Fundación
Karisma

Bogotá, 2 de junio de 2023

Honorables Representantes
CONGRESO DE LA REPÚBLICA

Ref: Proyecto de Ley 418 / 23 Cámara "Por la cual se expide el código del registro civil, identificacion de las personas y el proceso electoral colombiano"

Asunto: Comentarios de la Fundación Karisma al proyecto de ley de referencia

Honorable Representante,

Reciba un cordial saludo de la Fundación Karisma. Nos permitimos remitir esta comunicación para presentarle nuestras consideraciones y comentarios al **proyecto de ley 418 de 2023 Cámara (Código Electoral colombiano)**.

Este documento presenta nuestro análisis, comentarios y argumentos frente a las medidas contenidas en este proyecto de ley en lo referente a: **1. El uso de biometría y los sistemas de identidad en el marco de un Código Electoral; 2. Las auditorías técnicas a los sistemas informáticos utilizados en el proceso electoral; 3. El voto electrónico y 4. Otros mecanismos de transparencia.**

1. **Uso de biometría y sistemas de identidad en el marco de un Código Electoral**

   1.1. El uso irrestricto de todo tipo de biometría para la identificación y autenticación de las personas.

2. **Las auditorías técnicas a los sistemas informáticos utilizados en el proceso electoral**

   2.1. Las auditorías técnicas a los sistemas informáticos utilizados en los procesos electorales deben ser públicas, además de garantizar la transparencia y la confianza.

   2.2. Características básicas de una auditoría técnica, independiente y pública.

   2.3. Comentario final sobre la propuesta de auditoría técnica por parte de los partidos políticos y grupos significativos de ciudadanos.

3. **El Voto Electrónico**

Fundación
Karisma

3.1. No es oportuno implementar el voto electrónico. Esta tecnología no garantiza los principios de eficacia, inviolabilidad y secreto del voto
3.2. El voto electrónico ha sido rechazado en varios países democráticos
3.3. No hay claridad conceptual sobre qué es y cómo opera el voto electrónico en el proyecto de ley
3.4. El voto electrónico cede parte de la soberanía nacional a terceros
3.5. No es cierto que la progresividad en la implementación de la tecnologías de voto electrónico solucione los problemas intrínsecos de la misma
3.6. Sobre la viabilidad financiera

4. Transparencia y acceso a la información electoral

4.1. Acceso a la información.

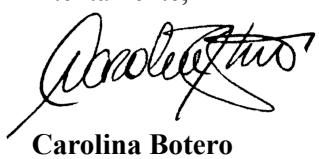
4.2. Sobre la observación electoral

Esperamos que en esta ocasión el trámite de la iniciativa legislativa sobre Código Electoral tenga un debate amplio sobre la participación de la sociedad civil y de los actores interesados, así como más minucioso para la comprensión de los problemas que hemos identificado y generar una iniciativa legislativa que subsane los retos en torno a los procesos electorales y que fortalezca el sistema democrático, la participación ciudadana, la transparencia y la garantía de derechos políticos y humanos relacionados.

Esperamos que estos argumentos contribuyan a una discusión legislativa detallada y sean acogidos para presentar modificaciones al texto de proyecto de ley. Ofrecemos nuestra experiencia técnica y nuestra trayectoría para discutir los temas expuestos en este documento.

Agradecemos su atención.

Atentamente,



Carolina Botero
Directora Ejecutiva
C.C.: 52.022.199 de Bogotá
Fundación Karisma

Fundación
Karisma

CONTENIDO

Fundación Karisma

1. Uso de biometría y sistemas de identidad en el marco de un Código Electoral

1.1. El uso irrestricto de todo tipo de biometría para la identificación y autenticación de las personas.

Desde el año 2021 la Fundación Karisma viene señalando los riesgos asociados al hecho de que la Registraduría pueda recolectar cualquier tipo de información biométrica en el cumplimiento de sus labores de identificación. Si bien una parte importante del código que se debate actualmente ya fue revisada y los temas relativos al sistema nacional de identidad se presentan aquí reducidos, lo que se mantuvo en el artículo 26, parte segunda, Disposiciones generales sobre la identificación de las personas, resulta preocupante en la medida en que no restringe los tipos de datos biométricos que la Registraduría puede recaudar ni el uso posterior que pueda hacer de ellos.

Esta es una oportunidad excepcional de erigir en Ley Estatutaria aquello que hoy en día sólo se encuentra regulado mediante jurisprudencia y actos administrativos, a saber la manera en que se recolecta información de las personas en las bases de datos de la Registraduría y más importante aún, qué información se recolecta. Sin embargo, por la misma razón es necesario aprovechar la oportunidad para trazar límites claros a dicha recolección de datos, en especial al tipo de datos que pueden recolectarse y al uso que puede dársele a los mismos. Limitar el tipo de biometría únicamente a biometría dactilar es una medida de seguridad que permite evitar abusos que sólo son posibles mediante otras formas de biometría, como la biometría facial. La recolección masiva –y sin posibilidad de rehusar el consentimiento– de datos biométricos faciales es el primer requisito técnico para construir sistemas de vigilancia masivos. Además la información facial se presta para usos discriminatorios, pues lleva implícita más información personal (como el tono de piel, o rasgos que pueden asociarse a la identidad o la expresión de género, entre otros) que la biometría dactilar y puede usarse para identificar personas sin que éstas están al tanto de que están siendo identificadas.

De igual manera, no hay nada que la biometría facial permita o facilite que no sea posible a través de al biometría dactilar. Además la primera lleva implícita mucha más información sobre una persona (con la biometría facial puede conocerse, por ejemplo, su tono de piel, su expresión de género o su edad aparente) que la segunda, lo que implica un uso mucho más invasivo que se presta, con mayor facilidad para su abuso. Por otra parte, debido a la manera en que son entrenados, los algoritmos de reconocimiento facial tienden a tener tasas más altas de fallos (instancias de falsos positivos o negativos en la concordancia del registro en la base de datos con la foto de la persona a autenticar) en el reconocimiento de los rostros de personas racializadas, de mujeres y de adultos mayores, lo que –en todas las instancias en que se utiliza reconocimiento facial como mecanismo de autenticación oficial– implica una desigualdad estructural en la garantía del derecho fundamental a la identidad legal.

