Observatorio de Derechos Digitales

El voto digital en Ecuador deja más dudas que certezas

Alerta No. 1
Octubre 2023

¿Qué es lo nuevo? Durante la primera vuelta de las elecciones anticipadas en Ecuador, por primera vez se ofreció el voto digital remoto como una opción para las personas que viven en el extranjero. Al mismo tiempo, las autoridades electorales promovieron el uso de la tecnología blockchain para proporcionar transparencia, visibilidad y auditabilidad de todos los resultados electorales. Sin embargo, los efectos de estas innovaciones tecnológicas no fueron los esperados.

¿Por qué es importante? Porque las fallas evidenciadas durante las elecciones del 20 de agosto de 2023 dejan entrever un serio problema de seguridad en el sistema electoral y, sobre todo, en la protección de datos personales de los y las votantes. Las votaciones telemáticas conllevan un alto riesgo en la privacidad de las personas que ejercen su derecho a elegir, ya que es posible vincular la elección efectuada con otra información recopilada en el back-end o procesamiento tras bastidores, de carácter personales.

¿Qué debe hacerse? Tiene que existir información clara y oportuna sobre cómo se toman estas decisiones y por qué. También es absolutamente necesario que la autoridad electoral trabaje en estrecha colaboración con expertos en seguridad digital antes y durante la implementación de innovaciones tecnológicas. Es importante dar un paso hacia atrás y revisar cuidadosamente la infraestructura actual para saber cómo avanzar de una manera más segura.

Durante la primera vuelta de las elecciones anticipadas en Ecuador, por primera vez se ofreció el voto digital remoto como una opción para las personas que viven en el extranjero. Al mismo tiempo, las autoridades electorales promovieron el uso de la tecnología blockchain para proporcionar transparencia, visibilidad y auditabilidad de todos los resultados electorales. Sin embargo, los efectos de estas innovaciones tecnológicas no fueron tan positivos como se esperaba.

I. Explicando el voto digital

¿Qué es el voto digital? Se puede definir como cualquier tipo de votación que depende de mecanismos digitales para que el voto ocurra. Esto puede incluir juntas receptoras digitales, escaneo digital del escrutinio o la transmisión digital de los resultados de la votación. Una elección completamente digital sería aquella en la que todas las partes del proceso ocurren de forma digital, sin el uso de registros en papel.

El voto digital remoto implica que el proceso de votación en sí sucede a través de internet, sin la necesidad de sistemas dedicados para el ingreso de los votos. Esto puede implicar que la votación se realice a través de un navegador web o que requiera la instalación de una aplicación dedicada en la computadora de la persona que desee votar.

Desde la perspectiva de la seguridad informática, el voto digital de cualquier tipo no es un asunto resuelto. En realidad, se considera uno de los desafíos más complejos en este campo. Cada vez que un país intenta implementar elecciones parcialmente electrónicas, el resultado suele ser problemático, y las y los investigadores en seguridad terminan descubriendo inevitablemente graves vulnerabilidades en el proceso. Por ejemplo, en las elecciones recientes en Brasil y Argentina.

La verdad es que hay un consenso entre expertas y expertos en seguridad digital, como comunidad: no sabemos cómo llevar a cabo la votación electrónica de ningún tipo de manera segura. Si además agregamos la problemática de llevar a cabo un proceso electoral completamente remoto, la complejidad y la dificultad aumentan de manera significativa.

II. ¿Cómo debería implementarse el voto electrónico?

Si, a pesar de todo, se desea implementar el voto electrónico de la forma en que Ecuador lo hizo, ¿cómo debería hacerse?

