VOTO ELECTRÓNICO
UNA SOLUCIÓN EN BUSCA DE PROBLEMAS

VOTO ELECTRÓNICO
UNA SOLUCIÓN EN BUSCA DE PROBLEMAS

Beatriz Busaniche
(compiladora)

edición de **Matías H. Raia**

TRENENMOVIMIENTO
Fundación Vía Libre
HEINRICH BÖLL STIFTUNG
CONO SUR

Voto electrónico : una solución en busca de problemas / Beatriz Busaniche ... [et al.]; compilado por Beatriz Busaniche ; editado por Matías Raia. - 1a ed . - Temperley : Tren en Movimiento, 2017.
160 p. ; 22 x 15 cm.

ISBN 978-987-3789-24-3

1. Difusión de Tecnologías. 2. Evaluación de la Tecnología. 3. Derecho a La Información . I. Busaniche, Beatriz II. Busaniche, Beatriz, comp. III. Raia, Matías, ed.
CDD 342.075

Este libro cuenta con el apoyo de:

HEINRICH BÖLL STIFTUNG
CONO SUR

www.cl.boell.org

Fundación Vía Libre

www.vialibre.org.ar

www.trenenmovimiento.com.ar - trenenmovimiento@gmail.com

Impreso en América Latina, en los talleres de Cooperativa de trabajo Tricao Ltda., CABA. Marzo, 2017.
Hecho el depósito que marca la ley 11.723

PRÓLOGO

Ártica y Fundación Vía Libre[1]

Actualmente, el voto electrónico forma parte de las discusiones sobre cómo las mediaciones tecnológicas pueden tener consecuencias en el nivel de los derechos humanos. En este caso, podemos considerar uno de los derechos reconocidos en el Pacto Internacional de los Derechos Civiles y Políticos, en el artículo 25, apartado b), en el que se establece que todos los ciudadanos gozarán del derecho a

> 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.

¿Cómo se dan estas garantías? Si bien las elecciones en todos los países tienen carencias y dificultades, y, además, en algunos países los problemas son de gran magnitud, las elecciones deberían ser objeto de monitoreo y control para acercarse lo más posible a las exigencias del Pacto. Por

1 Este texto forma parte de los cursos virtuales de Internet y Derechos Humanos realizados en forma conjunta por Ártica y Fundación Vía Libre.

ejemplo, mediante la participación de delegados de todos los partidos en pugna, la conformación de autoridades electorales con base ciudadana para el contralor de la elección, la participación de observadores internacionales y el despliegue de operativos de seguridad que velen por el normal desarrollo de elecciones libres y limpias.

Existen en el mundo distintos sistemas de votación, pero si un país está comprometido con los derechos políticos y la prevención del fraude, debe contar con un sistema que garantice un alto nivel de seguridad de la integridad y del secreto del voto. Cuando la ciudadanía concurre a las urnas, la comparecencia de cada persona se controla escrupulosamente verificándose su identidad, pero su voto queda completamente separado de la identidad del votante una vez que el sobre –que protege el voto de las miradas ajenas– se separa de sus manos para depositarse en la urna, donde ningún voto vale más que otro mientras sea válido.

Evidentemente, todos estos controles y garantías hacen que las elecciones supongan un enorme despliegue de recursos económicos, técnicos y humanos, necesario para que un acto tan serio y trascendente se realice en las mejores condiciones. Pese a cierta percepción presente en los medios de comunicación de que las elecciones son "lentas y anacrónicas", es cada vez más habitual que los resultados del primer escrutinio se den a conocer la misma noche de la elección y que incluso los ciudadanos puedan seguir las etapas subsiguientes por Internet.

Asimismo es cada vez más frecuente que durante las jornadas en que se celebran elecciones, se conozcan opiniones a través de los medios de comunicación que impulsan la transición hacia el voto electrónico. Se dice que el voto electrónico es más "ágil", "transparente", "sencillo" y "económico" –pero también sabemos que la prensa difunde con mayor frecuencia argumentos favorables, descuidando las voces que advierten de los riesgos de esta modalidad de votación.

Aunque parezca una novedad, el voto electrónico es una posibilidad en estudio desde hace más de cuarenta años. ¿Cuántos países en el mundo han implementado este sistema

de votación en ese lapso? Apenas un puñado, y algunos de ellos han desandado el camino, entre los que se encuentran países de economías avanzadas, como Alemania, Holanda y Reino Unido. Entre los países que están estudiando o que han implementado parcialmente el voto electrónico, se encuentra Argentina. En estos años, se está desarrollando un intenso debate al respecto.

Los integrantes de Fundación Vía Libre utilizan frecuentemente una frase ingeniosa acerca del voto electrónico: "es una solución en busca de un problema". Sin embargo, entraña múltiples problemas en sí mismo. Empecemos entonces, por reconocer y analizar estos problemas.

Problemas básicos del voto electrónico

En primer lugar, hay que señalar que el voto electrónico no es una única tecnología. Existen al menos tres modalidades básicas muy diferentes entre sí:

- Boleta única electrónica
- Urna electrónica
- Voto electrónico por Internet

A su vez, dentro de cada una de estas modalidades principales existen sistemas de voto diversos, cuyas diferencias dependen, en gran medida, de la oferta de las empresas proveedoras.

No obstante, hay tres problemas centrales del voto mediado por sistemas electrónicos de información, que son comunes a todas las modalidades de voto electrónico:

1) Los sistemas informáticos, pese a ser muy sofisticados, no son infalibles. Pueden fallar y fallan. Requieren de constantes "parches" para enfrentar problemas de funcionamiento intrínsecos o amenazas de seguridad externas. En comparación con los posibles errores y acciones fraudulentas que

afectan al voto tradicional, los riesgos del voto electrónico son mayores. En sistemas electorales de tradición democrática profunda, existen varias etapas en las que los ciudadanos pueden comprobar e impugnar errores. También existen mecanismos que hacen que la comisión de un fraude requiera de métodos muy burdos que fácilmente quedan en evidencia, mientras que la escala del fraude queda acotada físicamente (por ejemplo, adulteración de los resultados de urnas individuales). En tanto, en un sistema de voto electrónico, los errores y fraudes pueden pasar inadvertidos muy fácilmente, dado que reconocerlos requiere altos niveles de experticia técnica, mientras que la escala del fraude puede ser mayor.

2) Lo que sucede en un sistema informático no es inmediatamente accesible a la comprensión humana. Siempre nuestro acceso será mediado por otros sistemas que nos facilitan la "comunicación" con la máquina. Una urna electrónica, por ejemplo, puede contar votos y arrojarnos un resultado, pero ningún humano puede comprobar de forma directa la existencia real de esos votos.

3) Finalmente, el aspecto más importante es que el voto electrónico no puede garantizar que se cumplan los fundamentos de una votación democrática:

- *Secreto del voto.* Toda elección necesita que cada votante vote únicamente una vez y para eso debe quedar registrado que concurrió a las urnas. Pero a la vez, se debe garantizar la inviolabilidad del secreto del voto separando el registro del votante del registro del voto y dándole garantías al votante de que no es observado mientras vota. En el voto tradicional, estos dos requisitos pueden ser satisfechos sin mayores sofisticaciones. En cambio, en el voto electrónico nos encontramos con que nuestra "solución" no genera más que problemas: garantizar votos secretos pero no repetidos en el voto electrónico es algo para lo cual no hay una respuesta

teórica ni práctica. Los mecanismos utilizados se han mostrado capaces de ser vulnerados.[2]

- *Integridad.* Al ser los sistemas informáticos altamente vulnerables a errores –que pueden pasar inadvertidos– y al ser "cajas negras" de las cuales no sabemos exactamente lo que sucede en su interior,[3] resulta muy difícil garantizar que los votos no son adulterados, y por lo tanto no se puede tener la seguridad de una correcta asignación y conteo. El votante no puede estar seguro de que el voto emitido refleja su voluntad.[4] Las posibles soluciones para que pueda confirmar su voto (un comprobante impreso, por ejemplo) no son fiables y pueden comprometer el secreto del voto.

- *Fiscalización de las elecciones por parte de personas no especialistas (representantes de los partidos, la justicia y la ciudadanía).* Muchas veces se argumenta que los problemas del secreto y la integridad del voto podrían ser controlados con una muy estricta auditoría del software y el hardware utilizados para la votación. Sin embargo únicamente un reducido conjunto de técnicos, altamente especializados, es capaz de realizar tal auditoría (y aun así no pueden garantizar

---

2 Distintas universidades en el mundo han hecho experimentos en votaciones simuladas, demostrando que es posible adulterar los resultados de máquinas de votar o violar el secreto del voto. Ver, por ejemplo: "UnB quebra sigilo de urna eletrônica em testes organizados pelo TSE". UNB, 22/3/2012. En http://www.unb.br/noticias/unbagencia/unbagencia.php?id=637

3 Si bien es posible –y sería lo más sensato– utilizar siempre software libre cuyo código pudiera ser inspeccionado y verificado por cualquiera, resulta de todas formas imposible determinar que el código auditado sea efectivamente el que opera en todas las máquinas al momento de la votación, dado que pueden existir manipulaciones, ataques y virus en cualquier momento, incluso durante el transcurso del acto electoral.