Muchos de estos argumentos ya se habían presentado en 2021 cuando la Corte evaluó el proyecto de ley número 234 Senado, 409 de 2022 Cámara “Por el cual se expide el Código Electoral Colombiano y se dictan otras disposiciones”. En ese entonces la Fundación Karisma en compañía de El Veinte, la

Fundación para la Libertad de Prensa, Dejusticia, Linterna Verde e ISUR, presentaron una intervención ciudadana cuyos argumentos,por su relevancia presente, se reproducen a continuación[1]:

Tal como se mencionó en la intervención ciudadana, **el principal riesgo del uso de la biometría se ve reflejado en el derecho a la intimidad debido a que la biometría toma las características únicas de las personas y las conecta con diferentes áreas de la vida de ellas.** Por lo anterior, la ACNUDH dejo ver su preocupación al usar este tipo de tecnología en razón de que puede usarse para propósitos que van desde la seguridad nacional hasta la investigación criminal, el control fronterizo y la identificación para la provisión de servicios elementales[2]. Este tipo de sistemas, que se fundan en un sistema de identidad como el que se construye actualmente en Colombia, se prestan fácilmente para ser abusados y merecen una discusión regulatoria previa amplia.

En este sentido, desde Karisma advertimos que **el presente proyecto de ley no contempla límites para los tipos de datos biométricos que la RNEC puede recolectar de las y los ciudadanos, ni tampoco de los usos que puede hacer de los mismos.** Por ejemplo, no hay nada que evite que la recolección masiva de datos biométricos faciales posibilite el posterior despliegue de sistemas de vigilancia masivos.

Lo anterior también es preocupante porque los sistemas biométricos fallan, tienen errores en la lectura de los datos lo cual compromete el acceso de las personas vulnerables a servicios básicos cuando dependen de una autenticación plena. Un ejemplo de lo anterior es India, país en el cual está documentado cómo los fallos de reconocimiento biométrico están relacionados con el aumento de las muertes por inanición, en la medida en que las personas usuarias no pueden operar el sistema o este no logra autenticarlas adecuadamente.[3]

Además, otra consecuencia del uso de biometría es, como se mencionó en la intervención ciudadana, la discriminación por razón de origen, etnia y raza:

> *"En varios contextos, los datos de identificación terminan en sistemas de vigilancia masiva que discrimina ciertas poblaciones. Como lo menciona la Relatoría Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, el uso de tecnologías biométricas puede generar estructuras discriminatorias que "socavan de manera holística o sistemática el disfrute de los derechos humanos de determinados grupos, por motivos de raza, etnia u origen nacional, solos o en combinación con otros motivos"*
>
> *En la provincia de Xinjiang en China, las bases de datos biométricas creadas para otorgar identidad legal se utilizan para vigilar y ejercer violencia contra la minoría musulmana uigur. Esta base de datos contiene rostros, ADN, iris, voz y huellas. La Policía usa el sistema para identificar automáticamente uigures en cámaras privadas y públicas. Las personas de la comunidad solo pueden circular por ciertas zonas y, cuando se alejan, el sistema informa a las autoridades. Igualmente, sitios públicos como centros comerciales, edificios públicos, mercados y estaciones de tren tienen puntos de control*

[1] Fundación Karisma y otros (2021). Intervención ciudadana, pág. 5-6
[2] Ídem.
[3] ídem.
Ver también: India's Biometric ID System Has Led To Starvation For Some Poor, Advocates Say : NPR. (NPR, Consultado Noviembre de 2022)

> *que autentican a las personas y recogen datos de su comportamiento incluyendo localización, hora, frecuencia y razones de visita[4]"*

Lo anterior, como se puede observar muestra como el uso de biometría en sistemas de identificación puede afectar directamente derechos como la intimidad y la no discriminación de los ciudadanos. En el presente caso, permitir el uso de biometría en un documento de relevancia como la cédula de ciudadanía, no es conveniente y trae más problemas que soluciones.

Además teniendo en cuenta que los datos biométricos son considerados datos sensibles, según lo estipulado en el artículo 5 de la ley 1581 de 2012:

> *"ARTÍCULO 5o. DATOS SENSIBLES. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.[5]"*

Por lo tanto, la misma ley le ha dado protección especial al reglamentar que su tratamiento está prohibido (artículo 6), sin embargo se permitió la excepción del literal a), en la segunda parte que dice:

> *a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización[6];*

Si la propuesta del Código Electoral pasa cómo está, la RNEC tendría la facultad legal para recopilar todos los datos biométricos de las personas y usarlos según su criterio. El uso de todo tipo de biometría no tiene un fin que lo justifique, más allá que el afán de la RNEC por incluir tecnología en sus procedimientos. **Como está formulado, este proyecto permitiría que la RNEC pueda recolectar datos sensibles de las personas sin que exista un marco regulatorio claro que defina el trato y los usos permitidos y no permitidos de dichos datos, y sin que el titular tenga posibilidad de rehusar su consentimiento, pues se trata del proceso de expedición del documento nacional de identidad.**

Además de lo anterior, la biometría no garantiza que los procedimientos sean más expeditos. Esto por ejemplo fue evidenciado durante las elecciones de congreso del 2022, en las que la RNEC intentó implementar reconocimiento de biometría facial para el cambio de lugar de votación, pero los resultados fueron largas filas, problema de identificación y atraso en los procesos electorales que habilitaban a las personas a votar.

---

[4] Ídem.
[5] Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales.". Artículo 5.
[6] Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales.". Artículo 6.

Por otra parte, la biometría facial tampoco es una garantía de que la cédula digital sea más difícil de falsificar o proteja de la suplantación, pues no hay protecciones contra la posibilidad de crear falsos duplicados digitales de la aplicación de la cédula o explotar otras vulnerabilidades propias de los sistemas informáticos. Además, la seguridad digital del sistema de información que almacena los datos biométricos de toda la población colombiana carece de garantías y no es transparente. De implementarse un sistema de identidad de estas magnitudes sería necesario garantizar que dichos datos están adecuadamente protegidos.

Los beneficios de la cédula de ciudadanía con biometría facial no son claros, ni muestran una mejoría amplia que lo justifique. Dado que es necesario que la Registraduría Nacional del Estado Civil siga produciendo los documentos en físico para uso de las personas que no pueden, no tienen los medios económicos, no saben o no quieren usar tecnología, la inclusión de un equivalente funcional se vuelve una redundancia inútil. Lo anterior obliga a cuestionarse cuál es el sentido de la producción de un documento de identidad digital que no puede reemplazar al documento físico (pues las condiciones materiales no están dadas) y que, sin embargo, resulta en un costo elevado para el Estado.

De acuerdo con lo anterior, **la recomendación de la Fundación Karisma a este respecto es: limitar la recolección de datos biométricos por parte de la registraduría para que esté facultada únicamente a recoger datos biométricos dactilares, más no datos biométricos faciales, sin el consentimiento del titular.**

2. AUDITORIAS

2.1. Las auditorías técnicas a los sistemas informáticos utilizados en los procesos electorales deben ser públicas para garantizar la transparencia y la confianza en los resultados

Las auditorías técnicas a los sistemas informáticos son uno de los mecanismos que permiten evaluar y mejorar el funcionamiento de los mismos. Si se realizan de forma pública e independiente, también aportan a la transparencia del sistema y generan confianza en los resultados[7]. Es por estas características que, en la actualidad, dada la proliferación del uso de las TIC para materializar los derechos de la ciudadanía, las auditorías a los sistemas que utilizan los Estados para prestar servicios y garantizar derechos se han convertido en una regla general.