La verdad es que hay un consenso entre expertas y expertos en seguridad digital, como comunidad: no sabemos cómo llevar a cabo la votación electrónica de ningún tipo de manera segura

En primer lugar, se debería dedicar suficiente tiempo para llevar a cabo el trabajo para el desarrollo de esto. Como mínimo, probablemente se necesitarían 2 años, o tal vez incluso más. Luego, sería necesario encontrar un equipo para llevar a cabo esta tarea. Este debería ser un equipo multifuncional con una amplia experiencia en seguridad, criptografía y accesibilidad, pero también compuesto por expertas y expertos en el desarrollo de software. Dependiendo de las capacidades, es probable que el equipo esté conformado por al menos

20 personas. Para dejarlo claro, no existen muchas personas capaces de realizar este trabajo. Como se podría pensar, el presupuesto para este tipo de proyecto sería bastante grande.

Al considerar el grado de sensibilidad de los datos recopilados, es fundamental que tanto el código como los datos se almacenen y gestionen dentro del país. De lo contrario, no estaría claro qué leyes de protección de datos podrían infringirse y el riesgo de interferencia externa aumenta. Por esta razón, la aplicación debería ser desplegada dentro del Ecuador. Además, se debería utilizar certificados de seguridad de proveedores ecuatorianos. Obviamente, la protección de información de este tipo es extremadamente sensible. Eso significa que se requiere un enfoque multidimensional.

Al considerar el grado de sensibilidad de los datos recopilados, es fundamental que tanto el código como los datos se almacenen y gestionen dentro del país.

Existen varios puntos donde las cosas podrían salir mal. Primero, ¿qué sucede con las computadoras de los votantes, si tienen algún tipo de malware? ¿Cuál podría ser su influencia en el voto? En el caso de la elección anterior, se enviaron enlaces a los correos electrónicos de las personas que votan. Sin embargo, eso significa que cualquiera con acceso a las cuentas de correo electrónico podría obtener el enlace para votar.

Luego, una vez que los votos han sido registrados, ¿cómo se protegen y garantizan que los resultados puedan ser verificados, al mismo tiempo que se mantengan anónimos de acuerdo con los requisitos constitucionales? Para cada uno de estos problemas se deben implementar diversas medidas de seguridad. Por supuesto, las medidas no son suficientes. También se requieren sistemas de detección que puedan descubrir indicios de vulnerabilidad.

Por último, se tendrían que hacer distintos tipos de pruebas. Es probable que se necesite dedicar al menos unos 6 meses para probar un sistema así de forma adecuada. Las pruebas incluirían pruebas de rendimiento, de carga y de funcionalidad. También sería necesario incluir una prueba de seguridad. Y, para concluir, se tendrían que hacer revisiones importantes de seguridad por al menos una firma independiente de seguridad.

III. La peligrosa actuación del CNE en las elecciones del 2023.

Debe quedar claro que ninguna de estas tareas es sencilla. Lamentablemente, sabemos que nada de esto ocurrió en el Consejo Nacional Electoral, CNE. El contrato público para el desarrollo del sistema se firmó en junio de 2023. Se lo otorgó a una empresa de marketing que no tiene indicaciones públicas de trabajos previos en seguridad, criptografía o desarrollo de software. El contrato tenía un presupuesto aproximado de $700 000 y un plazo de 3 meses para completar el trabajo. El día de la votación hubo numerosos informes de fallos y reportes de personas incapaces de votar desde el extranjero. El sistema actual se construyó sobre la nube de Microsoft Azure, con datos y código almacenados en Estados Unidos y usando certificados de una

compañía en Riga. No está claro cuál ha sido el impacto en la seguridad de todos estos problemas, ya que el CNE no ha sido transparente sobre estos asuntos. En resumen, muchas cosas salieron mal en esta cuestión.

Durante las dos elecciones de 2023, el CNE también anunció ampliamente su uso de la tecnología blockchain para aumentar la transparencia y la seguridad de las votaciones. Sin embargo, al analizarlo más detenidamente, no está claro a qué se referían exactamente con estos pronunciamientos. El blockchain es un tipo de tecnología que solo es aplicable en situaciones muy específicas. Éstas incluyen la necesidad de distribuir ampliamente un conjunto completo de datos de manera que las modificaciones sean fáciles de detectar. También implica la necesidad de incentivos para que los participantes verifiquen de manera independiente la integridad del blockchain completo. Esto significa que cualquiera debería poder descargar el conjunto completo de datos y verificarlo, y que deberían recibir una compensación o incentivo de alguna manera por realizar este trabajo, ya que la verificación requiere recursos informáticos significativos.