4 "Voto electrónico: 'No hay tecnología confiable'. Entrevista al programador finlandés Harri Hursti". Infotechnology, 21/4/2009. En http://www.infotechnology.com/historico/Voto-electronico-No-hay-tecnologia-confiable-20090421-0003.html

completamente la validez del resultado).[5] Por lo tanto, la fiscalización de la elección por ciudadanos comunes se hace prácticamente imposible. Hay en el imaginario colectivo una idea de que esta fiscalización es una pesada obligación. Por el contrario, es un derecho. Sin el contralor ciudadano, no se pueden garantizar unas elecciones limpias y libres.

Por todos estos problemas, que serán ampliados y analizados en los próximos capítulos de este libro, es inadmisible en una democracia la utilización de urnas electrónicas que cuenten "votos virtuales". Tampoco es recomendable optar por un sistema que emita votos en papel "de respaldo", que solamente sirva para que los votantes puedan confirmar su voto y hacerlo valer cuando hay sospechas de fraude. La elección debe ser fiscalizada permanentemente, con garantías para todos los partidos, candidatos y ciudadanos y no únicamente cuando se sospecha que puede haber sido adulterada.

Lejos de ser una tecnología que avanza a paso firme y que "tarde o temprano" se implementará en todos los países, el voto electrónico ha sido adoptado lenta y cautelosamente, y en ocasiones ha sido desestimado o cancelado.

Muchos de los países que se proponen aplicarlo están desde hace años en etapa de evaluación o han realizado experiencias apenas en algunas circunscripciones y en algunas elecciones locales. En ciertos casos esta modalidad no ha superado las etapas de prueba satisfactoriamente,[6] y en otros, directamente ha sido abandonado o prohibido, como en Holanda y Alemania.[7] En los países en los que se presenta como caso de éxito, como Brasil, Venezuela y la India, se han reportado

---

5 Busaniche, Beatriz. "Voto electrónico: los riesgos de una ilusión", *La Nación*, 28/6/2011. En http://www.vialibre.org.ar/2011/08/14/voto-electronico-los-riesgos-de-una-ilusion-3/

6 Países en estudio o implementación parcial: http://www.euskadi.net/botoelek/otros_paises/ve_mundo_impl_c.htm

7 Países con voto electrónico legalmente prohibido o paralizado: http://www.euskadi.net/botoelek/otros_paises/ve_mundo_paralizado_c.htm

problemas que ponen en duda la confianza ciudadana.[8] Más información sobre la implementación y fracaso del voto electrónico en distintos países, se desarrolla en el artículo redactado por Tomás Aguerre, "Voto electrónico: un debate entre lo seguro y lo moderno", incluido en este libro.

En dichos países, además, no se ha demostrado todavía que esta modalidad mejore la participación ciudadana disminuyendo el abstencionismo o la anulación de votos.[9] Por el contrario, conlleva problemas de participación para adultos mayores y personas de bajo nivel educativo.

Además, el voto electrónico, contrariamente a lo que se cree, no garantiza que las elecciones resulten menos onerosas para el Estado[10] ya que el sistema tiene costos que antes no se tenían: compra o fabricación de las máquinas, desarrollo de software, elecciones piloto y testeos previos al día de la elección, certificación, auditorías, capacitación, soporte técnico y actualización (¿en cuántas elecciones se puede seguir usando una misma máquina?; ¿es posible usar el sistema con tranquilidad sin actualizaciones de seguridad periódicas?). Estos costos pueden incrementarse aún más, en caso de que se utilice tecnología patentada y software privativo propiedad de un proveedor privado, como se hace usualmente.

Vale la pena agregar un comentario para quienes consideran que el voto electrónico es ambientalmente más sostenible. Si bien hay sistemas de votación en los que hay múltiples boletas entre las cuales elegir, lo cual genera contaminación y derroche de papel, no debemos olvidar que los componentes electrónicos de las máquinas de votar también se descartan cuando se rompen, y a diferencia del papel, son difícilmente

---

8 Países con implementación: http://www.euskadi.net/botoelek/otros_paises/ve_mundo_impl_c.htm

9 En las elecciones nacionales de 2014 en Brasil, Dilma Rousseff ganó por 3.360.000 votos. Hubo 5.200.000 votos nulos, es decir, una incidencia del 5,8%.

10 En Brasil, el presupuesto de las últimas elecciones fue de R$ 5.920.427.796, según el Diario Oficial (En http://www.jusbrasil.com.br/diarios/59599459/cnj-26-09-2013-pg-18). El costo fue de unos USD 50 por voto.

reciclables (algunos no lo son en absoluto, siendo además muy compleja su disposición final). Frente a este problema, la solución más sencilla es cambiar la impresión de boletas de cada partido y candidatura por la impresión de una boleta única en la que los votantes señalen sus preferencias con un lápiz.

El caso del sistema de boleta única electrónica

Por supuesto, la evaluación del voto electrónico debe tener en cuenta las distintas modalidades que existen en la actualidad. Aquellos sistemas donde la emisión de votos es electrónica (urna electrónica y voto por Internet) son los más perjudiciales, dado que no ofrecen las garantías necesarias para fiscalizar el resultado de la elección. Por otra parte, existen sistemas de boleta única electrónica, que aunque parezca que conllevan un peligro menor, también presentan serios problemas.

La boleta única electrónica combina la selección del voto por medios electrónicos y el registro y conteo por medios mixtos (electrónicos y tradicionales), superando varios de los problemas de la urna electrónica.

El ciudadano confecciona su voto en una pantalla táctil ubicada en el cuarto secreto. Al finalizar, imprime una boleta que incluye los datos de su voto y, adicionalmente, un código de barras o un chip adherido, la cual finalmente deposita en una urna normal. Las boletas son contadas pasando el chip o código de barras por una máquina lectora que computa los votos, con el control visual de los delegados y fiscales de la mesa, que deben asegurarse de que el voto cargado por la máquina coincida con la información que lleva impresa la boleta. Este procedimiento vendría a acelerar la disponibilidad de los resultados y sería menos tedioso para quienes participan en el escrutinio. Además, los partidos y agrupaciones políticas se ven exonerados de la impresión y reparto de listas, eliminándose también la posibilidad del robo de boletas.

No obstante, los sistemas de boleta única electrónica presentan nuevos problemas. Entre ellos, cabe mencionar:

- La privatización de una parte importante del sistema electoral. Estos sistemas de votación son, por lo general, adjudicados por el Estado a empresas privadas. Estas empresas suelen tener en su poder las patentes de los sistemas y el copyright del software. Así, una parte importante del sistema electoral pasa a estar bajo control privado.
- Las fallas técnicas de las máquinas y otros inconvenientes en el día de la elección (cortes de luz, por ejemplo) pueden afectar el desempeño de un circuito en el que ocurra este tipo de problemas.
- Las personas adultas mayores y aquellas con menor nivel educativo tienen dificultades importantes para emitir su voto. La asistencia que se les brinda *in situ* afecta el secreto del voto.[11]
- Los chips RFID, utilizados en varios de estos sistemas, emiten señales que pueden ser interceptadas a distancia y con esto comprometer el secreto del voto.
- La garantía de que la máquina que imprime los votos no guarda información de los mismos plantea dificultades, dado que si bien el diseño de la máquina puede no incluir esta función, esta podría ser adulterada en cualquiera de los puntos que van desde su fabricación hasta el momento de la votación. Esta eventual adulteración puede pasar inadvertida con mucha facilidad.
- El sistema es más caro que el voto tradicional. Implica una inversión muy alta en el software y el hardware de las máquinas de votación, y en las boletas con chips. Ciertamente, lo que se ahorra en papel, se paga varias

11 Pomares, Julia y Zárate, Soledad. "Cambios en la forma de votar: la primera elección provincial completa de un sistema electrónico de votación. Salta, 2013", marzo 2014. Disponible en http://www.cippec.org/-/cambios-en-la-forma-de-votar-la-experiencia-del-voto-electronico-en-salta

veces en máquinas cuya capacidad de reutilización es baja debido a la obsolescencia tecnológica, a la necesidad de hacer frente a nuevas amenazas de seguridad, y a la distancia temporal entre votaciones.

- El sistema no implica ventajas ambientales demostrables. Los componentes electrónicos de las máquinas y de las boletas suponen desafíos para su gestión una vez que son desechados.
- En los sistemas donde la elección de la boleta se realiza digitando el número de lista, se considera que favorece las candidaturas mediáticas. El votante memoriza o anota el número de "su" candidato para digitarlo en el momento de votar, lo cual refuerza la importancia de candidatos personalistas (como en el caso de Brasil).
- En los sistemas donde se obtiene la boleta pasando por dos pantallas, al elegir al partido antes que al candidato, al revés que en el caso anterior, se podría estar perjudicando a candidatos. El votante no ve qué candidatos hay hasta que no elige el partido o lema.