Entre todos los beneficios que incluyen las auditorías uno de los más importantes es la generación de confianza en la robustez, efectividad y transparencia del sistema. La cadena de software, hardware, servidores, protocolos de comunicación, medidas de seguridad que permiten el funcionamiento de una solución informática son de una complejidad tal que solo personas con conocimientos específicos y capacidades técnicas pueden comprender completamente cómo y para qué sirve. En otras palabras, las personas del común, la ciudadanía, no pueden comprender a plenitud su funcionamiento, convirtiendo estos en cajas negras.

---

[7] Durante los últimos 20 años se ha producido suficiente literatura por organizaciones expertas en la materia que nos permite hablar de unos estándares internacionales respecto de la incorporación de tecnología en procesos electorales. Así se deriva del análisis de documentos como los siguientes:
De organizaciones intergubernamentales:

- Consejo de Europa: Certification of e-voting systems Guidelines for developing processes that confirm compliance with prescribed requirements and standards -2011- o Legal, operational and technical standards for e-voting -2004-
- La Organización para la Seguridad y la Cooperación en Europa (OSCE): Handbook For the Observation of New Voting Technologies -2013-, Election Observation Handbook -2010-
- El Programa de las Naciones Unidas para el Desarrollo (UNDP); Electoral Results Management Systems -2016-.

También por actores regionales:

- Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) en Argentina: Análisis de factibilidad en la implementación de tecnología en diferentes aspectos y etapas del proceso electoral -2017-
- La Misión de Observación Electoral (MOE) en Colombia: Implementación del voto electrónico en Colombia -2014-
- Organización de los Estados Americanos (OEA): Tecnologías aplicadas al ciclo electoral -2014-.

De otras organizaciones sin ánimo de lucro de fuera de América Latina:

- Instituto Internacional para la Democracia y Asistencia Electoral (IDEA), Introducing Electronic Voting: Essential Considerations -2011-, Certification of ICT's in elections -2014-, International Electoral Standards Guidelines for reviewing the legal framework of elections -2002-
- La Fundación Internacional para los Sistemas Electorales (IFES) Electronic Voting & Counting Technologies A Guide to Conducting Feasibility Studies -2011-. Junto con NDI Implementing and Overseeing Electronic Voting and Counting Technologies -2013-.
- El Centro Carter. Developing a Methodology for Observing Electronic Voting -2007-, Handbook on Observing Electronic Voting -2021-.

Más recientemente se debe mencionar la guía del Commonwealth para ciberseguridad "Cybersecurity for Elections: A Commonwealth Guide on Best Practice"

Siendo así, cuando hablamos de elecciones soportadas o ayudadas por la tecnología las auditorías se vuelven cruciales. Si hay tecnología que media entre el voto depositado en una urna y el resultado, la ciudadanía tiene derecho a conocer de forma precisa y detallada qué papel juega la tecnología en el proceso y si existen posibilidades de que su voto no sea tenido en cuenta, que sea alterado su sentido, o que se rompa el secreto del mismo debido a vulnerabilidades o a un funcionamiento anormal en el sistema tecnológico que intermedia. Solo así se garantizará que los resultados de las elecciones son legítimos y que la participación de toda la ciudadanía se ha dado en condiciones iguales y óptimas.

En el caso colombiano, desde hace años se han introducido soluciones tecnológicas que incluyen software y hardware para las elecciones nacionales. En 2022 algunos de los programas que se contrataron fueron el software para el cambio de lugar de votación, la aplicación para proveer información a la ciudadanía sobre los puestos de votación, el hardware y software utilizado para el proceso de escrutinio, el software para la selección de jurados de votación y el software para la inscripción y acreditación de testigos electorales, entre otros.

Para el escrutinio, se consolidan los votos y se gestionan las reclamaciones usando soluciones tecnológicas. Estos mismos sistemas también permiten hacer la declaración del ganador. Es completamente natural, entonces, que en Colombia, que es un estado democrático, se requiera una auditoría que sea técnica, independiente y pública[8] sobre los software de escrutinio y del proceso electoral en general para garantizar la transparencia e integridad de las elecciones, y para generar confianza en los resultados.

1.2 Características básicas de una auditoría técnica, independiente y pública

Ahora bien, las auditorías a las tecnologías que intervienen en el proceso electoral deben cumplir nueve características básicas si se quiere que garanticen la transparencia e integridad de las elecciones y así debe consagrarse en la ley:

1. Una auditoría debe ser entendida como una revisión detallada y completa de un sistema informático buscando determinar si éste es robusto, confiable, seguro, si realiza exclusivamente las operaciones y funciones para las cuales fue diseñado y si garantiza la integridad en el procesamiento de toda la información[9], aspecto fundamental para un sistema electoral. Esto implica que los auditores deben tener acceso a todas las partes y componentes del sistema y en particular a todo el código fuente del software desarrollado. Además, la protección de los derechos económicos de un privado no deben convertirse en una barrera para el acceso a la información relacionada con las elecciones por parte del auditor. Los resultados de la evaluación deben ser acogidos para generar mejoras. Respecto de los hallazgos que no sean tenidos en cuenta por el desarrollador deberá explicar las razones para no hacerlo e incluir, de ser necesario, un plan de mitigación.

[8] Es necesario señalar que cuando se publica una auditoría de este tipo se puede ocultar ciertos detalles técnicos o ciertas vulnerabilidades cuyo conocimiento no aportarían mucho a la ciudadanía y que podrían facilitar un ataque.
[9] Misión de Observación Electoral y K-LAB.protocolo de auditoría para el software de escrutinio Elecciones Colombia 2018. Disponible en: https://www.moe.org.co/publicacion/propuesta-moe-protocolo-de-auditoria/

2. Aunque depende de la complejidad y el tamaño del sistema que se va a analizar, toda auditoría requiere de diferentes experticias, de un plazo de tiempo considerable para ser realizada y también implica un acceso completo a los sistemas (en particular al código fuente de las aplicaciones), a la versiones funcionales del software, a los equipos usados para correr los sistemas (hardware), a los servidores y bases de datos donde se aloja la información, a los registros (logs) de cada componente del sistema y todos los documentos que expliquen y sean producidos por el sistema.

