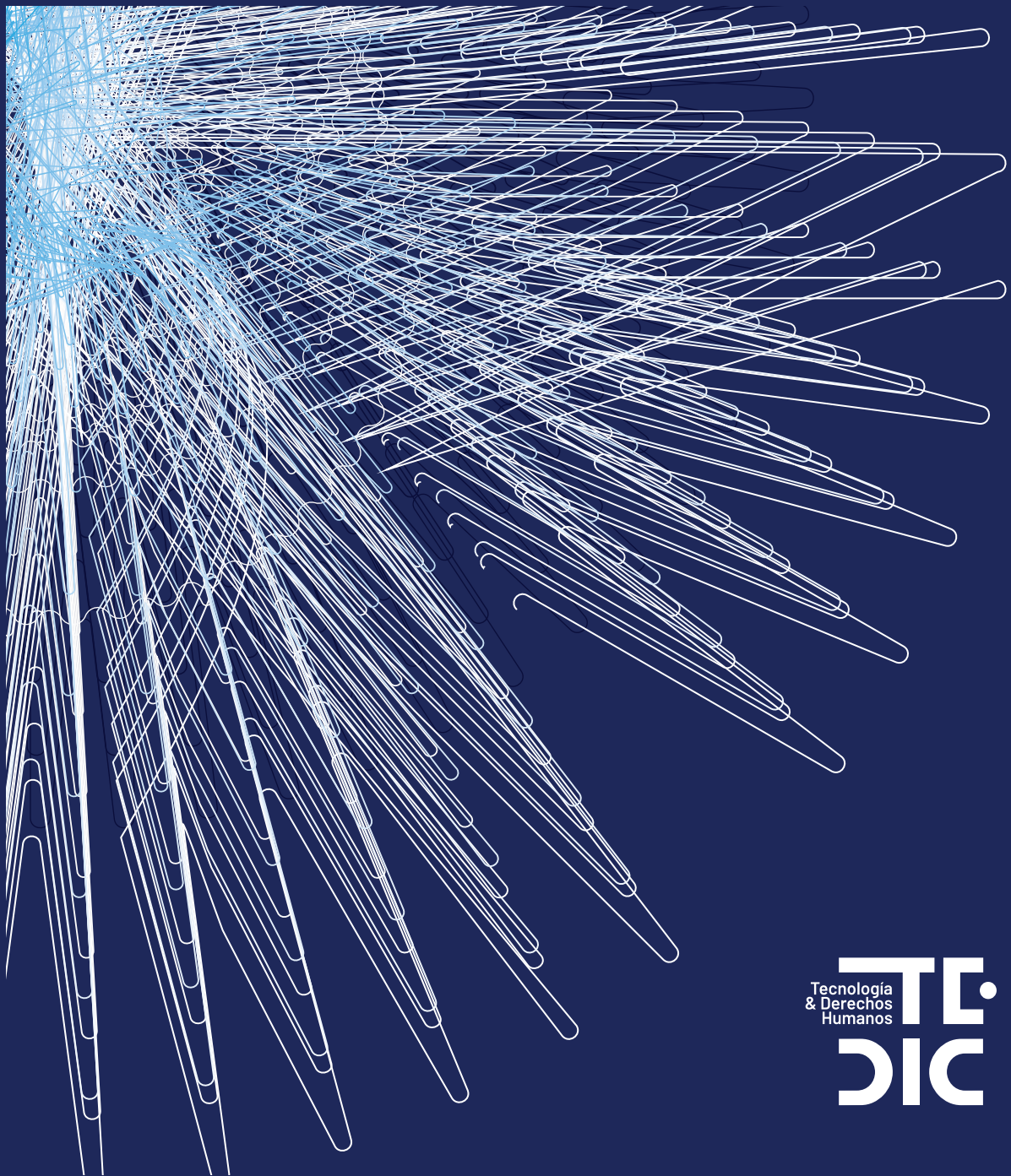


ANÁLISIS LEGAL AL PROYECTO DE LEY SOBRE IMPLEMENTACIÓN DE BIOMETRÍA EN EL SISTEMA DE VOTACIÓN ELECTRÓNICA



ANÁLISIS LEGAL AL PROYECTO DE LEY SOBRE IMPLEMENTACIÓN DE BIOMETRÍA EN EL SISTEMA DE VOTACIÓN ELECTRÓNICA

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.

ANÁLISIS LEGAL AL PROYECTO DE LEY SOBRE IMPLEMENTACIÓN DE BIOMETRÍA EN EL SISTEMA DE VOTACIÓN ELECTRÓNICA

OCTUBRE DE 2019

RESPONSABLE DEL ANÁLISIS LEGAL Y REDACCIÓN

Maricarmen Sequera Buzarquis

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

DATOS BIOMÉTRICOS EN EL SISTEMA DE VOTACIÓN ELECTRÓNICA EN PARAGUAY	5
Vigilancia, control social y violación de nuestros derechos	5
En resumen	8

DATOS BIOMÉTRICOS EN EL SISTEMA DE VOTACIÓN ELECTRÓNICA EN PARAGUAY

El proyecto de ley sobre Implementación de Biometría en el sistema de votación electrónica en Paraguay denominado “Que modifica los artículo 98, 201 y 208 de la ley 834/96”, presentado el de 16 de octubre de 2019, por los senadores Fidel Zavala, Stephan Rasmussen, Patrick Kemper, Antonio Apuril, Georgia María Arrúa.