Algunas conclusiones

Definitivamente, el voto electrónico no tiene que demostrar que "no es peor", sino que debería demostrar que es realmente mejor que los sistemas de votación existentes. En diversas áreas del proceso electoral la tecnología puede ayudar, y mucho. Pero cabe preguntarse si vale la pena incorporar la tecnología precisamente como intermediaria entre el ciudadano y su decisión. Consideramos que al menos no debe hacerse sin un detenido examen de las reales ventajas y desventajas del actual sistema de votación, en el marco del sistema electoral y de partidos en el que se pretende implementar y, obviamente, no antes de un amplio proceso de debate ciudadano informado.

Un comentario final se refiere a la interacción existente entre la tecnología utilizada para la votación, por un lado, y el

sistema electoral y el sistema de partidos, por otro lado. Toda tecnología de votación –en papel y electrónica– determina en cierta medida la forma y el alcance en que las personas ejercen su derecho democrático al voto. Cambiar la tecnología de votación es, en sí mismo, un cambio en el sistema electoral. Por lo tanto, hasta el detalle más pequeño de estas tecnologías debe ser estudiado desde un punto de vista político. Ante todo, debemos desconfiar de las soluciones estandarizadas, que difícilmente se adapten a las peculiaridades de cada sistema político. Además, es necesario prever la manera en que un eventual cambio en la dinámica electoral interactúa con las otras partes del sistema. Por ejemplo, es fundamental evaluar la medida en que un tipo de tecnología puede favorecer a determinada clase de opciones electorales, cómo puede interactuar con sistemas electorales complejos en los cuales hay muchas candidaturas y elecciones simultáneas, hasta qué punto favorece o perjudica la participación de determinados sectores sociales, etcétera.

Centrarse únicamente en los aspectos técnicos del voto electrónico, que se encuentran en la esfera de los expertos, conlleva el riesgo de obturar el necesario debate político y ciudadano que una cuestión tan importante como el derecho al voto requiere.

INTRODUCCIÓN
¿Qué es el voto electrónico?

Beatriz Busaniche y Federico Heinz

Existen varias definiciones para lo que se denomina comúnmente como "voto electrónico". En un sentido amplio, se considera voto electrónico a la incorporación de recursos informáticos en cualquier parte del proceso electoral, ya sea en el registro de ciudadanos, la confección de mapas de distrito, la logística electoral, el ejercicio del voto en sí mismo, el escrutinio y la transmisión de resultados. Sin embargo, en esta introducción, vamos a considerar estrictamente dos de las áreas del sufragio: la emisión del voto en sí misma y el recuento de votos.

En un sentido estricto denominaremos *voto electrónico* a los mecanismos diseñados para emitir y contar los sufragios en un único acto, a través de algún sistema informático instalado y en funcionamiento en el lugar mismo donde el elector concurre a expresar su voluntad política.

Entonces, entendemos por voto electrónico a todo sistema informatizado para el acto de emitir y contar los votos en la

mesa de votación, donde los ciudadanos y las ciudadanas entran en contacto directo con los dispositivos electrónicos. Consideramos el uso de computadoras, urnas electrónicas o dispositivos similares para la emisión y recuento automatizado del sufragio. Los mecanismos en los que la computadora no está directamente involucrada en el acto de emisión del voto, así como aquellos que utilizan la informática exclusivamente para la automatización del recuento y la consolidación de resultados quedan así expresamente fuera de nuestra atención.

No existe una única forma de implementar voto electrónico, más bien podríamos decir que existen tres grandes tipos de sistemas a utilizar, que difieren no solo en su implementación, sino y fundamentalmente en sus riesgos y beneficios. Los mecanismos más frecuentemente identificados se pueden agrupar en tres grandes conjuntos:

a) los sistemas de recuento automático de votos mediante reconocimiento óptico de las marcas hechas en la boleta por parte de los ciudadanos (sistemas que hacen hincapié en el escrutinio electrónico);

b) los sistemas de registro electrónico directo (RED, o DRE por su sigla en inglés) ejemplificados comúnmente con los denominados *kioscos de votación* o *urnas electrónicas*;

c) los sistemas de votación a distancia a través de Internet.[1]

Sistemas usados

a. Sistemas de recuento automático

Los primeros sistemas de esta clase datan del siglo XIX, cuando se comenzaron a implementar en la ciudad de Nueva York mediante tarjetas perforadas. Actualmente, la mayoría

1 Tula, María Inés (coord.). *Voto Electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales*, Buenos Aires, Ariel Ciencia Política - Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC), 2005.

de los sistemas de este tipo se basan en el reconocimiento óptico de marcas hechas por el votante sobre la boleta, ya sea de forma directa o a través de una máquina de marcar boletas. Entre los años 1994 y 2003, por ejemplo, Venezuela utilizó sistemas de este tipo, basados en boletas impresas en papel con un espacio rellenado por el elector y posteriormente contabilizados mediante un sistema de reconocimiento óptico de caracteres.

En principio, los sistemas de recuento automático resuelven el problema más álgido de la incorporación de tecnología al sufragio: al mantener el principio de que la voluntad del elector se expresa en un trozo de papel anónimo, desacopla el acto de emisión de voto (que debe ser inauditable) del acto de escrutinio (que debe ser auditable en todos sus detalles). De esta manera es posible construir un sistema en el cual todos los resultados en los que la informática está involucrada pueden ser auditados independientemente de los dispositivos usados y el software en sí, mediante el simple recurso de realizar un recuento manual.

Aun así, la aplicabilidad de estos mecanismos no puede tomarse en forma aislada, sino en el contexto del sistema completo del cual forman parte. Es posible realizar muchas decisiones respecto del sistema como un todo que pueden anular total o parcialmente las ventajas del mecanismo.

Un elemento que no puede faltar en la aplicación de sistemas de recuento automático es la auditoría manual de los resultados arrojados por una porción estadísticamente significativa de las máquinas usadas, seleccionadas al azar luego del acto eleccionario. De lo contrario, una programación maliciosa del software de tabulación de votos podría alterar los resultados sin ser detectada.

Estos sistemas pierden una porción importante de sus ventajas cuando la boleta no es marcada a mano por el elector. Las máquinas de marcar boletas vuelven a introducir en el sistema muchos de los problemas asociados con las máquinas de registro directo. Si bien permiten que el votante verifique que las marcas en la boleta se correspondan con sus elecciones,

suponen un doble trabajo para el votante (elegir por un lado, controlar por otro), lo que aumenta la probabilidad de que el elector no realice concienzudamente el control. Esto hace factible el mismo ataque que se puede hacer en las máquinas de RED: introducir código que intente adulterar la intención del votante, pero abandonar el intento si el votante rechaza la boleta. De esta manera se pueden secuestrar los votos de todos aquellos ciudadanos que no sean lo suficientemente cuidadosos. También se pone en riesgo el anonimato del voto, toda vez que la máquina de marcar boletas podría agregar, además de las manchas legítimas, algunas que pasen por "suciedad" pero que, en realidad, codifiquen información que permita reconstruir la secuencia de emisión de los votos.

Otro mecanismo que reduce la utilidad de estos dispositivos es el de pasar la boleta por el escáner antes de introducirla en la urna, en vez de hacerlo al abrir esta. Esto no solo aumenta los costos –requiere un escáner por mesa, mientras que de otro modo puede utilizarse el mismo escáner para varias de ellas–, sino que potencialmente permite registrar la secuencia en la que se emitieron los votos, y así reconstruir la relación de cada votante con su voto.

Una crítica común a este tipo de mecanismo señala la dificultad que presentan en el caso de elecciones complejas, en particular cuando se realiza una elección para múltiples cargos en múltiples niveles de distrito. En una elección en la cual, por ejemplo, se deba elegir concejales de la ciudad, intendente, legisladores provinciales, legisladores nacionales, gobernadores y presidente, la magnitud de la boleta dificulta al votante el marcado de todas las opciones, así como su posterior lectura detallada. Sin embargo, esto es más una crítica de las elecciones complejas que del sistema de recuento automático en sí: mientras más compleja es una elección, más difícil es votar en ella y contar los votos. La "solución" a este problema ofrecida por los sistemas RED consiste, básicamente, en barrerlo bajo la alfombra: como en ellos es imposible contar a mano los votos, disfrazan el vicio de virtud declarando que es una tarea "innecesaria".