3. La auditoría que se consagre en el nuevo código debe tener tres cualidades para que pueda cumplir su función: 1) debe ser técnica, en el sentido de que debe ser realizada por expertos en la materia o en la tecnología a revisar y en la que se evalúa y prueba aquellos componentes tecnológicos o técnicos del sistema a profundidad (por ejemplo, si el software está escribo en lenguaje Java, el experto que analice el código debe conocer a profundidad el lenguaje Java); 2) debe ser independiente, es decir, su ejecución y resultados no puede estar sujeta contractualmente ni al desarrollador de la tecnología ni a partidos políticos o grupos significativos de ciudadanos ni al organizador de la elecciones ni a sus contratistas; 3) debe ser pública, es decir, que sus resultados deben darse a conocer de forma segura a la ciudadanía para generar confianza (por razones de seguridad la versión pública de la auditoría puede omitir los detalles técnicos de las vulnerabilidades activas aunque sí debe incluir las acciones para mitigarlas).

4. Un sistema cómo el que se usa en Colombia requiere programas específicamente desarrollados que usan bibliotecas de software ya establecidas, corren en servidores y computadores que usan componentes de hardware, sistemas operativos, sistemas de base de datos, componentes aplicativos ya definidos, se conectan con redes que tienen sus componentes y protocolos. Todas estas partes establecidas pueden tener vulnerabilidades conocidas o no, y, por lo tanto, deben ser actualizadas periódicamente. Además, los auditores deben, dentro de lo posible, poder evaluar todos estos componentes.

5. Contrario a lo sucedido hasta la fecha, las auditorías a los sistemas tecnológicos implementados en el proceso electoral, sin importar la etapa ni el tamaño del sistema, no deben limitarse a la fase funcional del mismo. Es decir, la auditoría no debe limitarse a verificar si la interfaz gráfica del sistema (frontend) cumple de forma correcta con las funciones que se estableció previamente que tendría o si tiene todas los componentes o secciones preestablecidas. Según lo visto por Karisma en su ejercicio de observación técnica en las elecciones colombianas, la Registraduría solo ha facilitado espacios de observación técnica que se comparten con los auditores contratados. El alcance de estos espacios escasamente cobija sólo lo funcional.

6. Sin afectar su independencia, las auditorías deben ser abiertas y permitir la participación activa de los partidos políticos y de los grupos de ciudadanos. Estos deberían poder citar a los auditores a explicar los procedimientos utilizados y sus hallazgos. En el mismo sentido, los desarrolladores deberán explicar los cambios aplicados para mejorar el sistema y los mecanismos de mitigación de las vulnerabilidades residuales.

7. Es necesario que las auditorías se realicen con el tiempo suficiente para realizar una evaluación completa de todos los niveles del sistema (documental, hardware y software incluyendo el código fuente) y que los hallazgos sean puestos en conocimiento del operador para ser corregidos antes de que el sistema entre en funcionamiento. Desde Karisma consideramos que el tiempo mínimo para presentar hallazgos y realizar las correcciones del caso es, como mínimo, seis meses antes del uso de la tecnología. Por tanto la contratación de los desarrolladores y de las auditorías debe realizarse con suficiente antelación, el proceso se debería comenzar al menos un año antes del día que será usado el sistema.

8. Ya que las características propias de una auditoría exigen un análisis completo y detallado de todas los componentes del sistema y dista de la simple observación, se debe establecer claramente el alcance de rol de los auditores y diferenciarlo de los observadores (técnicos o no). De forma tal que se facilite las tareas del auditor, de los observadores y no se generen falsas expectativas o confusiones sobre el alcance de las funciones[10].

9. Si bien las auditorías son indispensables, estas deben estar acompañadas de otros mecanismos de transparencia como la observación electoral, la publicación activa de datos abiertos, la transparencia en la contratación y, por supuesto, la posibilidad de verificar y acompañar el proceso electoral por parte de la sociedad civil, partidos políticos y grupos significativos de ciudadanos.

1.3 Comentario final sobre la propuesta de auditoría técnica por parte de los partidos políticos y grupos significativos de ciudadanos

Finalmente, consideramos necesario abordar la propuesta discutida en el Congreso colombiano respecto de que la auditoría la podrían realizar los partidos políticos. Empezamos por señalar que debido a la carga de trabajo y al nivel de experticia que requiere una auditoría técnica a un sistema de la complejidad del usado en las elecciones en Colombia es poco probable que las organizaciones políticas en Colombia cuenten con los recursos, la capacidad técnica y humana, y el tiempo para hacer la revisión de todos los sistemas incluidos en el proceso electoral. De forma tal que, sería preocupante que esto quede así regulado en la ley y en la práctica debido a los costos y la falta de capacidad las auditorías no se realicen.

Hay que tener en cuenta que la auditoría debe realizarse de forma independiente, de forma que sirva como mecanismo para generar confianza y transparencia para toda la sociedad y no solo para un partido o movimiento político con la capacidad suficiente para implementar una revisión detallada. Que la auditoría sea realizada por un partido o grupo significativo podría generar sesgos políticos en la interpretación de los resultados, perdiéndose así el objetivo primordial de hacer más transparente y confiable el sistema.

[10] *Guía básica para la discusión sobre auditorías tecnológicas al proceso electoral en Colombia 2022*,

Al respecto, queremos señalar que es un deber del Estado, y no de los partidos, garantizar la transparencia e integridad de los sistemas tecnológicos. Trasladar la responsabilidad de realizar la auditoría a los partidos solo hará más difícil su ejecución de forma completa y, probablemente, limite su capacidad de dar tranquilidad respecto al sistema.

Para Karisma considera que esta labor la debe realizar la autoridad electoral o un tercero contratado para ello, en cuyo caso, la transparencia debe extenderse al proceso de contratación. En cualquier caso, es fundamental que los partidos políticos y la ciudadanía en general puedan participar efectivamente en calidad de observadores y tener acceso total a las evaluaciones, hallazgos y conclusiones de los expertos, de manera tal que se fortalezca la transparencia del proceso y la confianza electoral.

3. VOTO ELECTRÓNICO

2.1. No es oportuno implementar el voto electrónico. Esta tecnología no garantiza los principios de eficacia, inviolabilidad y secreto del voto

La Fundación Karisma expresa su preocupación por la posible implementación del voto electrónico en el país. Consideramos que la aplicación de esta tecnología no garantiza los principios de *e*ficacia, inviolabilidad y secreto del voto. Además afecta la publicidad del escrutinio y la transparencia del sistema. Solicitamos al Congreso que elimine del presente proyecto de Código Electoral la regulación que permite el uso del voto electrónico.

Así, la integración de tecnologías para el voto, deben contener mecanismos que garanticen la separación de los actos de autenticación del votante, el acto de sufragio y el acto de conteo para evitar la identificación del sufragante con su voto.

