El eterno retorno del voto electrónico

Diego Saravia[1], Jorge Ramirez[2]
[1] Departamento de Física. Facultad de Ciencias Exactas. Universidad Nacional de Salta
[2] Departamento de Informática. Facultad de Ciencias Exactas. Universidad Nacional de Salta
[1]dsa@ututo.org, [2]jorge@dragonlibre.net

Resumen. En diferentes distritos de la Argentina se adoptaron modalidades de voto electrónico en comicios generales. Antes, ddurante y después del desarrollo de los mismos, así como en el debate legislativo sobre la posible implementación a nivel nacional, se advirtieron vulnerabilidades y otros inconvenientes que ponen en tela de juicio la pertinencia de su adopción. Aquí resumimos algunos de esos problemas y elaboramos un listado de propuesta para orientar el debate a futuro.

Palabras Clave: Voto electrónico. Requerimientos. Vulnerabilidades. Software Libre. Derechos Humanos.

1 Introducción

Desde el año 2015 se han implementado distintas variantes de voto electrónico en distintas partes del país; los casos más notables son los de la Ciudad de Buenos Aires, la provincia de Salta y la provincia de Neuquén, por la importancia de los cargos puestos en juego en esos comicios.

La adopción del voto electrónico ha seguido adelante a pesar de las objeciones fundadas presentadas por diferentes especialistas, así como los problemas registrados en todos esos comicios sin que se tomaran suficientes previsiones para evitar que volvieran a ocurrir.

Ante cada incidente, o frente a cada nueva propuesta de adopción de este sistemas, la discusión parece comenzar de nuevo, desconociendo las experiencias, los estudios y los dictámenes que se han producido desde ámbitos académicos y profesionales.

En el presente trabajo repasamos algunos de los cuestonamientos planteados, exponemos un conjunto de lineamientos generales para la posible elaboración de pautas mínimas. presentamos algunas consideraciones de carácter general y presentamos una serie de propuestas para el futuro.

2 Objeciones

Durante el desarrollo de los comicios y durante los debates impulsados desde el oficialismo en su proyecto de reforma electoral, han surgido numerosos cuestionamientos que han puesto en tela de juicio no sólo la implementación efectiva del voto electrónico sino la propia pertinencia de la adopción del mismo en el corto plazo.

Hasta ahora, el modelo adoptado ha sido el denominado “Boleta Única Electrónica”, que separa las instancias de generación o emisión del voto de las tareas de almacenamiento y escrutinio.

El siguiente listado no es exhaustivo pero ilustra con claridad el tipo de problemas señalados:

- Intrusiones remotas en el servidor de MSA, empresa a cargo de las elecciones de la Ciudad de Buenos Aires en 2015. Las intrusiones se produjeron desde antes de que se desarrollaran los comicios e incluyeron la señalización del ingreso y la edición no autorizada de información crítica[1].
- Presenta muchas características que permiten violar el secreto del voto (uso de un celular, almacenamiento subrepticio de información, transferencia de datos)[2] [3].
- El software utilizado no está disponible para el escrutinio público. Sólo las entidades que han realizado auditorías acceden a una parte de él. Por ejemplo, en las máquinas usadas en CABA y Salta -al menos- el software que se encarga de la grabación de los chips RFID no fue puesto a disposición para su estudio.
- En los comicios realizados este año en Neuquén, varios ciudadanos afirmaron que el voto generado por la máquina no coincidía con lo que habían elegido [4] [5]. Además,

Durante las exposiciones realizadas tanto ante la Cámara de Diputados como ante la Cámara de Senadores, numerosos especialistas pusieron de relieve numerosos riesgos para la adopción de este tipo de sistemas.

Por otra parte, un equipo conformado por CONICET realizó un informe[6] a partir de la solicitud del Ministerio del Interior, Obras Públicas y Vivienda, en el cual el grupo de especialistas recomendó “no avanzar en el corto ni mediano plazo con la implementación de un sistema electrónico para la etapa de emisión de voto”.

Pocas de las advertencias surgidas de las experiencias e informes mencionados fueron abordados de manera de alcanzar una solución que alcance un alto grado de

consenso entre los especialistas. Sin embargo, la implementación del voto electrónico continuó, y se siguen escuchando afirmaciones genéricas o infundadas de parte de funcionarios públicos.

3 Construcción de pautas mínimas.

El sistema electoral es esencial para la democracia; las alteraciones que sufra afectarán gravemente a la voluntad popular. Esto significa que la instauración de un sistema de este tipo afecta a la población en su conjunto, así como a las instituciones democráticas; todas ellas constituirían "stakeholders" [7] que deberían tenerse en cuenta para elaborar los requisitos.