Según el motivo del proyecto de ley, “[...] es de vital importancia para garantizar el identificación del elector y que otra persona no utilice la cédula de identidad de un tercero para votar en su nombre”. Es agregar la implementación de un dispositivo informáticos o electrónicos de lecturas biométrica, ya sea huella dactilar, iris y/o reconocimiento facial de las ciudadanía habilitada para votar. La base de datos de datos biométricos será proveído por la policía Nacional a través de sus departamentos de identificaciones, entregaran al Tribunal de Justicia Electoral a través de Codirección de Registro electoral de departamento de identificación.

En primer lugar, desde TEDIC alertamos al Gobierno y al Congreso Nacional sobre los riesgos de este anteproyecto de ley que socava los derechos fundamentales consagrados en la Constitución Nacional como son: libertad de expresión, anonimato, intimidad (privacidad), y otras normas constitucionales como el secreto al voto para el ejercicio democrático. Al igual que hicimos en publicaciones anteriores reiteramos el llamado de atención sobre la implementación del voto electrónico y sus implicancias para el sistema democrático.

En segundo lugar el **Estado paraguayo tiene la obligación de respetar y proteger el derecho a la libertad de opinión y expresión y a la privacidad**, de acuerdo con los artículos 19 y 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), ratificado por Paraguay el 10 de junio de 1992, así como los artículos 11 y 13 de la Convención Americana sobre Derechos Humanos («Convención Americana»), ratificada el 24 de agosto de 1989. Estos derechos están estrechamente vinculados y «el derecho a la privacidad se entiende a menudo como un requisito esencial para la realización del derecho a la libertad de expresión» (A / HRC / 23/40).

VIGILANCIA, CONTROL SOCIAL Y VIOLACIÓN DE NUESTROS DERECHOS

¿Que garantías se tiene para que no se correlacionen la identidad de la persona habilitada para votar con la emisión del voto? ¿Cómo se garantiza el derecho constitucional al secreto del voto? ¿Se prevé salvaguardas para evitar la manipulación y adulteración de las copias de las huellas dactilares y reconocimiento facial que pretende utilizar el TSJE? Así como se terceriza el servicio de proveer las maquinas para el voto electrónico, ¿también se alquilarán los dispositivos de lectura biométrica del sector privado? ¿Ellos tendrán acceso a la base de datos biométricos? ¿Cómo se evitará la venta de las bases de datos biométricos como sucede con la base de cédulas de identidad? ¿Habrán sanciones en caso de abuso por parte de los responsables de las bases de datos? ¿Qué harán si se clonan los datos biométricos? Estas son sólo algunas preguntas e inquietudes que surgen a partir del análisis de este proyecto de Ley.

Desde TEDIC, planteamos preocupaciones sobre el hecho de que la recopilación de datos de identidad personal y sensible, incluida la información biométrica, interfiere indebidamente con el anonimato las personas habilitadas para votar. La creación de bases de datos personales, potencialmente accesible por las autoridades gubernamentales y terceros, interfiere con la «zona de privacidad» necesaria para la realización de la libertad de expresión garantizada por los artículos 19(2) del PIDCP y 13(1) de la Convención Americana. Además, la mera posibilidad del uso indebido de tal información por parte del gobierno o de terceros también puede tener un efecto paralizador sobre la capacidad de las personas para ejercer libremente su voto en las elecciones, que es pilar fundamental de la democracia.

Si bien desde TEDIC reconocemos que la prevención del fraude en las elecciones nacionales puede ser un objetivo legítimo del orden público, nos preocupa que la recopilación de información de identidad requerida por el proyecto de ley, sea innecesaria y desproporcionada en virtud del artículo 19(3) y del artículo 13(2) y los artículos 26 de Libertad de expresión, 33 derechos a la intimidad y 118 del Sufragio consagrados en la Constitución Nacional. Los artículos del proyecto de ley requieren que todas las personas divulguen sus datos de identidad biométrica, independientemente de si han sido o no sospechosas de conductas indebidas y sin ninguna garantía aparente. Es preocupante que esta recolección indiscriminada de datos de identidad biométrica no sea el «medio menos intrusivo» necesario para prevenir la actividad fraudulenta. Es decir que para justificar la recolección de datos biométricos, que son datos sensibles, se deben analizar formas alternativas que afecten en menor medida los derechos de las personas y pueda alcanzar los objetivos que se persiguen.

Por su parte, el ex Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión (ONU), Frank La Rue y el Alto Comisionado de Derechos Humanos (ONU), Navi Pillay han expresado preocupación por las violaciones del derecho a la intimidad debidas a la falta de medidas de protección eficaces en la utilización de tecnologías biométricas.