2.2 El voto electrónico ha sido rechazado en varios países democráticos

El uso de voto electrónico no cuenta con aprobación internacional generalizada. En países como Alemania, Países Bajos, Reino Unido, Irlanda, Finlandia, Noruega, Kazajistán[11] que inicialmente habían transitado o probado la tecnología de voto electrónico, se ha desistido de esta idea dado los

[11] Asociación de Tecnología, Educación, Desarrollo, Investigación, Comunicación. «Urnas electrónicas», hechos y experiencias para un voto informado. Disponible en: https://www.tedic.org/urnas-electronicas-hechos-y-experiencias-para-un-voto-informado/
Asociación de Tecnología, Educación, Desarrollo, Investigación, Comunicación. «Urnas electrónicas», hechos y experiencias para un voto informado. Disponible en: https://www.tedic.org/voto-electronico-solucionismo-electronico/
Véase también: https://twitter.com/TEDICpy/status/1120453271624265730

riesgos para la integridad[12] de las elecciones y hay otros como Corea del Sur[13] que aún contando con experticia técnica han decidido no incorporarlo por falta de garantías. Su principal argumento es que el componente altamente técnico impide a la ciudadanía hacer un control y seguimiento del sistema y de los resultados, lo que vuelve el voto y su consolidación un proceso poco transparente. Adicionalmente, el uso de tecnologías que permiten el voto electrónico abre la posibilidad a la manipulación del sistema y sus resultados por una única persona o un grupo pequeño de personas (desde dentro o fuera del país), un escenario poco probable en el sistema analógico debido a su complejidad y magnitud.

Respecto de los problemas con el voto electrónico el caso alemán es muy diciente. La Corte Constitucional alemana falló en contra de la utilización de estas tecnologías, debido a su incompatibilidad con la constitución de ese país y la posible vulneración de las garantías electorales. Según el tribunal, la confianza de la ciudadanía y de los actores políticos en el sistema y los resultados debe ser pilar fundamental de la construcción de leyes electorales, algo que la complejidad innata del voto electrónico impedía. Las elecciones como acto público, exigen que cualquier ciudadano pueda comprender cabalmente cómo funcionan y los pasos esenciales para determinar los resultados, algo que (repetimos) impide el voto electrónico[14].

La implementación del voto electrónico en Países Bajos fue revertida en 2006 luego de que se realizarán auditorías solicitadas por grupos de ciudadanos quienes no sentían confianza sobre las máquinas electrónicas utilizadas en el proceso electoral[15]. Dichas revisiones técnicas revelaron serias inconsistencias en los sistemas, respecto a la transparencia y el secreto del voto. Como se lee en el reporte de la MOE: “En mayo de 2008 el gobierno holandés prohibió el uso de máquinas electrónicas para la votación regresando al uso de tarjetones electorales y lápices rojos para votar”[16].

Recientemente podemos señalar en Argentina[17] la implementación del voto electrónico en la provincia de Neuquén. En el Reporte de observación del Observatorio Electoral de la Universidad Nacional del Comahue[18] quedó señalado que en algunas mesas los votos fueron computados como nulos ya que los

---

[12] Departamento de Seguridad Gobierno Vasco. Voto electrónico en el mundo. Disponible en: https://www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2haukon/es/ , Computerphile. Why Electronic Voting is a BAD Idea. Disponible en: https://www.youtube.com/watch?v=w3_0x6oaDmI y Tom Scott. Why Electronic Voting Is Still A Bad Idea. Disponible en: https://www.youtube.com/watch?v=LkH2r-sNjQs

[13] Alejandro Bercovich. Corea del Sur, sistema de votación coreano con boleta única de papel. Disponible en: https://www.youtube.com/watch?v=Lx69LWfzSFI

[14] Fundación Vía Libre. Alemania: urnas electrónicas anticonstitucionales. Disponible en: https://www.vialibre.org.ar/alemania-urnas-electronicas-anticonstitucionales/

[15] Newsweek. Netherlands abandons Electronic vote Counting Amid Hacking Fears. Disponible en: https://www.newsweek.com/dutch-election-electronic-voting-hacking-russia-france-macron-trump-clinton-564198

[16] Misión de Observación Electoral. Implementación del voto electrónico en Colombia. Disponible en: https://www.moe.org.co/wp-content/uploads/2017/06/Libro-Implementaci%C3%B3n-del-Voto-electr%C3%B3nico-en-Colombia.pdf

[17] Joaquín Sorianello. Voto electrónico ¿avance tecnológico?. Disponible en: https://www.youtube.com/watch?v=mVNzL0l5U3k

[18] Observatorio Electoral de la Universidad Nacional del Comahue. Reporte de observación elecciones provinciales Neuquén 2023. Disponible en:

votantes no leyeron el mensaje de error del voto que era impreso por la máquina antes de depositarlo en las urnas. En otros casos fueron computados como votos nulos porque en la urna se depositaron sin impresión textual ni chip. Se asume que el votante no colocó la boleta única electrónica en la máquina y luego la puso en la urna. En el mismo reporte se señala que el sistema está gestionado por una única empresa, otorgándole el control absoluto del proceso y que las audiencias para observación de los componentes del sistema que brindó la Justicia Electoral de la Provincia de Neuquén para analizar el software y hardware del sistema de Boleta Única Electrónica no son suficientes para garantizar el correcto funcionamiento del sistema.

En suma, el debate sobre la utilización del voto electrónico en el mundo sigue vigente y no parece haber un consenso entre los países sobre las ventajas de implementar este tipo de mecanismos al proceso electoral.

2.3 No hay claridad conceptual sobre qué es y cómo opera el voto electrónico en el proyecto de ley

Es importante dejar en claro que hay distintas modalidades de voto electrónico[19] dependiendo de cuales son las funciones realizadas por el sistema y si deja constancia o no de este proceso.

Todo sistema de votación requiere por lo menos 3 procesos.

1. Identificar y autenticar el votante. Con el fin de asegurar que la persona que ejerce el derecho esté legalmente habilitado para hacerlo, sea quien dice ser y no se presente suplantación o duplicidad.
2. Emitir el voto. La persona que vota debe expresar su voluntad y esta se debe materializarse en un registro que pueda ser contabilizado
3. Consolidar el resultado. En este proceso se deben contabilizar los votos y permitir llegar a un resultado sin que se modifique en ningún momento la intención del voto emitido.

Para cada uno de estos procesos se puede usar tecnología, sin embargo hay un acuerdo generalizado en que un mismo sistema que pueda identificar al votante y emitir el voto es bastante problemático, ya que en esos casos es imposible garantizar el secreto del voto.

Un sistema que emita y consolide el resultado puede ser problemático si no cuenta con mecanismos adicionales de transparencia que faciliten constatar el sentido del voto emitido y que permitan realizar un seguimiento de la consolidación del resultado de forma que no se modifiquen los resultados parciales o finales.