El 2005, un artículo publicado por Patricia Pesado [8] y otros señalaba que los sistemas de votación deben considerarse como sistemas críticos, y cualquier desarrollo/adquisición/implmentación debería guiarse en base a esa caracterización. El informe de CONICET mencionado anteriormente también adopta el mismo criterio.

En 2016, Montes y otros [9] presentaron un conjunto de Consideraciones sobre el voto electrónico. Allí los autores plantean una serie de requerimientos que pueden servir como base para establecer pautas mínimas para el desarrollo y la incorporación de tecnología en el proceso electoral.

Precisamente, la rigurosidad de dicho informe debería servir de base para la discusión. Las eventuales objeciones que surgieran respecto de las conclusiones a las que arribó el equipo deberían someterse a discusión en lugar de reproducir argumentos "ad hominem" reñidos con cualquier marco epistemológico científico.

El riesgo de que la voluntad sea alterada es grave incluso en su potencialidad: no hace falta verificar si realmente ha ocurrido el aprovechamiento de alguna vulnerabilidad para poner en jaque el consenso que su legitimidad requiere, ya que la posibilidad de su manipulación por parte de sectores de la población, o la imposibilidad de ésta de controlar que el proceso se desarrolle de manera correcta, socavan uno de los soportes fundamentales del sistema democrático: la seguridad de los ciudadanos de que sus preferencias no son manipuladas ni está en juego el secreto del voto.

Es primordial recordar que el Pacto Internacional de Derechos Civiles y Políticos [10] declara que todos los ciudadanos gozarán del derecho de "votar y ser elegidos en elecciones periódicas, auténticas, realizadas por sufragio universal e igual y por voto

secreto que garantice la libre expresión de la voluntad de los electores" (Artículo 25, inciso b). Por lo tanto, un sistema que no lo garantice significa una violación a los derechos humanos

4 Consideraciones

Los sistemas de voto electrónico que se han implementado en el país suponen que todo o parte de los procesos de emisión y conteo estén mediados por dispositivos cuyo compartimiento no es inmediatamente evaluable para cualquier ciudadano.

Un ser humano no tiene incluido un lector RFID en su equipamiento biológico, ni es capaz de leer un código QR, ni puede detectar si existe información adicional en una boleta impresa. Eso significa que se requieren características adicionales a las que prescriben la Constitución y las leyes para realizar algo que debería ser una parte esencial del proceso electoral: que un votante compruebe que el voto que se guardó es idéntico al que quiere, que su emisión no puede posibilita que se adicionen informaciones que puedan comprometer el secreto del voto, que el voto emitido no sufre modificaciones, etc.

Si para realizar esas comprobaciones se requiere de una formación en particular (como los "fiscales informáticos"), o la labor está limitada por el secreto empresarial (como en el código fuente del software usado en la emisión y el conteo de votos), se estarán agregando restricciones al ejercicio efectivo del control electoral.

Una de las principales debilidades de estos sistemas son su instrumentación concreta y las particularidades de su uso en cada elección. Así, si bien se podría asumir que las máquinas no se conectan durante la votación, se ha observado casos en los cuales sin que nadie sea notificado, las autoridades o empresa, nuevo actor emergente, instrumentan medidas que rompen supuestos. En Salta en el 2015, se encontraron computadores en escuelas remotas conectados a antenas satelitales mientras la gente votaba. Consultadas las autoridades respondieron que se trataba de un "experimento"; experimento del cual no habían notificado a los partidos políticos ni electores. Véase http://www.ututo.org/evoto/evotointernet.jpg

Otro aspecto que es menester abordar es la pretensión -sostenida por empresas proveedoras de equipamiento para el voto electrónico y autoridades electorales- de adoptar la "seguridad por oscuridad". Existe abundante producción que desacredita este enfoque; un buen resumen de las creencias infundadas en las que se basa fue expuesta por Mercury y Neumann [11]. Por el contrario, la posibilidad de múltiples

análisis diferentes e independientes aportará mayor confiabilidad en el software empleado, de modo de que constituyan un mecanismo seguro.