Otra crítica común a estos mecanismos, e igualmente inmerecida, es la que objeta la facilidad con la que se puede alterar o anular un voto mediante el agregado de marcas por parte de quienes realizan el escrutinio. Si bien la factibilidad del ataque es real, es exactamente la misma que con cualquier sistema basado en papel, que a su vez es mejor que la de cualquier sistema completamente electrónico: mientras que las boletas pueden ser alteradas, esto debe ser hecho individualmente con cada boleta, y el impacto de una persona corrupta se circunscribe a las boletas bajo su custodia. En el sistema electrónico, en cambio, una única persona corrupta tiene el potencial de infectar un gran número de máquinas, comprometiendo de esa manera incluso la integridad de votos en masa, incluyendo los de mesas cuyos fiscales actúen de buena fe.

b. Sistemas de registro electrónico directo (RED)

Los sistemas RED o DRE son aquellos que más se corresponden con el imaginario popular de las "urnas electrónicas". Representan, además, el modelo preferido de la mayoría de las empresas que participan de este mercado. Las urnas electrónicas usadas en Brasil, así como en varios estados de EE. UU. o en las últimas elecciones de Venezuela pertenecen a esta clase.

Los sistemas RED se caracterizan por realizar simultáneamente el registro y la tabulación del voto mediante un dispositivo informático, operado directamente por el votante mediante un teclado, una botonera especial, o una pantalla táctil. Además, algunos sistemas de RED ofrecen ayuda para personas con algún tipo de discapacidad, por ejemplo mediante una interfaz de audio para superar las dificultades visuales. A diferencia de los sistemas de recuento automático, en los que el soporte fundamental del voto es la boleta marcada por el ciudadano, en las máquinas RED el registro se realiza directamente en la memoria del dispositivo.

Muchos proveedores de equipamiento señalan como una ventaja del sistema el hecho de que permite "independizar

del papel" a la elección. Por lo general, recomiendan no usar la opción ofrecida por algunos modelos de máquinas RED de usar impresoras similares a las que funcionan dentro de las cajas registradoras para generar una cinta de auditoría, argumentando que "desnaturaliza el voto electrónico". En todo caso, las máquinas RED no usan el papel emitido para sus resultados, sino que se basan enteramente en los registros presentes en su memoria.

Los sistemas RED pueden configurarse de tal modo que permitan al usuario corregir sus opciones y hasta votar en blanco, pero no permiten invalidar el voto ni cometer errores clásicos que resultan en la anulación del voto.

Por otro lado, estos sistemas suelen ser también los preferidos por aquellos que trabajan en las elecciones, porque son los que más trabajo ahorran: no hay boletas que custodiar, el recuento de votos es inmediato, y no hay riesgo de que un nuevo recuento de votos arroje una diferencia con el anterior. La máquina obtendrá siempre el mismo resultado independientemente de si este refleja la voluntad de aquellos que la usaron para votar o no.

En esta preferencia, se hace evidente un punto de tensión entre los intereses de los ciudadanos (que necesitan que el resultado refleje sus elecciones) y los de quienes están encargados de conducirlo (que desean terminar la tarea con la mayor rapidez y el menor esfuerzo posible, descargando tanta responsabilidad como se pueda por eventuales errores o actos de corrupción).

c. Sistemas de votación a través de Internet

También conocidos como sistemas de votación a distancia, se trata de mecanismos para emitir el sufragio desde una computadora común conectada a la red de redes, permitiendo que los sufragantes emitan su voluntad desde sus propios domicilios, desde puntos públicos de acceso, e incluso desde el extranjero. Existen variantes de estos sistemas que permiten emitir el voto no solo desde una computadora personal, sino

eventualmente también desde un teléfono celular o un sistema de televisión digital.

Uno de los desafíos más graves que enfrenta este tipo de sistemas es la identificación del votante, imprescindible para asegurar varias propiedades importantes del mecanismo, tales como evitar que alguien vote más de una vez o en nombre de otra persona, o que voten personas que no están habilitadas para hacerlo. Este problema suele resolverse mediante una clave unívoca y personal, que puede incluir elementos físicos de autenticación tales como la posesión de una tarjeta de identificación criptográfica o un generador de claves pseudoaleatorias.

Aun con los métodos de autenticación más sofisticados, no queda claro que sea posible reconciliarlos con los requerimientos de identificación exigidos por la ley, que por lo general requieren la verificación de documentos de identidad por parte de autoridades electorales. Un problema adicional asociado al de la identificación es que estos sistemas obligan a que la máquina que recibe el voto tenga conocimiento de quién lo está emitiendo. Esto ofrece un punto único de ataque para quien quiera violar el secreto del voto: basta con obtener la información almacenada en el servidor del sistema de votos para averiguar cómo votó cada persona que lo usó.

Los defensores de estos sistemas señalan que se prestan a ser usados en lugares en los que la participación en las elecciones no es obligatoria y está permitido votar por correo. El argumento es sólido, en el sentido de que es un sistema que puede ser usado en contextos en los que la experiencia muestra que el riesgo de fraude es bajo.

Es interesante señalar que hay experiencias exitosas de uso de votación a distancia en ciertos ámbitos específicos, en particular en aquellos en los que los participantes tienen un grado alto de familiaridad y acceso a recursos informáticos y está ausente la exigencia de anonimato. El proyecto *Debian*, por ejemplo, un proyecto comunitario de desarrollo de software integrado por personas de todo el mundo que no tienen oportunidad de encontrarse físicamente para votar, utiliza voto a distancia como una herramienta cotidiana, con

excelentes resultados. El sistema es robusto, justo y difícil de engañar, pero solo funciona gracias al hecho de que el voto no es secreto.

Principales problemas detectados en los sistemas de voto electrónico

Estos sistemas suelen venir de la mano de contundentes afirmaciones acerca de sus virtudes, tales como una mayor transparencia del acto electoral, la eliminación del clientelismo político, la rapidez e infalibilidad del conteo, el menor costo de cada elección, y la mayor participación ciudadana.

Lamentablemente, estas afirmaciones categóricas no vienen acompañadas de datos sólidos que las sustenten, y algunas empresas proveedoras invierten un esfuerzo nada despreciable en evitar que sean verificadas por terceras partes independientes, como fue el caso de Sequoia Systems en 2008, que intentó impedir una auditoría independiente de seguridad encomendada por el estado de Nueva Jersey argumentando que llevarla a cabo violaría los términos de uso del software que controla las urnas.

De hecho, ninguna de esas afirmaciones soporta un análisis profundo y, si bien algunas de ellas pueden ser ciertas para algunos casos particulares, la experiencia internacional demuestra que en la realidad están muy lejos de reflejar el verdadero desempeño de las urnas electrónicas. Detengámonos, entonces, en estas afirmaciones categóricas alrededor del voto electrónico.

1. La transparencia

La afirmación de que las urnas electrónicas aportan a la transparencia del comicio es, probablemente, la más aventurada. Es difícil comprender cómo un proceso opaco se haría más transparente mediante el recurso de agregar una "caja

negra". Lejos de aportar a la transparencia, la urna electrónica obstaculiza la capacidad de la mayoría de los ciudadanos de fiscalizar la elección.

Cualquier persona sabe cómo verificar, con solo mirar, que una urna está vacía o que un precinto de seguridad está intacto, y el sistema educativo apunta a garantizar que todas las personas sepan leer, escribir y contar. Pero estas habilidades son inútiles a la hora de ver qué pasa "dentro" de una urna electrónica: la inspección ocular no sirve para ver si está vacía sino que es necesario usar un programa diseñado a tal fin, que imprima un ticket que diga "sí, estoy vacía". La pregunta es: ¿Podemos creerle?

Cuando la urna imprime los resultados, los obtiene de operar sobre sus registros internos, almacenados en medios magnéticos que los fiscales no pueden leer por sus propios medios. La única "comprobación" posible de que la urna está efectivamente vacía, o de que los totales son correctos, es repetir la operación, la que previsiblemente dará siempre el mismo resultado. Aun si confiáramos en que el programa de la urna es correcto, el fiscal promedio carece de los conocimientos y las herramientas necesarios para comprobar si el programa que está instalado en la urna ha sido adulterado o no.

Incluso un fiscal con grandes conocimientos de programación y electrónica digital, provisto de herramientas especializadas, probablemente demoraría días en verificar con algún grado de confianza que la urna está efectivamente "en cero", mientras que hacerlo con el mismo grado de confianza con el que puede hacerse inspeccionando el interior de una urna de cartón es efectivamente impracticable. Se trata de un problema de la misma complejidad que la construcción de programas de computadora libres de errores, algo que el estado del arte aún no nos permite. Para peor, las acciones que debería realizar este hipotético auditor especializado son mucho más invasivas que las necesarias para adulterar el funcionamiento de la urna, de modo que, suponiendo que nos diga que la urna está "limpia", no solo no va a poder

demostrárselo a alguien que no esté similarmente especializado, sino que no tenemos manera de saber si lo que hizo, en realidad, fue verificarla o subvertirla.

Este es un problema fundamental de las urnas electrónicas: mientras la verificación de su confiabilidad dependa exclusivamente de comprobar que "funciona bien", la tarea de su fiscalización queda necesariamente en manos de una élite tecnológica, a la que el resto de la población no tiene más remedio que creerle. Para corromper la fiscalización de una elección basada en papel, es necesario contar con fiscales corruptos en un número importante de mesas, pero en el caso de las urnas electrónicas basta con sobornar o extorsionar a un grupo pequeño de personas fácilmente identificables.