Existen diferentes modalidades de voto electrónico. Por ejemplo, el voto electrónico presencial, a través de máquinas ubicadas en los puestos de votación, y el voto electrónico a distancia (también

https://observatorioelectoral.uncoma.edu.ar/wp-content/uploads/2023/05/Informe_Elecciones_Neuqu_n_.2023_versi_n_2-1.pdf

[19] Asociación de Tecnología, Educación, Desarrollo, Investigación, Comunicación. «Urnas electrónicas», hechos y experiencias para un voto informado. Disponible en: https://www.tedic.org/voto-electronico-parte-2-modalidades-basicas-y-sus-falencias/

conocido como por internet o digital)[20], en el cuál, como su nombre lo indica, el sufragio se realiza a través de programas conectados a internet o el correo electrónico donde el votante debe autenticarse, seleccionar la candidatura que apoya y enviar su voto.

El voto electrónico a distancia, hasta ahora no tiene plenas garantías para que se mantenga el secreto del voto y por esta razón se descartó en la discusión de actualización del código electoral adelantada en 2020 y que fue tumbada por la Corte Constitucional.

El voto electrónico presencial también tiene diferentes modalidades dependiendo de la constancia o no de la emisión del voto. En este sentido puede ser mixto y dejar constancia impresa que se deposita en una urna física, como por ejemplo la modalidad de Boleta Única Electrónica que se ha usado en Argentina[21] o el voto electrónico provisto por Smartmatic para las elecciones en Venezuela[22], o ser solamente contabilizado por la máquina en el momento en que se ejerce el sufragio y generar un resultado de mesa que se envía a un sistema central de consolidación sin constancia física de cada voto, como funciona en Brasil[23], lo que fue usado en las últimas elecciones por el expresidente Jair Bolsonaro en sus acusaciones sobre fraude[24].

En cuanto a la consolidación surge una nueva diferencia entre posibles sistemas de votación electrónica presencial, si generan un resultado y lo transmiten, voto a voto o consolidado al cierre de las mesas, lo que plantea un riesgo al tener máquinas conectadas a internet y susceptibles de manipulación remota. O si los resultados se consolidan y comprueban por personas en cada mesa de votación y se transmiten por un sistema diferente.

El código electoral habla de Voto electrónico y de voto electrónico mixto en su artículo 153 donde se definen las modalidades del voto. La definición del tipo debería ser única, ya que los dos sistemas tienen desafíos diferentes.

En el proyecto de ley no es posible determinar con claridad qué capacidades tendrán las máquinas o sistemas que se utilicen. En el Artículo 153, sobre las modalidades del voto, se establecen dos modalidades posibles: el “Voto electrónico mixto”, el cual se ayuda de la tecnología para los procesos de emisión y conteo de los votos. Esto se realizará mediante una terminal electrónica en la cual se

---

[20] Derechos Digitales. Voto Electrónico en Chile y marco normativo electoral: problemas legales de un cambio tecnológico tentador. Disponible en: https://www.derechosdigitales.org/14836/voto-electronico-en-chile-y-marco-normativo-electoral-problemas-legales-de-un-cambio-tecnologico-tentador/

[21] TEDxTalks. Joaquin Sorianello. Voto electrónico ¿Avance tecnológico? Disponible en: https://www.youtube.com/watch?v=mVNzL0l5U3k

[22] BBC.Cómo funciona el sistema de voto electrónico de Smartmatic, la empresa que denunció manipulación en la elección de la Constituyente en Venezuela. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-40815645

[23] Asociación de Tecnología, Educación, Desarrollo, Investigación, Comunicación. Voto electrónico en Paraguay. El encierro de la democracia en una caja negra. Disponible en: https://www.tedic.org/wp-content/uploads/2020/12/Voto-electronico-Busaniche-web.pdf y BBC. Brazil election: Do voting machines lead to fraud? Disponible en: https://www.bbc.com/news/63061930

[24] Asociación de Tecnología, Educación, Desarrollo, Investigación, Comunicación. Voto electrónico Parte 2: modalidades básicas y falencias. Disponible en; https://www.tedic.org/voto-electronico-parte-2-modalidades-basicas-y-sus-falencias/

consignará la preferencia del elector, que no podrá estar conectado a una red pública (internet) y producirá una constancia física que se depositará en una urna y el "Voto electrónico", como el marcado por el votante con ayuda de tecnología en el proceso de emisión y/o conteo del voto. Si las dos son posibles no es claro que modalidad finalmente es la permitida ya que la segunda engloba la primera y cualquiera de las otras opciones posibles a las que nos referimos anteriormente. Además, el artículo 237 añade, de forma contradictoria, capacidades a las máquinas de voto electrónico entre las que están imprimir actas (lo que implica consolidar los resultados de la mesa de votación) y transmitir los resultados electorales. Esta última función implica que el sistema esté conectado a una red pública, lo que hace vulnerable a la máquina ya que está conectada a internet y se pierde la capacidad de contrastar el conteo ya que la máquina es la que realiza el proceso.

En caso de que la máquina sea la encargada de emitir, contabilizar, totalizar los resultados, y de enviar los mismos al sistema de seguimiento, la trazabilidad del proceso se pierde. Es decir, no queda un rastro físico que permita a partidos y ciudadanos contrastar resultados y acopiar pruebas para sustentar sus reclamaciones. Para el caso Colombiano, la existencia de comprobantes en papel, es una garantía de que se respete el sentido del voto de la ciudadanía. Ejemplo de ello es lo sucedido durante las pasadas elecciones legislativas.

Respecto del voto electrónico el proyecto de ley incluye otros artículos que son problemáticos. El primer problema es el Artículo 123 que señala que los jurados de votación revisarán el buen funcionamiento del sistema, esto implicaría que todo los jurados serán expertos con capacidad de verificar el hardware y software de las máquinas, algo imposible. Para Karisma lo único que pueden verificar los jurados es si el sistema inicia el conteo en ceros y si el hash del sistema es el mismo que les fue previamente entregado.

El segundo inconveniente es que el proyecto de ley no incluye una modalidad de voto electrónico nulo. Esta posibilidad debe ser consagrada para los casos en que la boleta impresa no refleje la voluntad política de la persona que está votando o cuando el sistema por errores de software o de impresión emita un comprobante que no cumpla los requisitos legales.

2.4 El voto electrónico cede parte de la soberanía nacional a terceros

El voto electrónico implica, per se, delegar en un sistema controlado, diseñado y, en ocasiones, propiedad de un tercero la emisión, conteo y/o consolidación de los sufragios que deciden el futuro político de una nación. Es usual que los terceros administren y gestionen el sistema, debido a su complejidad (como sucede el caso cdolombiano), lo que pone en sus manos un proceso básico de la democracia y por tanto su soberanía.