“los casos en que la biometría no se almacena en un documento de identidad, sino en una base de datos centralizada, incrementando los riesgos para la seguridad de la información y dejando a los individuos vulnerables. A medida que aumenta la información biométrica, las tasas de error pueden aumentar significativamente”- Martin Scheinin – Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo de la ONU.

Según la organización internacional Privacy International: “Los datos biométricos son métodos automatizados que pueden de manera precisa reconocer a un individuo con base en las características físicas o de comportamiento. La tecnología usada en la biometría incluye el reconocimiento de huellas digitales, huella palmar, facial, patrones de venas, iris, voces y otras exposiciones del cuerpo incluyendo ADN y la secuencia de la pulsación de las teclas, entre otros”. Es decir, la biometría se refiere a la medición de y distintivo físico, características biológicas y conductuales utilizadas para la identidad de personas.

Cabe resaltar que la biometría, en este caso el reconocimiento facial o la huella dactilar por ejemplo, no se trata de la cara o del dedo, sino cómo esa identidad digital puede ser usada para determinar derechos. Es una identidad que no se puede cambiar, no se vuelve a imprimir las huellas o caras cuando las mismas han sido clonadas por terceros como podría ser el caso de la cédula de identidad.

Los métodos de identificación biométricos pueden resultar en errores, son susceptibles de ser engañados y pueden retardar el proceso electoral. Entre algunos de los casos se destacan, la clonación de huellas dactilares para marcar el ingreso en Aerolínea Argentina en el 2019, la captación de huellas de la ministra de defensa de Alemania a través de fotografías de ella sin su consentimiento en el 2014. Por otro lado estudios internacionales estudiaron 11 sistemas de identificación biométrica distintos en los cuales probaron copias de huellas dactilares creadas en gelatina, encontrando que los 11 sensores aceptaban las huellas de gelatina, con mas del 60% de aceptación positiva del sistema.

La ausencia de una ley integral de protección de datos personales como posible salvaguarda para evitar la recopilación y el uso innecesario y desproporcionado de la información de identidad también nos genera una fuerte preocupación. por el hecho de que el proyecto de ley no cumple las condiciones de legalidad establecidas los artículos 19(3) y 13(2) y lo expresado en la Constitución Nacional. El proyecto de ley no indica cómo se almacenarán los datos recopilados y si existirán restricciones al acceso, uso y retención de dichos datos por parte del gobierno o de terceros. Sin estas salvaguardas, la ciudadanía habilitada para la votación tendrá completa ignorancia sobre si serán asegurados o protegidos sus datos personales.

La propuesta legislativa paraguaya no presenta un análisis de impacto previo para justificar la implementación de este tipo de sistema. Es obligatorio, según los estándares de tratamientos de datos, una evaluación de impacto. Existe poca legitimidad en el uso de este tipo de sistemas: sólo 2 países en el mundo utilizan datos biométricos de forma automatizada en el día de votación y son: Venezuela y Brasil (este último parcialmente).

Se sugiere que la propuesta de ley sea aplazada para tener un debate amplio de múltiples partes interesadas, o simplemente el rechazo por no contemplar las preocupaciones citadas más arriba y que violan los preceptos constitucionales y normas de derecho internacional público.

EN RESUMEN

Se necesita con urgencia una ley integral de protección de datos personales. Se pretende se implementará sin un marco jurídico que permita garantizar el tratamiento de los datos biométricos de forma adecuada por parte del Estado y el sector privado. Ante abusos o filtraciones de datos biométricos, el Estado no tiene previsto una autoridad competente para velar por la protección de los mismos.

1. **El dato biométrico es un dato sensible**, lo que requiere mejores mecanismos de salvaguarda que este proyecto de Ley no contempla. Los desafíos para garantizar el cuidado de los datos ante posibles prácticas discriminatorias que se podrían realizar a partir de la correlación de identificación de la persona habilitada para votar y su voto, no son tomados en cuenta en el texto del proyecto.
2. **Es vigilancia**. Las huellas dactilares pueden ser un mecanismo más de control que podría agravar prácticas de vigilancia y hostigamiento a minorías y grupos vulnerables. Las carencias que tiene Estado para resguardar la información privada de los ciudadanos vuelve a estos registros aún mas problemáticos y con un alto riesgo en ser filtrados.
3. **No existe una evaluación de impacto para el uso del sistema de datos biométricos**: No se realizó una análisis de impacto previo para evaluar la importancia de la implementación de un sistema de recolección de datos biométricos. Cualquier interferencia por parte del Estado debe estar basada en fundamentaciones sólidas, sustentadas en datos y diagnósticos serios e independientes, a fin de cumplir con las condiciones de necesidad y proporcionalidad requeridas para la legitimidad de toda medida que pretenda limitar derechos fundamentales.
4. **Existen pocos países en el mundo, entre ellos Venezuela y Brasil (parcial) en América y países de África, que utilizan datos biométricos para dar de alta a la persona habilitada para votar en el día de la votación**. Se observa que en la Unión Europea no se utiliza.