Estas dificultades a menudo son desestimadas, argumentando que se pueden realizar elecciones de prueba controladas para ver cómo se comporta la urna, y señalando que estas urnas se han usado en muchos lugares sin problemas. Lamentablemente, este argumento ignora el hecho de que es muy sencillo programar la máquina de modo que no se comporte de la misma manera durante las pruebas que durante la elección, y que la experiencia demuestra que en la mayoría de las elecciones, la necesidad de actualizar el software (ya sea el mismo software de la urna o su sistema operativo) lleva a que el programa que corre durante la elección pueda no ser el mismo que se usó durante las pruebas.

Por lo demás, la afirmación de que estas urnas han sido usadas sin problemas es harto aventurada: no sabemos si hubo problemas o no, precisamente porque la opacidad del mecanismo no nos permite comprobarlo adecuadamente. Es perfectamente posible que en esas elecciones haya habido problemas masivos, sin que nadie haya podido probarlo y ese es precisamente el escenario que las urnas electrónicas facilitan. De hecho, hay elecciones como las de EE. UU. en 2004, en las que las diferencias entre las encuestas en boca de urna y los resultados finales sugieren fuertemente que las urnas dieron resultados incorrectos.

2. *El fin del clientelismo*

El clientelismo político es un problema social, económico y educativo que no se soluciona con tecnología. Para que la "compra de votos" funcione, es necesario contar con un mecanismo que permita al comprador un grado importante de confianza en que el votante efectivamente votará por el candidato al que prometió votar. En las elecciones en papel, esto puede hacerse a través del denominado "voto en cadena", mecanismo que algunos sistemas de voto electrónico hacen efectivamente imposible.

Sin embargo, pensar que el voto en cadena y el clientelismo son lo mismo es un error: el voto en cadena es solo un mecanismo para romper el secreto del voto. No es el único, y las urnas electrónicas ofrecen mecanismos alternativos potencialmente mucho más eficaces. Esto se debe a la naturaleza fundamentalmente distinta de las urnas electrónicas. Por ejemplo, mientras que las urnas normales son contenedores pasivos de información, los circuitos de la urna electrónica emiten radiación electromagnética. Experimentos realizados en Holanda demostraron que estas emisiones hacían posible detectar por quién votaba una persona desde una distancia de 25 metros, usando solo dispositivos disponibles comercialmente.

Por ejemplo, en el estado de Ohio se descubrió, dos años después de usarlas, una grave falencia en las urnas electrónicas que permite violar el secreto del voto luego de los comicios: los reportes emitidos por la urna al final del recuento permiten reconstruir el vínculo entre voto y votante. Este caso es particularmente grave, porque ilustra un aspecto a menudo ignorado del cálculo de riesgo a la hora de usar una urna electrónica: el hecho de que no conozcamos vulnerabilidades en la urna no quiere decir que no existan, ni que nadie las conozca. Alguien que estuviera en conocimiento de esta vulnerabilidad hubiera podido organizar una compra o extorsión masiva de votos que hubiera sido indetectable y requerido un esfuerzo logístico mucho menor que el voto en cadena.

3. La rapidez en el conteo

Una de las escasas ventajas promocionadas que podría ser verificable es la rapidez en el conteo. De hecho, cuando todo sale bien, los resultados pueden ser inmediatos. El problema surge cuando evaluamos el impacto potencial de las distintas cosas que pueden salir mal. Mientras que en la urna de papel, la influencia de un inconveniente es por lo general proporcional a la magnitud de este, en las urnas electrónicas un problema muy pequeño puede tener consecuencias muy graves. Esto lleva a que si los resultados de la urna electrónica no son inmediatos, por lo general no se los puede obtener nunca. Por lo general, no hay un punto medio.

El 16 de diciembre de 2007, por ejemplo, se utilizaron cuatro urnas electrónicas de la firma Altec Sociedad del Estado (Río Negro) en la localidad de Las Grutas, en Argentina. Transcurrida la jornada electoral, una de esas urnas arrojó un resultado sorprendente: 0 votos. Fue afortunado que, en este caso, las urnas hayan llevado registro en papel, porque el registro digital se había perdido completamente, pero aun así el escrutinio demoró horas, porque los votos impresos sobre una tira de papel eran mucho más difíciles de identificar que las boletas originales. La única explicación de la empresa proveedora de la urna fue que "alguien debe haber sacudido la urna".

De la misma manera, existen casos en los que una falla técnica en una urna electrónica produjo que la urna contara miles de votos en mesas en las que votaban solo cientos de personas, o el caso de Nueva Jersey, en el que los resultados fueron inmediatos, pero el total de votos emitidos no coincidía con la suma de los votos emitidos por partido. ¿Puede decirse que ese resultado es inmediato, cuando en realidad es evidentemente incorrecto?

La rapidez, sin confianza ni seguridad, no sirve para mucho en un proceso electoral. Esta es un área en la que la eficacia (hacerlo bien) debe primar por sobre la eficiencia (hacerlo rápido).

4. La economía

La idea de que usar urnas electrónicas permite economizar dinero en los comicios ha sido refutada por auditores independientes que la pusieron a prueba. En el estado de Maryland, por ejemplo, entre 2002 y 2003 se compraron 19 mil máquinas de pantalla táctil a la firma Diebold. Para poder concretar la compra, el Estado tomó un crédito de 67 millones de dólares, 44 de los cuales fueron a las arcas de la empresa en concepto de compra y mantenimiento de las urnas. Antes de incorporar estos dispositivos, Maryland usaba un sistema de escaneo óptico.

Según el informe de la organización *Save Our Votes*, publicado en febrero de 2008,[2] el cambio de tecnologías implicó un aumento promedio de 179% en el costo total por votante. En uno de los condados, el aumento fue de 866%. Por cierto, las máquinas de Diebold aún no se terminaron de pagar y ya deben ser renovadas. El estado de Maryland está considerando volver al sistema de escaneo óptico.

5. La participación ciudadana

Un tema crítico a la hora de evaluar la implementación de voto electrónico es la participación ciudadana. Nuestras democracias modernas están golpeadas por el descrédito de las clases dirigentes y la falta de confianza en los sistemas políticos. El halo de modernidad que otorga el voto electrónico parece ser la panacea para entusiasmar a los votantes y alentar la participación en los comicios.

Sin embargo, es importante destacar que la incorporación de urnas electrónicas tiene efectos claramente contrarios al objetivo de mejorar la participación ciudadana. Sin ir más

---

2 "Cost Analysis of Maryland's Electronic Voting System", febrero de 2008. Disponible en http://www.saveourvotes.org/reports/2008/08-costs-mdvotingsystem.pdf

lejos, las personas poco afines con los sistemas computacionales serán los primeros excluidos: adultos mayores o personas de escasos recursos, personas con dificultades visuales o con bajísimo nivel educativo que hoy día no requieren mayor preparación para elegir una boleta, ponerla en una urna y emitir su voluntad política, se verán enfrentados a un sistema mucho más complejo para votar.

Pero este no es el único inconveniente. Quizás el mayor problema es que aquellos que hoy auditan las elecciones en nuestro nombre (maestras de escuela, empleados públicos, fiscales de partidos políticos) se verán incapaces de auditar eficazmente un sistema de esta naturaleza. Solo personas altamente calificadas en ingeniería de software, electrónica y hardware podrán comprender el funcionamiento de estos sistemas. Incluso personal calificado en seguridad de sistemas de información se manifiesta incapaz de evaluar, validar y corroborar el funcionamiento correcto de urnas electrónicas. Estos mismos expertos difícilmente se atrevan a firmar a conciencia una certificación de seguridad de las urnas pues no existe método formal de validación que los avale.

Así, la participación real y tangible de la ciudadanía se verá reducida a la confianza ciega en un pequeño número de fiscales informáticos que, aun teniendo amplios conocimientos de la materia, no podrán certificar la validez de un resultado en el que todos los demás tendremos que confiar. Aquellos que tenemos la voluntad política de ejercer nuestro derecho a auditar nos veremos limitados por carecer de conocimientos técnicos, y tendremos que dejar la participación real a una pequeña élite de técnicos autorizados.

Si bien no existen sistemas perfectos, la diferencia de impacto es sustancial. Una mesa de votación tradicional puede registrar inconvenientes y ser anulada. El impacto sobre los resultados globales será mínimo. Sin embargo, un error mínimo en un sistema de votación electrónica puede alterar el resultado de una elección simultáneamente en un gran número de mesas.