Basándonos en información pública, no parece que en las elecciones de 2023 se haya utilizado realmente la tecnología blockchain para estos propósitos. De hecho, la única evidencia pública del uso de blockchain en el sistema es una página web donde se pueden consultar las actas y obtener cierta información. En ningún lugar se ofrece la posibilidad de descargar los datos en sí ni de verificar su integridad.

El sistema actual se construyó sobre la nube de Microsoft Azure, con datos y código almacenados en Estados Unidos y usando certificados de una compañía en Riga.

La conclusión a la que debemos llegar es que este blockchain parece servir únicamente como una base de datos privada del CNE, lo que significa que todos los posibles beneficios en términos de seguridad, verificación de integridad y transparencia se pierden por completo.

También es importante mencionar que el trabajo de integración de la tecnología blockchain con el resto de los sistemas electorales fue realizado por una pequeña empresa ecuatoriana en colaboración con una empresa más grande con sede en Chile especializada en blockchain. Al momento de escribir esto, no pudimos verificar la cantidad del contrato público utilizado para este desarrollo, pero es razonable asumir que al menos parte del presupuesto asignado por el CNE se destinó a Chile para una tecnología que no parece haber sido útil ni utilizada por nadie.

Hay muchas irregularidades en la forma en que se gestiona la administración de las elecciones en Ecuador, especialmente desde el punto de vista digital.

En resumen, la tecnología electoral es un campo complejo. Hay muchas

irregularidades en la forma en que se gestiona la administración de las elecciones en Ecuador, especialmente desde el punto de vista digital. También surgen interrogantes acerca del manejo de la adquisición de servicios digitales públicos. ¿Qué experiencia tiene el CNE en cuanto al voto digital? ¿Qué expertas o expertos han consultado? Estas preguntas deben resolverse con urgencia, a propósito de las próximas elecciones del 15 de octubre de 2023.

IV. Los derechos digitales en riesgo.

En el contexto del voto digital en Ecuador es crucial comprender cómo los datos utilizados en este proceso pueden tener un impacto significativo en la identificación de los votantes y, en consecuencia, en su privacidad y seguridad. Uno de los aspectos más críticos radica en cómo los datos recopilados pueden, de manera inadvertida, hacer que una persona sea identificable, lo que podría llevar a situaciones de discriminación y vulneración de derechos.

El voto digital implica la recopilación de datos, personales o no, además de la elección del votante. Aunque los sistemas de votación – se supone- están diseñados para mantener el anonimato de los votantes, existe un riesgo inherente de que los datos recopilados puedan ser utilizados para identificar a una persona en particular. Esto se debe a que, en algunos casos, los votantes pueden proporcionar información adicional al votar, como su ubicación geográfica o detalles demográficos. Esta situación se ahonda aún más en los procedimientos de votación telemática o electrónica, a través de los cuales existe evidente recopilación de información personal y de uso de dispositivos, a diferencia de los procesos de elección en urna.

Las votaciones telemáticas implican un alto riesgo en la privacidad de la persona. Es posible vincular la elección efectuada con otra información recopilada en el back-end o procesamiento tras bastidores, que también son datos personales. Con este tipo de vinculaciones es posible inferir otros aspectos de la vida del votante. Esto puede abrir la puerta a la discriminación o el acoso por parte de terceros que accedan indebidamente a estos datos, una guerra establecida por la simpatía de votos a través del uso de esta información a gran escala, afectando por ende la capacidad de toma de decisión de los votantes.

Uno de los aspectos más críticos radica en cómo los datos recopilados pueden, de manera inadvertida, hacer que una persona sea identificable, lo que podría llevar a situaciones de discriminación y vulneración de derechos

En ese sentido, en caso de existir una brecha respecto de esta información y facilidades de vinculación entre el voto y el votante, su uso podría ir en detrimento de la libertad política, además de la imparcialidad del proceso electoral.