5 Propuestas y conclusiones

A partir de las consideraciones referidas más arriba, planteamos una serie de afirmaciones para el debate, con el objetivo de ir conformando -de manera independiente de intereses partidarios o corporativos- un cuerpo de acuerdos sobre la implantación del voto electrónico:

- El desarrollo de cualquier sistema de votación, y especialmente cuando supone la incorporación de tecnología, debe considerarse como un sistema crítico.
- La verificación de cualquier instancia del proceso electoral debe ser factible para la mayor cantidad de personas posibles. Idealmente, cualquier elector debería contar con los medios para comprobar por sí mismo, sin intermediaciones, que se preservan el secreto y la integridad del voto, y que no se producen alteraciones en los cómputos de los resultados.
- Si la verificación del proceso electoral sólo puede ser realizada por un grupo de personas, la democracia está siendo limitada. El elector se ve obligado a confiar en el "experto" ya que no puede comprobar por sí mismo que no se produzcan alteraciones en el proceso. Este requerimiento se ve gravemente dificultado si un dispositivo actúa como mediador entre la voluntad del votante y el voto, y no existe la posibilidad de escrutar de manera independiente y por múltiples fuentes que no se hayan producido alteraciones.
- La verificabilidad del proceso no puede depender exclusivamente del gobierno y/o de una empresa privada. No puede asumirse *a priori* que los intereses de los mismos sean coincidentes con los de la sociedad en su conjunto.
- Completa publicidad del software usado, lo que requiere -aunque no exclusivamente- que el código fuente del mismo sea público. En ese sentido, debe requerirse que el mismo se distribuya bajo una licencia libre o de código abierto.

- Debe poder verificarse en tiempo real que el sistema no ha sufrido alteraciones y que no han quedado registros ajenos a las estrictas necesidades del propio proceso.
- Deben descartarse las opciones que buscan la “seguridad por oscuridad”, principio desacreditado en el mundo de la seguridad informática. La seguridad no debe depender del mecanismo sino de la custodia adecuada de “las llaves” que contienen el proceso.
- La incorporación de tecnología en el proceso electoral debe ser precedida por una definición de requerimientos mínimos ampliamente debatidos, de modo que la verificación de los mismos no esté sujeta a ambigüedades. La validación de los mismos debe contar con un consenso amplio, en el que la legalidad y el cumplimiento de preceptos constitucionales esté garantizado conforme a un amplio consenso.
- No debe avanzarse en el corto plazo en la adopción de dispositivos y mecanismos mediadores en la generación y emisión del voto.
- Toda propuesta de incorporación de tecnología en las distintas etapas del voto debe ser amplia y públicamente evaluada con anterioridad. En particular, deben ser comprobables sin ambigüedades las ventajas que dicha adopción traería.

Este conjunto de afirmaciones seguramente no agota el tema y puede ser sometido a discusión. Precisamente, la posibilidad de confrontar ideas, de discutir las ventajas y desventajas, de elaborar nuevos enfoques, son parte constitutiva del pensamiento científico y el mejor reaseguro para defender los intereses colectivos.

Referencias

1.Lijalad, A.: El voto hackeado: expediente muestra iregularidades en el voto electrónico en Capital Federal, http://www.politicargentina.com/notas/201608/16044-voto-caba-2015.html.
2.. Busaniche, B., Heinz, F., Aguerre, T., D’Ippolito, N., Smaldone, J., Ferreira Rubio, D.: Voto electrónico: una solución en busca de problemas. Tren en Movimiento, Buenos Aires (2017).
3....Ramirez, J.: La Máquina del Tiempo, http://dragonlibre.net/seguridad/la-maquina-del-tiempo/, (2017).

4.. Abrevaya, S.: Denuncias de irregularidades en Neuquén | Alerta por problemas con las máquinas de voto electrónico, https://www.pagina12.com.ar/179993-denuncias-de-irregularidades-en-neuquen.
5.....Fuertes, G.: El voto electrónico acumuló denuncias por irregularidades, https://www.tiempoar.com.ar/nota/neuquen-denuncian-fraude-e-irregularidades-con-las-maquinas-de-voto-electronico.
6.....Arce, I., Cristiá, M., Maldonesi, P., Melgratti, H., Uicich, G., Wolovick, N., Zavalla, E., Bergero, F.: ANÁLISIS DE FACTIBILIDAD EN LA IMPLEMENTACIÓN DE TECNOLOGÍA EN DIFERENTES ASPECTOS Y ETAPAS DEL PROCESO ELECTORAL. 54.
7. Glinz, M., Wieringa, R.J.: Guest editors' introduction: Stakeholders in requirements engineering. IEEE software. 24, 18–20 (2007).
8....Pesado, P.M., Feierherd, G.E., Pasini, A.C.: Especificación de requerimientos para sistemas de voto electrónico. In: XI Congreso Argentino de Ciencias de la Computación (2005).
9.. .Montes, M., Penazzi, D., Wolovick, N.: Consideraciones sobre el voto electrónico. In: X Simposio de Informática en el Estado (SIE 2016)-JAIIO 45 (Tres de Febrero, 2016) (2016).
10.....Naciones Unidas: ACNUDH | Pacto Internacional de Derechos Económicos, Sociales y Culturales, http://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx.
11.....Mercuri, R.T., Neumann, P.G.: Security by obscurity. Communications of the ACM. 46, 160 (2003).