6. Otros problemas generales

A todo esto vale agregar que, en la gran mayoría de los casos, los proveedores de urnas electrónicas son empresas privadas cuya composición accionaria deberíamos conocer en detalle antes de confiarles un proceso público y ciudadano como es la emisión del voto. ¿Cuáles serán los mecanismos para auditar a las empresas proveedoras? ¿Cómo sabremos cuáles son sus vinculaciones políticas y sus intereses en cada elección? ¿Estamos dispuestos a privatizar un proceso ciudadano como el acto de votar?

Estas preguntas surgen a la luz de escándalos ocurridos en los EE. UU. donde, por ejemplo, uno de los principales accionistas de una de las empresas proveedoras de urnas (ES&S) resultó ser un senador republicano con obvios y marcados intereses en el resultado electoral.[3]

No son pocos los inconvenientes que aparecen a la hora de evaluar la automatización de la emisión del voto. Sin embargo, es muy poco lo que se discute y ciertamente escaso el conocimiento sobre los mismos. El acto de votar es lo suficientemente importante como para que nos ocupemos de este tema, y nos preocupemos frente a incorporaciones acríticas de tecnología que, lejos de mejorar nuestras democracias, son amenazas al derecho esencial de la ciudadanía a votar en condiciones de secreto, transparencia y seguridad.

---

3 Harris, Bev. "Senator Hagel Admits Owning Voting Machine Company", Scoop (en itálicas), 31/01/2003. Disponible en: http://www.scoop.co.nz/stories/HL0301/S00166.htm

1.
nuevas aproximaciones al voto electrónico

Voto electrónico: un debate entre lo seguro y lo moderno

Tomás Aguerre

Los límites a la ingeniería constitucional están fijados caso por caso por el análisis de condiciones, es decir, por la pregunta, ¿bajo qué condiciones podrá cualquier intervención en particular, cualquier instrumento en particular, producir el efecto que se pretendía? Para mí esa es la cuestión principal.

Giovanni Sartori, 1996

Sabemos que una parte de cualquier discusión pública consiste en imponer los términos en los que se va a dar. La lucha política, después de todo, es la lucha por apropiarse de los términos valorados por la sociedad para cargarlos con el sentido propio.

La discusión sobre la posible implementación de voto electrónico en la Argentina comenzó con el intento de enmarcar ese debate en la idea de que agregarle tecnología al sistema de emisión del voto implica, necesariamente, modernizarlo.

Sin embargo, una serie de países en el mundo de los que tranquilamente podría asegurarse que van en el camino de la modernización transitaron el camino del voto electrónico (o comenzaron a hacerlo) y decidieron "volver" hacia la boleta de papel. El hecho de decir que adoptar el sistema de papel sea "volver" supone, incluso, que el camino indefectiblemente conduce hacia un páramo de voto electrónico al que, algún día, habrá que llegar.

Pero ese no es el caso en países como Alemania, Finlandia, Holanda, Australia y una larga lista que sigue con ejemplos de sistemas electorales que incorporaron tecnología o quisieron hacerlo y detectaron fallas que comprometían nada menos que la fiabilidad del resultado de la elección. En la actualidad, solo tres países usan algún sistema de voto electrónico para todo su sistema electoral nacional: Venezuela, Brasil e India.

El voto electrónico en Alemania

El caso de Alemania es uno de los más citados en la bibliografía especializada sobre el tema. El fallo del Tribunal Constitucional de marzo de 2009 declara la incompatibilidad de la Ley de Ordenamiento Federal de Aparatos Electorales del 3 de septiembre de 1975 (y sus sucesivas modificaciones) específicamente para su aplicación para la 16.° elección al parlamento alemán.[1] El sistema que utilizó el país entonces fue el de máquinas de votación que registraban y guardaban el voto en una memoria interna, para luego realizar el escrutinio en el propio aparato que imprimía los resultados finales de la mesa. El fallo es producto de una demanda interpuesta por dos particulares quienes sostuvieron, entre varias cosas, que la confiabilidad del software instalado en los aparatos electorales (provistos por la empresa holandesa Nedap) no fue controlable por el público, que el examen que realizó el Ejecutivo no fue público y que no se permitieron auditorías independientes. El código fuente del software no estuvo abierto al público y no hubo garantía técnica de que las copias del software utilizado en las máquinas fueran concordantes con los modelos testeados.

La respuesta del Ministerio del Interior alemán fue que la publicidad del acto electoral estuvo garantizada porque el público pudo controlar la impresión del resultado electoral al finalizar el acto y el observador y la junta electoral pudieron

1 Fallo del Tribunal Constitucional Alemán, 2009. Disponible en: http://www.juridicas.unam.mx/publica/librev/rev/juselec/cont/27/dcl/dcl20.pdf

cotejar los resultados. Respecto a las auditorías, el gobierno aseguró que el Instituto Federal Físico-Técnico de Alemania examinó en detalle la máquina electoral y que se realizaron controles por parte de las administraciones comunales y las juntas electorales.

La sentencia del tribunal alemán está fundada en dos principios que surgen de su Constitución:

1) el principio de la publicidad de la elección, que ordena que todos los pasos esenciales de la elección estén sujetas a control público y

2) en la utilización de aparatos electorales electrónicos, el ciudadano debe poder controlar los pasos esenciales del acto electoral y la determinación del resultado de manera fiable y sin conocimientos técnicos especiales.

La Corte no prohibió el voto electrónico sino que declaró inconstitucional el marco jurídico que no garantizó el mandato constitucional de publicidad del acto electoral. Sostuvo, entonces:

> la utilización de aparatos electorales que pueden registrar el voto electrónicamente y pueden determinar el resultado electoral de manera electrónica es, según ello, solo compatible con la ley fundamental bajo estrictas condiciones.

En cuanto al control del proceso electoral, el tribunal sostiene que, de implementarse este tipo de sistemas de emisión de voto, es recomendable el respaldo en papel para el votante. Ahora bien, el control del proceso no termina ni empieza en ese momento. La sentencia sostiene que una de las irregularidades en la implementación del voto electrónico fue que el propio Ministerio del Interior alemán

> emitió las homologaciones para las máquinas que se iban a usar. El 15 de agosto de 2005, anunció la autorización definitiva del sistema que iban a usar las computadoras fabricado por Nedap, el hardware, los módulos de storage y el software. Invocando secretos comerciales de Nedap, el ministro se negó a hacer públicos los documentos que Nedap entregó al ministerio para la fiscalización del sistema y los resultados de los testeos.

En ese sentido, el fallo asegura que

> los procedimientos para examinar el sistema y la aprobación por parte del ministerio deben ser públicos. Cualquier interés de los fabricantes en proteger su secreto comercial debe estar subordinado al principio de la democracia (…). Para que exista la posibilidad de testear el aparato de manera independiente, la publicación de los documentos y reportes del Physikalisch-Technische Bundesanstalt y del código del software de las máquinas es la única forma de fiscalizar realmente el proceso electoral.

La idea de control y auditoría es mucho más amplia que el momento de chequear el voto contra la máquina y por eso la Corte sostuvo que no es suficiente el control de las instituciones públicas. Todos los procesos que estaban previstos en el Ordenamiento Federal de Aparatos Electorales (una legislación en la que Alemania trabajó desde los años '70) resultaron insuficientes como garantía de los principios constitucionales sobre emisión del voto:

> ni una participación del público interesado en el proceso de evaluación o del permiso de aparatos electorales, ni la publicación de los informes de evaluación o caracteres de construcción (incluyendo los códigos fuente del software en el caso de aparatos electorales guiados por ordenador) contribuyen decisivamente en asegurar el nivel exigido constitucionalmente de controlabilidad y comprensión del proceso electoral (…). La participación del público necesita por ello, para lograr la exigida supervisión fiable, medidas complementarias ulteriores.

Aunque en la última enmienda a la ley federal electoral en 2013 no se eliminó la posibilidad de voto electrónico (pero sí se dejó establecido que si se hiciera debe contar con respaldo en papel), desde el fallo de la Corte no se volvieron a usar sistemas de voto electrónico en Alemania a nivel federal.

El voto electrónico en Irlanda

El caso de Irlanda permite mostrar un ejemplo de un sistema que, en la práctica, había "funcionado bien" según parámetros que se suelen utilizar para medir la efectividad del sistema (el grado de "aceptación" de quienes lo usaron, la satisfacción por la celeridad, etcétera). La primera propuesta de voto electrónico en Irlanda se realizó en 1998 y en el año 2000 se introdujo la legislación que permitió el voto electrónico. Para el 2002, Irlanda hizo las primeras pruebas piloto con el objetivo de extenderlo al resto del país: ese año, en dos elecciones consecutivas (las generales de mayo y el referéndum por el tratado de Niza de la Unión Europea) el voto electrónico alcanzó a cubrir el 18% del electorado.

Pasaron apenas unos meses para que un informe confidencial del Ministerio del Interior irlandés se filtrara a la prensa: allí se aseguraba que la integridad del proceso electoral en los lugares donde se implementó el voto electrónico no estaba garantizada. Entre otras fallas, el memorando interno que tomó estado público destacaba la posibilidad de que un software malicioso sencillo de programar pudiera generar una pantalla falsa en la máquina para hacer votar incorrectamente al elector.