Es necesario tomar en consideración que actualmente existen ya filtraciones de datos de carácter personal de contacto (particularmente correos electrónicos) que han sido utilizados con finalidades de campaña política sin el consentimiento de los usuarios. En ese sentido, tampoco podría

aseverarse que el nivel de la protección de datos personales (que bajo previsión normativa de la Ley Orgánica de Protección de Datos personales es mandatorio) sea proporcional al nivel de riesgo que conlleva este tipo de tratamientos.

Una de las medidas de seguridad fundamentales es la obturación y el cifrado de cualquier dato que pueda vincular un voto a una persona específica. Esto significa que cualquier información que pueda identificar directa o indirectamente a un votante, como nombres, números de identificación o cualquier otro dato personal, debe ser tratada de manera que sea imposible de asociar con la elección efectuada. Este enfoque de anonimización es esencial para garantizar que el voto sea verdaderamente secreto y que los votantes no puedan ser objeto de represalias o discriminación debido a sus elecciones políticas.

Además, el almacenamiento seguro de los datos de votación es un aspecto crítico de la protección de datos. Esto implica que los datos deben ser resguardados de manera que sean inaccesibles para personas no autorizadas. Esto incluye la implementación de sólidas medidas de seguridad, como el cifrado de datos tanto en reposo como en tránsito.

La prevención del acceso no autorizado es especialmente importante para proteger los datos de votación contra posibles amenazas cibernéticas. Los sistemas de votación digital deben contar con protocolos de seguridad robustos que detecten y eviten intrusiones, así como mecanismos de respuesta a incidentes para abordar cualquier amenaza de seguridad de manera oportuna y efectiva.

Otro punto importante en este escenario es el de la transparencia y la auditabilidad como pilares fundamentales en cualquier proceso electoral, ya que garantizan la confianza de los ciudadanos en la integridad y la imparcialidad del sistema. El Código de la Democracia establece en su Art. 113 que "el CNE podrá decidir el uso de métodos electrónicos o telemáticos de votación y escrutinio en forma total o parcial, para las distintas elecciones" previstas en dicha ley. En este caso, introducirá modificaciones a su reglamento de acuerdo con el desarrollo de la tecnología que aplique.

Otro punto importante en este escenario es el de la transparencia y la auditabilidad como pilares fundamentales en cualquier proceso electoral, ya que garantizan la confianza de los ciudadanos en la integridad y la imparcialidad del sistema

Por el momento, si bien se ha identificado la necesidad del uso de tecnologías, no se ha delimitado su uso ni su fiscalización en el ámbito legal. En el mismo sentido, tampoco se ha establecido, bajo previsión normativa y técnica, una garantía de voto que asegure "la seguridad y las facilidades suficientes", como señala el mismo artículo.

Por ello, la aplicación de la protección de datos por diseño y por defecto en los sistemas de votación digital es esencial para salvaguardar el proceso electoral. Esto implica que, desde la fase inicial de planificación y diseño, se

deben considerar y abordar los riesgos respecto de derechos y libertades, garantizando que las configuraciones predeterminadas sean las más protectoras para los votantes.

En fin, el proceso electoral, particularmente el telemático, así como el uso de tecnologías para veeduría y escrutinio no tienen un sustento legal claro, a excepción del mandato expreso de su uso. Si bien la novedad que implica el uso de tecnologías en las votaciones parece ser un avance, parecería que las autoridades obviaran la importancia de estructurar los cimientos adecuados para su utilización efectiva, por un lado, la garantía de seguridad de los datos, que incluye confidencialidad, acceso y trazabilidad de la información y por otro, las garantías de protección de datos, que implican minimización de su uso para la finalidad establecida, además del debido resguardo de los derechos e intereses de los votantes.

Con el apoyo de:

CAD
Centro de Autonomía Digital

Orden Conflicto Violencia
Programa de Investigación