Voto Electrónico: riesgos nuevos y sin justificación

En la madrugada del jueves pasado, la Cámara de Diputados dio media sanción al proyecto de reforma electoral que, entre otras cosas, prevé la adopción del “voto electrónico” e impone penas a ciudadanos comunes que busquen vulnerabilidades en el sistema.

Las implementaciones de sistemas similares evidenciaron vulnerabilidades, que repasaremos más abajo. Las ventajas que podría aportar, como la de impedir el robo de votos, podrían conseguirse mediante la boleta única de papel, ampliamente probada en el mundo.

El 29 de setiembre las Comisiones de asuntos Constitucionales, de Justicia y de Presupuesto y Hacienda habían emitido dictamen favorable por mayoría al texto que se aprobó en general con los votos de 152 diputados; 75 legisladores del FPV, el FIT y Proyecto Sur votaron en contra.

Más allá de las afirmaciones de corte publicitario, el sistema que promueve la normativa en consideración muestra importantes debilidades y riesgos que difícilmente puedan considerarse aceptables para asegurar la transparencia y el libre ejercicio del derecho a votar.

Durante el debate en Comisiones, convocaron a diversos expertos y especialistas; en general, los expertos en seguridad, así como abogados vinculados a temas de derechos humanos, coincidieron en los cuestionamientos al sistema que se consagra en el proyecto. Entre quienes manifestaron objeciones al voto electrónico ante los legisladores estuvieron Daniel Penazzi (UNC), Javier Smaldone, Beatriz Busaniche y Enrique Chaparro.

Fallas comprobadas

Se utilizó un sistema de boleta única electrónica en las elecciones de la Ciudad de Buenos Aires y en Salta durante el año 2015. En esos procesos se verificó una serie de errores, algunos de los cuales fueron corregidos posteriormente.

A continuación, detallamos algunos de los problemas más relevantes que se han verificado

-Se pudieron robar las credenciales necesarias para el envío de resultados; como consecuencia, alguien podría modificar los resultados haciéndose pasar por la persona autorizada para la carga. Joaquín Sorianello pudo obtener desde un sitio de Internet las claves privadas necesarias para la transmisión de los resultados desde los lugares de votación. Sorianello comunicó el problema a la empresa encargada del sistema; ésta, en lugar de solucionar y agradecer el aviso, le inició una demanda que derivó en el allanamiento del domicilio de Sorianello.

En resumen, la propia empresa reconoció que la vulnerabilidad existió, pese a las afirmaciones tajantes del … de que el sistema es inviolable.

El caso está reflejado en un artículo del J. Alex Halderman, director del Center for Computer Security and Society de la Universidad de Michigan; el texto integra el libro Real World Electronic Voting: Design, Analysis and Deployment (CRC Press), editado por Feng Hao y Peter Ryan y que estará disponible a fines de este año.

- Otro problema verificado en las elecciones bonaerenses fue el “ataque multivoto”, un error de programación detectado por investigadores independientes a partir del código fuente del sistema electoral usado en Salta y Buenos Aires. Este error posibilitaba que mediante un smartphone se grabara más de un voto por candidato en una boleta, que luego serán contabilizados de forma múltiple. Esta falla está reconocida en el informe de auditoría firmado por el profesor Righetti de Ciencias Exactas de la UBA, si bien destaca que el error fue corregido para el balotaje.

Hubo otro ingreso grave que no tuvo mucha difusión: según el pedido de allanamiento de la fiscal Silvina Rivarola, Martín Leandro Manelli ingresó al servidor donde había datos sensibles de la elección porteña, donde realizó modificaciones de información. De la información del expediente de la investigación, difundido por el portal Politica Argentina, se desprende que hubo varios accesos desde distintos IP, algunos de los cuales habrían producido modificaciones en la información técnica del sistema electoral (por ejemplo, datos de identificación de personas o establecimientos).

Durante los debates en las Comisiones de la Cámara de Diputados, el especialista Javier Smaldone demostró que un teléfono que incluya la tecnología NFC (común en los dispositivos Samsung) puede leer el contenido de un voto si se lo aproxima al chip de la boleta con el sufragio ya grabado; esto podría utilizarse para romper el secreto de voto, al posibilitar que una persona externa verifique si un elector votó por determinada opción. El vídeo con una demostración de esta técnica está en https://youtu.be/t-JbREDsh6I

¿Se pueden corregir las fallas?