A pesar de las repercusiones negativas y el manto de sospecha sobre el sistema, el gobierno irlandés avanzó con el plan de implementación de voto electrónico para las elecciones locales y europeas de 2004. Entonces creó la Comisión Independiente de Votación y Escrutinio Electrónico para que examinara el sistema propuesto.

La comisión emitió un informe en el que sostuvo que puede recomendar la utilización del sistema de voto electrónico pero que, así como estaba reglamentado, no podía garantizar la seguridad del voto y la rigurosidad del escrutinio.[2]

---

2 El informe "Secrecy, Accuracy and Testing of the Chosen Electronic Voting System" de la Commission on Electronic Voting de Irlanda está disponible en: http://www.umic.pt/images/stories/publicacoes1/Part%200%20Index.pdf

Para cumplir con ese requisito democrático, los especialistas realizaron una serie de consideraciones que debía tener un nuevo proyecto de implementación del voto electrónico: que tuviera en cuenta las potenciales fallas en el software, la seguridad física e informática de la transmisión de los datos, la cantidad insuficiente de auditorías y testeos independientes, entre otras.

El gobierno no dio marcha atrás con el sistema pero lo puso en suspenso: aun con las máquinas adquiridas y las pruebas piloto hechas, en 2004 se votó con el sistema de papel. La inversión que hizo Irlanda en el sistema fue uno de los argumentos principales de las autoridades para no descartar de plano la posibilidad de seguir usando el voto electrónico: a las 52 millones de libras iniciales que se le pagaron a Nedap, se agregaban ahora los costos de mantenimiento y de actualización del sistema (que la ONG irlandesa ICTE calculaba en 700.000 euros anuales y 20.000.000 por única vez,[3] respectivamente).

Finalmente, el 23 de abril de 2009 el entonces ministro John Gormley anunció que quedaba descartado el sistema de voto electrónico, en base al alto costo de mantenimiento y actualización y la insatisfacción y sospechas que generó entre los electores.

El voto electrónico en Holanda

El 16 de mayo de 2008, apenas un año antes que en el caso irlandés, el gobierno de Holanda había tomado la misma decisión: abandonar el sistema de voto electrónico que había comprado a una empresa local, Nedap. La decisión se tomó luego de que, en 2008, un juez consideró que el sistema presentaba irregularidades que lo volvían directamente ilegal.

---

3 Informe disponible en http://www.stdlib.net/~colmmacc/e-voting-ireland.pdf

El sistema venía previamente cuestionado: en 2007, la comisión creada para analizar la seguridad y fiabilidad del voto electrónico en el país emitió el informe "Voting with confidence" donde se estableció, entre otras consideraciones, que

> el voto con boleta de papel en centros de votación (NdA: se analizaba también la posibilidad de voto remoto) es la opción preferida en términos de transparencia y verificabilidad. En la práctica, sin embargo, hubo algunos problemas con el recuento de votos de papel; un método de voto electrónico en centros de votación que le otorgue un respaldo en papel al votante es más seguro y posible de realizar; en ese caso, las máquinas deben estar protegidas contra la radiación allí donde sea factible y económicamente posible.[4]

La cara visible de la batalla contra el voto electrónico en Holanda fue la de un grupo de activistas informáticos denominado "We don´t trust voting computers", quienes, además de presentaciones judiciales, realizaron una demostración pública en un programa de televisión de las múltiples formas en las que se podía acceder y tomar el control de las máquinas Nedap sin demasiado esfuerzo. En menos de cinco minutos, lograron correr su propio software en una máquina de la empresa y repartir votos de acuerdo a sus preferencias, engañando al elector que utilizaba la máquina.

Tras los múltiples informes que demostraron las vulnerabilidades del sistema, la Secretaría de Estado Interior anunció que la regulación que había aprobado el voto electrónico en 1997 quedaba en suspenso hasta introducir las modificaciones necesarias para garantizar su seguridad. Hasta el día de hoy, Holanda mantiene el sistema de voto por medio de boleta de papel.

---

4 Informe disponible en http://www.cs.ru.nl/B.Jacobs/PAPERS/VotingSummaryConclusionsRecommendations.pdf

El voto electrónico en Finlandia

El recorrido de Finlandia fue similar: en 2006 aprobó una ley que permitía la prueba piloto con voto electrónico para las elecciones municipales de 2008 en algunos distritos. La prueba piloto arrojó alrededor de 200 incidentes con votantes que tuvieron problemas para dejar registrado su voto. A partir de esos inconvenientes, votantes de tres municipios elevaron quejas sobre la ley electoral que aprobó la prueba piloto. En la primera instancia, la Corte Administrativa de Helsinki sostuvo que las elecciones fueron ilegales y, luego, la Suprema Corte anuló las elecciones en esos tres municipios, que debieron repetirlas en septiembre de 2009.

En 2010 Finlandia puso en suspenso el sistema. Los cuestionamientos fueron los mismos que en el resto de los países: problemas de implementación, bajas capacidades del sistema de ser auditado y el riesgo potencial pero cierto de que el software fuera intervenido y los resultados manipulados, según relató la propia auditoría del Ministerio de Justicia.[5]

El voto electrónico en Polonia

Polonia, así como Australia, se presenta como un caso en donde el voto electrónico ni siquiera pasó la instancia de la formación de comisión y debates para su estudio. Polonia lo puso en debate como una posible herramienta para abordar dos cuestiones: los bajos niveles de participación electoral y los votantes polacos en el extranjero. Pero las propuestas siempre quedaron más en el orden de lo discursivo que en lo legislativo.

Las primeras expresiones fueron más bien contrarias por parte de las autoridades electorales. Wojciech Łączkowski,

---

5 La ONG Electronic Frontier Finland publicó algunos de los resultados de esa auditoría, disponibles en https://effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf

director de la Comisión Electoral Nacional entre el 94 y el 97, sostuvo que

> el acercamiento al uso de tecnología que ayude al escrutinio debe hacerse con mucho cuidado, haciendo énfasis en que si bien el uso de la técnica es indispensable en tiempos modernos, traslada la responsabilidad de la *accountability* de las personas a las máquinas, las computadoras y los operadores.

Su sucesor del 98 al 2010, Rymarz Ferdinand, se expresó en el mismo sentido, apuntando a la necesidad de discutir el tema con especialistas.

La Comisión Nacional Electoral organizó entonces una serie de conferencias, incluyendo una Conferencia Internacional de Voto Electrónico (Varsovia, 14-16 de junio de 2000) a partir de la cual salieron análisis sobre la posibilidad de instaurar ese sistema en el país, evaluando fortalezas y debilidades.[6] Los ciclos de conferencias continuaron y la última se realizó en 2013 donde se expusieron algunas de las conclusiones sobre el estado de la situación y una serie de principios para un posible avance:

–el *e-voting* y el usos de máquinas de votación se ha discutido ampliamente durante las últimas décadas pero el uso de tecnologías de la información en los procesos electorales es un tema mucho más amplio: en la actualidad, el trabajo de organización electoral es inconcebible sin la informatización de los sistemas en distintos niveles del proceso (delimitación de distritos, planificación financiera, confección de padrones, etcétera). En cuanto a la utilización de tecnologías en el sistema de emisión del voto, se presentan preguntas sobre los métodos de implementación y las formas de contratación y adquisición de los sistemas;

---

6 Conclusiones finales de la conferencia disponibles en: http://www.aceeeo.org/en/events/22nd-annual-conference-warsaw-poland

–a la hora de implementar tecnologías de la información y de la comunicación en el proceso electoral es vital construir las medidas de seguridad en los sistemas para garantizar la integridad del proceso y evitar la posibilidad de manipulación de información con fines maliciosos;

–cuando los organismos adquieren sistemas de TICs y equipos es fundamental que los procedimientos de contratación sean competitivos y abiertos para garantizar la transparencia y asegurar que los sistemas cumplen con el objetivo de mejorar el proceso electoral;

–cuando se considera el potencial de los sistemas de votación, los organismos electorales deben involucrar en la planificación a todos los actores para asegurar que hay suficiente aceptación pública de la incorporación de tecnología en el sistema de votación;

–un elemento clave para la introducción de sistemas de voto electrónico es tener suficientes instancias de testeo independientes, certificaciones y auditorías que garanticen una total transparencia del sistema.

Más allá de las declaraciones y las diversas publicaciones, no se presentó ninguna iniciativa específica tendiente a modificar la legislación electoral para la introducción de alguna forma de voto electrónico. Al día de hoy Polonia sigue utilizando el sistema de boleta de papel.

Para las elecciones locales de 2014, se contrató con poca anticipación un sistema informático para el momento del escrutinio. Al finalizar las elecciones se registraron problemas en algunas circunscripciones en donde falló el sistema y hubo que contar los votos a mano, lo que derivó en una semana de incertidumbres y marchas en las calles que puso en duda la legitimidad del sistema.