Si bien las alianzas con privados no deben ser demonizadas y, por el contrario, resultan útiles en muchos casos, el Estado debe evaluar qué capacidades entrega, y sobre todo, qué medidas toma para asegurarse de conservar el poder de decisión para evaluar las actuaciones de terceros en su nombre, y para garantizar, que la soberanía nacional no sea superpuesta a intereses privados o extranjeros.

La construcción de capacidad técnica en el Estado para operar y controlar los sistemas tecnológicos que se implementen en elecciones es una medida democrática primordial. Que entidades como CNE, Registraduría o Procuraduría tengan la capacidad de entender y operar el sistema para verificar que los derechos de la ciudadanía no están siendo vulnerados debe ser uno de los contrapesos y medidas de transparencia explícitamente reguladas en el nuevo código.

Por un lado, el conocimiento del sistema permitirá aumentar la transparencia, pues se crea una línea directa de diálogo con la ciudadanía, sin la necesidad de consultar la voluntad de terceros privados. Por el contrario, que el Estado dependa de un privado para operar y para resolver peticiones de la ciudadanía, supedita a esta a la voluntad de una empresa privada, como lo explicamos en nuestros informes de observación electoral de 2022[25].

Por otro lado, que el Estado tenga capacidad de controlar el sistema que se utiliza para las elecciones, sin terceros, aumenta no solo su poder soberano, sino la posibilidad del Estado para hacer control interno y contrapesos entre instituciones. Respecto de este último punto, debe recordarse la decisión del Consejo de Estado en el caso del partido MIRA, ya que fue la dependencia del Estado de un tercero uno de los causales de que no fuera posible reconstruir lo sucedido a detalle en las elecciones de 2016. En consecuencia, una de las recomendaciones fue que el Estado adquiriera un sistema propio, pero además, que estuviera en capacidad de operar y controlarlo a un nivel de detalle que impida que el sistema se convierta en un obstáculo para el principio de la efectividad del voto.

2.5. No es cierto que la progresividad en la implementación de la tecnologías de voto electrónico solucione los problemas intrínsecos de la misma

No es cierto que la progresividad en la implementación de la tecnologías de voto electrónico solucione los problemas intrínsecos de la misma. Quienes defienden el voto electrónico señalan de forma imperativa que se deben incorporar tecnologías al sistema electoral para no quedar atrapados en el obsoletismo electoral. Además, señalan que los problemas de integridad, transparencia y confianza en el sistema inherentes al voto electrónico no aplican ya que en Colombia el voto electrónico se implementará de forma progresiva y usando planes piloto. Al respecto, es importante señalar varias asuntos:

No está claro cómo será la implementación progresiva y en qué consistirán los pilotos. En estas condiciones no hay certeza de cómo se garantizará la igualdad entre los resultados obtenidos fruto de del pilotaje y los oficiales o cómo se resolverá las discrepancias.

Más importante aún, una prueba piloto de un sistema informático está limitada por la muestra usada y por la pérdida constante de vigencia de la tecnología probada. En este sentido, un piloto por grande que sea, no iguala las condiciones reales de las elecciones nacionales y los problemas no previstos son una posibilidad muy real. Además, dado que la tecnología cambia rápidamente debido a

[25] Fundación Karisma. Segundo informe de observación electoral: primera vuelta presidencial Colombia 2022. Disponible en. https://web.karisma.org.co/segundo-informe-de-observacion-electoral-primera-vuelta-presidencial-colombia-2022/

vulnerabilidades descubiertas, actualizaciones o recomendaciones de los auditores no es posible garantizar las mismas condiciones.

Siendo así, la progresividad y las pruebas piloto si bien son útiles al implementar cualquier tecnología, no resuelven los problemas intrínsecos del voto electrónico y dado la magnitud del sistema electoral no suponen una prueba fiable de su integridad y transparencia.

2.6 Sobre la viabilidad financiera

Finalmente, si bien Karisma, no comparte el argumento de supeditar la garantía y protección de los derechos fundamentales a cuestiones económicas. Teniendo en cuenta los problemas del voto electrónico, los recursos limitados y la necesidad de garantizar el derecho a la participación política mediante otras acciones urgentes, como es la de una auditoría a la tecnología que ya se implementa en el proceso electoral, llamamos la atención sobre si vale la pena gastar el presupuesto en una tecnología que no cuenta con aprobación técnica y que puede poner en peligro la democracia. De forma similar llamamos la atención en el sentido de que si se implementa el voto electrónico incorporando las limitaciones que se requieren en las máquinas para garantizar el secreto del voto y la integridad de su sentido (no autenticar identidad, no tener papel en el escrutinio y no estar conectadas a Internet) lo que se terminará implementando son costosas impresoras.

3. OTRAS MEDIDAS DE TRANSPARENCIA

3.1. Acceso a información

Respecto al acceso de información en el proceso electoral, los informes que generamos los años pasados con base en nuestra experiencia como observadores, junto a la Misión de Observación Electoral, son claros en señalar la necesidad de acceder a la información electoral de forma oportuna. Esto con el fin de permitir no sólo la observación, sino también el seguimiento y las reclamaciones que podrían hacer los partidos y grupos significativos de ciudadanos y las posibles investigaciones de la academia sobre los comportamientos y resultados de las elecciones, entre otras cosas[26].

Dado que el sistema electoral está tercerizado, ya sea para su organización física, la divulgación de los resultados o la realización del preconteo y el escrutinio, es necesario que los privados que se encargan de prestar sus servicios permitan a la ciudadanía acceso suficiente para garantizar su derecho al control y a la participación política. Esto se debe exigir desde el momento de la contratación para evitar opacidad o niveles de acceso diferente según el contratista.

Además, se debe evitar condicionar el acceso a información mediante cláusulas o contratos de confidencialidad que protejan los intereses de los privados y limiten los derechos de la ciudadanía. En

[26] Fundación Karisma. 14 recomendaciones para proteger la democracia y la efectividad del voto en las elecciones del futuro. Disponible en: https://web.karisma.org.co/14-recomendaciones-para-proteger-la-democracia-y-la-efectividad-del-voto-en-las-elecciones-del-futuro/

caso de tercerización, se debe crear un mecanismo que permita controlar el actuar de las nuevas empresas involucradas en las elecciones.

En ese orden de ideas, resulta fundamental caminar hacia la publicación de los datos electorales como datos abiertos. Según el Ministerio TIC los datos abiertos son información pública dispuesta en formatos que permiten su uso y reutilización bajo licencia abierta y sin restricciones legales para su aprovechamiento[27]. En concordancia, la Ley de Acceso a Información Pública (Ley 1712 de 2014) define datos abiertos como "aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas (como la Registraduría) ".