En la medida que se detecta una debilidad, podría ser corregida o mitigada; sin embargo, no podría asegurarse que no se encuentren nuevas vulnerabilidades -por un lado- y el aseguramiento del secreto del voto y la integridad de los sufragios no son sencillos de asegurar. Como señalara el matemático Edsger Dijkstra, la prueba de un programa puede usarse para mostrar la presencia de errores, pero nunca para mostrar su ausencia.

La tarea de probar el sistema, detectar fallas y corregirlas, requiere de períodos de tiempo superiores a los que están en juego, puesto que se pretende adoptar el voto electrónico en las próximas elecciones nacionales.

Tratándose de un sistema tan sensible para la propia democracia, y en el que los afectados por su implementación abarcan a la totalidad de la población, la validez del mismo no puede convalidarse por la sola opinión de un grupo de expertos; como mínimo, el sistema completo (tanto hardware

como software) debería estar accesible al estudio de cualquier ciudadano, (ley de linus).

El proyecto en debate no sólo no establece mecanismos para esa validación, sino que establece penalidades para quien -de manera independiente- realice pruebas sobre los elementos del sistema. En concreto, *alguien que descubriera una falla* como hicieron Sorianello y Manelli -entre otros- *serían penados con prisión de 1 a 3 años*, según reza el artículo 139 propuesto.

Avanzando sin mirar al costado

Además de la exhibición de las vulnerabilidades constatadas en las experiencias pasadas, hubo objeciones profundas al modelo planteado por el oficialismo, convalidado por el massismo. Se pusieron en evidencia debilidades potenciales, limitaciones teóricas y restricciones prácticas.

Sin embargo, los legisladores firmantes del dictamen mayoritario no elaboraron respuestas a las objeciones planteadas.

No hubo ninguna instancia en la que se plantearan los objetivos que debería cumplir el nuevo sistema, ni se consideraron alternativas. Es más: el oficialismo planteó el tema como "a todo o nada", sin "Plan B".

En tanto, el presupuesto 2017 girado por el Ministerio de Hacienda ya contempla la implantación del sistema, por lo que prevé un costo para las elecciones legislativas de 6.175 millones de pesos, un 58% más de lo que costaron las presidenciales del año pasado.

El proyecto aprobado por diputados establece que el sistema de votación será responsabilidad del Poder Ejecutivo, quien debe presentarlo ante la Cámara Nacional Electoral 240 días antes de la elección (Art. 18 del proyecto, modificaciones sobre el art. 62 bis del Código Electoral Nacional); esto implica que el Ejecutivo debería estar presentando el sistema en Enero para que pueda usarse en las PASO. A partir de allí, la Cámara deberá definir los procedimientos de auditoría e impugnaciones, y a partir de ese momento sólo habrá 60 días para presentaciones. Pasado ese lapso, la Cámara debe resolver sobre la aprobación del sistema.

Esto significa que en menos de 3 meses -en el mejor de los casos- se deberá desarrollar un sistema que respete las pautas electorales, y además debería ser exhaustivamente probado y analizado para poder presentarse ante la Cámara. Indudablemente, para que esto sea posible el Ejecutivo ya debe tener resuelto cuál es el sistema, y ese lapso podría eventualmente destinarse a pruebas... aunque ese lapso seguiría siendo extremadamente breve.

Existen aportes valiosos sobre las características que debería cumplir un sistema de voto electrónico; los investigadores Penazzi, Montes y Wolowick plantearon una serie de requerimientos mínimos, que también fueron respaldados por la Sociedad Argentina de Informática. Esas pautas deberían aún operacionalizarse para definir las especificaciones del

sistema de votación de una manera verificable; sin embargo, y más allá de las dudas de muchos especialistas sobre la viabilidad misma, los plazos que están en juego vuelven completamente irreal la adopción de estas recomendaciones.

En Resumen

Si el proyecto es aprobado en la Cámara Alta, se habrá dispuesto la adopción de un sistema caro, con severas vulnerabilidades comprobadas, estableciendo límites a la posibilidad de que ciudadanos comunes lo sometan a prueba, que genera nuevos riesgos para el mantenimiento del secreto del voto y con pocas ventajas, la mayoría de las cuales puede alcanzarse mediante la boleta única en papel.

El apuro, la negativa a evaluar alternativas y los nuevos riesgos comprobables del sistema que se impulsa, abre graves interrogantes sobre las verdaderas intenciones que sustentan la instauración de este sistema y las consecuencias que traerá para la democracia argentina.