Este tipo de datos deben estar puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que puedan reutilizarlos y crear servicios derivados de los mismos[28]. En este caso, para que partidos políticos, grupos ciudadanos, misiones de observación electoral y ciudadanía en general puedan ejercer sus derechos de participación y control al poder público.

Reiteramos que los órganos, organismos y entidades estatales independientes o autónomos (como la registraduría) y de control están obligados a publicar datos abiertos, igual que los partidos o movimientos políticos y los grupos significativos de ciudadanos.

Existe ya un documento CONPES[29], lineamientos por parte del Ministerio TIC sobre la publicación de datos y hay una infraestructura facilitada para ello. De hecho hay una Guía Nacional de Apertura de Datos[30] que explica paso a paso las actividades a realizar para desarrollar la identificación y priorización de los conjuntos de datos a publicar por las entidades.

La organización electoral (RNEC y CNE) pueden adoptar medidas sobre el acceso a la información; estas nos acercarán un poco más al objetivo de credibilidad y confianza en el sistema electoral que tanto preocupa a diversos sectores en la actualidad.

La implementación de la publicación de datos electorales como datos abiertos permite la consulta, descarga, procesamiento y reutilización de la información, es una medida de transparencia electoral. El tipo de información que debería ser ofrecida por la autoridad electoral abarca cuentas claras, las estadísticas sobre el comportamiento en inscripción de cédulas, datos estadísticos de los jurados de

---

[27]Datos abiertos. ¿Tu primera vez con datos abiertos? Aquí te contamos por dónde empezar. Disponible en: https://www.datos.gov.co/stories/s/-T-primera-vez-con-Datos-Abiertos-Aqu-te-contamos-/smn2-7atz

[28] Datos abiertos. ¿Tu primera vez con datos abiertos? Aquí te contamos por dónde empezar. Disponible en: https://www.datos.gov.co/stories/s/-T-primera-vez-con-Datos-Abiertos-Aqu-te-contamos-/smn2-7atz

[29] Consejo Nacional de Política Económica y Social. CONPES 4070. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjU09GqjPr-AhXdSDABHXsSAZkQFnoECBYQAQ&url=https%3A%2F%2Fcolaboracion.dnp.gov.co%2FCDT%2FConpes%2FEcon%25C3%25B3micos%2F4070.pdf&usg=AOvVaw2iVwqtXROeNTgCFtwERQra

[30] Ministerio de Tecnologías de la Información y la Comunicación de Colombia. Guía para el uso y aprovechamiento de Datos Abiertos en Colombia. Disponible en: https://herramientas.datos.gov.co/sites/default/files/2021-08/Guia%20de%20Datos%20Abiertos%20de%20Colombia.pdf

votación, testigos electorales, los datos de la votación mesa a mesa de preconteo y escrutinio, entre otros[31].

Además de ello, las autoridades electorales deben informar a la ciudadanía sobre la pertinencia de la incorporación de tecnologías en el proceso electoral, dar información suficiente sobre los algoritmos y la forma como se interconectan los procesos y la forma en qué se implementara con las condiciones de seguridad que se requieren. Esto requiere de procesos de socialización oportuna.

Por su parte, tanto en el preconteo como en el escrutinio el acceso a la información y la transparencia respecto a los datos tiene que ser una máxima rectora. Así, los tiempos de entrega de los datos de preconteo, aún cuando estos no tengan vinculación jurídica, deben ser compartidos con la ciudadanía en general a la mayor brevedad posible posterior al cierre de las urnas. Sobre el escrutinio los datos deben estar desagregados y permitir la trazabilidad completa de los mismos.

3.2. Sobre la observación electoral

A partir de la experiencia que hemos tenido tanto en la revisión de las propuestas de modificación al código electoral pasados como en la observación técnica con la que hemos acompañado la MOE, hay una aspecto que aún nos preocupa en la redacción actual del proyecto de código electoral y es el uso del término auditoría de forma ligera, lo que genera confusión en las funciones y alcance de auditores y observadores técnicos de los partidos.

Como ya lo mencionamos en el apartado de la auditoría, este es un proceso realizado por expertos técnicos que requiere muchos recursos, además de acceso a profundidad a los diferentes componentes del sistema y un tiempo importante de dedicación para su elaboración. Estos factores hacen muy difícil que los partidos políticos y grupos significativos de ciudadanos puedan realizar una auditoría al sistema electoral. Sin embargo, sí es posible hacer observación técnica de estos sistemas .

La observación se entiende como un proceso de menor alcance donde se atienden una serie de reuniones en las que se muestra la funcionalidad, se explican las medidas de seguridad, se da indicaciones sobre los mecanismos de acceso a la información, entre otras cosas, de cada una de las partes del sistema, idealmente se muestran además los resultados del proceso de auditoría y se despejan las inquietudes que puedan tener los representantes de partidos políticos y grupos significativos de ciudadanos, misiones de observación, entendes de control y otros actores interesados en el proceso electoral.

Los simulacros, las presentaciones de componentes del sistema, las muestras de código y otras actividades resultan especialmente útiles para que misiones electorales nacionales e internacionales, las organizaciones de la sociedad civil y los partidos políticos puedan observar el sistema electoral y hacer sus respectivas recomendaciones. Por esta razón, hacemos un llamado a que se conserven estas actividades, se amplíe la duración de las mismas, se aumente el acceso a la información de forma

[31] MOE. El derecho al acceso a la información durante las Elecciones en Colombia 2022, una mirada desde la observación electoral'. Disponible en: https://www.moe.org.co/informe-moe-el-derecho-al-acceso-a-la-informacion-durante-las-elecciones-en-colombia-2022-una-mirada-desde-la-observacion-electoral/

previa a los eventos; para garantizar una debida preparación, y para que se establezcan agendas precisas que permitan optimizar la observación. En ningún caso la observación debe limitarse solo a la capa de funcionalidad.

Finalmente, es necesario revisar con cuidado los deberes, facultades y obligaciones de las misiones de observación, técnicas o no. La imposición de sanciones como no permitir participar de futuras elecciones, la limitaciones a los derechos de libertad de expresión de las misiones, la imposición de sanciones por molestar a funcionarios públicos, la obligación de rendir cuentas mediante informes a la Registraduría o de firmar cláusulas de confidencialidad eliminan quitan todo sentido a las misiones electorales, ya que o impiden realizar un ejercicio de control ciudadano pleno o impiden presentar resultados y hacer críticas al proceso adelantado por la Registraduría.

Es imperativo que el Congreso revise estos artículos con cuidado y construya una propuesta que garantice sus derechos, los de los ciudadanos y elimine toda intención de la Registraduría de limitar o controlar el control participativo directo.