El voto electrónico en Australia

En el caso de Australia, se puso en estudio el tema luego de las elecciones de 2013, cuando una pérdida masiva de boletas arrojó dudas sobre la fiabilidad del sistema electoral de boleta única de papel. Por entonces el gobierno australiano encargó a una comisión del Congreso que estudie la posibilidad de introducir tecnología en el sistema de votación y almacenamiento.

El informe de la comisión sostuvo, entre varias cosas, que "incluso los más ardientes defensores [del voto electrónico] deben reconocer que en términos logísticos sería imposible para nuestras autoridades electorales implementarlo para las próximas elecciones que son en menos de dos años". Luego de escuchar a expertos y examinar casos internacionales, la comisión concluyó que "es claro para nosotros que Australia no está en posición de introducir ningún sistema de voto electrónico a gran escala sin comprometer catastróficamente la integridad del sistema electoral".[7]

Respecto a las diversas modalidades de voto electrónico, la comisión australiana aseguró que

> las máquinas son vulnerables al hackeo en algún nivel. Eso puede ser mitigado por un sistema que no solo grabe el voto electrónicamente sino que también imprima un respaldo físico para el recuento posterior. En otras palabras, demasiados gastos para igual tener que acercarse al centro de votación y aun así votar a través de una máquina en vez de una boleta de papel.

El reporte concluyó que "independientemente de las posturas filosóficas sobre el voto electrónico no es posible introducir el sistema en el corto plazo sin enormes costos e inaceptables riesgos para la seguridad".

En 2015, Australia volvió al sistema de boleta única de papel.

---

7 El informe del Congreso australiano está disponible en: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2013_General_Election/Second_Interim_Report

El voto electrónico en Estonia

Incluso en países donde algún tipo de sistema de voto electrónico funciona, los problemas de vulnerabilidad y fiabilidad del sistema son parte de la discusión. En las elecciones municipales del 2005, Estonia se convirtió en el primer país del mundo en probar el voto por Internet desde un lugar remoto, es decir, sin tener que acercarse hasta una mesa de votación, luego de un debate legislativo que comenzó en 2002.

El sistema permite optativamente votar por Internet desde un lugar remoto (la instancia de acercarse al centro de votación sigue vigente y es, de hecho, la que más se utiliza); la identificación se hace a través del documento nacional de identidad que es una tarjeta inteligente; el voto por Internet es previo al día de la votación y se puede modificar considerándose el último voto como el válido (algo que definió la Corte, tras una serie de presentaciones que hacían referencia a las ventajas que tenía un votante que podía cambiar su voto respecto a uno que no).

En 2005, casi el 2% utilizó el mecanismo de voto por Internet y fue creciendo en las sucesivas elecciones hasta llegar al 30% de la población eligiendo ese sistema en 2015. En el medio hubo discusiones sobre los riesgos en la implementación y en la ejecución. En el 2011 el Center Party y candidatos independientes presentaron una queja por fallas en el sistema que se resolvió de una manera bastante peculiar.

El código electoral de Estonia prevé que las quejas sobre el proceso electoral se pueden presentar hasta tres días después del día de las elecciones. Como la queja se presentó sobre el voto por internet desde accesos remotos (que se hace antes) y no por el sistema de votación del día de la elección solo se tomó como válida la presentación de un estudiante universitario y no la de los partidos, que presentaron en el término de tres días pero posteriores al día de la elección. La queja del estudiante –que pedía suspender los resultados de la elección– fue rechazada ya que la Comisión Nacional Electoral del país aduciendo que los mecanismos para garantizar que

no habían ocurrido manipulaciones funcionaron, sin aclarar cuáles habían sido esos mecanismos. La presentación se elevó hasta la Corte Suprema que rechazó la queja rápidamente considerando que un votante solo puede presentar un recurso de queja cuando sus derechos propios fueron violados.

En base al informe de la Organization for Security and Cooperation in Europe/Office for Democratic Institutions and Human Rights (OSCE/ODIHR), la especialista en seguridad informática, Barbara Simons, sacó las siguientes conclusiones sobre el proceso electoral de 2011 en Estonia: el sistema de emisión del voto tiene numerosos problemas críticos; el secreto del voto es vulnerable; los dispositivos de los votantes son vulnerables; los servidores son vulnerables al ataque de cualquiera; el sistema no es abierto ni transparente y no hubo ninguna evaluación de seguridad por parte de técnicos en seguridad informática independientes.[8]

Las pocas garantías que ofrece sobre el carácter secreto del voto es una de las principales críticas que recibe el sistema de Estonia. En su análisis sobre las elecciones de 2011, el especialista Sven Heiberg establece que:

> la única garantía posible de que el voto sea verdaderamente anónimo sería en presencia de, por lo menos, dos oficiales electorales, auditores y posibles observadores. Todos los procedimientos están previamente definidos y escritos pero incluso sin violar ninguno de esos procedimientos, el dueño del sistema puede manipular el resultado de la elección a gran escala sin ser detectado.[9]

En el 2014, el gobierno creó una comisión de investigadores independientes que realizó un informe muy crítico con el sistema. La comisión analizó el sistema que se utilizó en 2013,

---

8 El informe está disponible en http://www.osce.org/odihr/77557?download=true

9 El análisis es parte del trabajo "The Application of I-voting for Estonian Parliamentary Elections of 2011", disponible en http://research.cyber.ee/~jan/publ/evote2011.pdf

la documentación del sistema, el código fuente, el software y realizó experimentos en un laboratorio de recreación de voto por Internet.[10] Según la comisión,

> el sistema tiene varios problemas de seguridad: usa una arquitectura de seguridad que pudo haber sido adecuada cuando el sistema se introdujo hace una década pero que hoy está peligrosamente desactualizada. Desde que se diseñó el sistema, los ciberataques se volvieron una amenaza real y concreta. El sistema delega una extrema confianza en los servidores y las computadoras personales, el lugar más vulnerable para un ataque. El informe demuestra múltiples maneras en las cuales se puede modificar votos ya emitidos, comprometer el secreto del voto, interrumpir el proceso electoral o sembrar dudas sobre la legitimidad del resultado.

Los expertos consideraron que se debía suspender la aplicación de esta forma de votación, pero las quejas fueron rechazadas por el Comité de Voto por Internet del país.

En 2015, Estonia celebró sus elecciones con el sistema de voto por Internet.

El voto electrónico en Estados Unidos

En Estados Unidos existe una serie de variantes de sistemas de emisión del voto, no solo de Estado a Estado si no de condado a condado. Un trabajo de tres organizaciones independientes (The Verified Voting Foundation, The Constitutional Litigation Clinic at Rutgers School of Law y The Common Cause Education Fund) revisó los sistemas y el funcionamiento de los sistemas en las elecciones de 2012, a partir de parámetros e indicadores construidos en

10 El informe se encuentra disponible en https://estoniaevoting.org/findings/summary/

elecciones anteriores por el Brennan Center.[11] En el análisis se hace fuerte hincapié en una idea que en el debate argentino quiso instalarse como rectora: que la seguridad del voto electrónico estaba garantizada por el respaldo de papel que emiten las máquinas.

El informe de estas tres organizaciones divide los sistemas de votación que se usan en Estados Unidos en dos tipos: los sistemas de boleta de papel en los que el elector marca su voto (ya sea de forma manual o con un asistente tecnológico, el lápiz óptico) y los sistemas de voto electrónico, tengan o no tengan un respaldo en papel. En consonancia con los fallos e informes de otros países, el trabajo adhiere a la noción de que la impresión del voto cuando se procesa a través de un dispositivo tecnológico no modifica el carácter electrónico del voto.

Tras analizar la implementación de los sistemas en todo el país, los autores se manifiestan abiertamente en favor del sistema de boleta de papel por sobre cualquiera de los dos tipos de voto electrónico (el que imprime y el que no imprime un respaldo en papel). Dice el informe: "los autores creen que la boleta de papel y los sistemas ópticos de escrutinio, acompañados por sistemas de marcado de boletas accesibles para cualquiera, deben reemplazar a los sistemas de voto electrónico, con o sin respaldo de papel".

Entre otras cosas, el informe lista una serie de fallas que ocurrieron en elecciones anteriores en sistemas que presentaban boleta de papel de respaldo y sistemas que no: principalmente, se hace referencia a "problemas de calibrado" en las máquinas, es decir, una mala configuración inicial de las máquinas que produjo retrasos en los centros de votación. Para esos casos, el sistema de respaldo de papel provocó dos escenarios: o el votante olvidó de contrastar su voto y registró un voto equivocado o lo contrastó, dio aviso a las autoridades y se frenó el proceso electoral para que se vuelvan a calibrar

11 El trabajo está disponible en http://countingvotes.org/sites/default/files/CountingVotes2012_Final_August2012.pdf

las máquinas. Cualquiera de ambos escenarios representa un perjuicio que el sistema de papel no tiene: en el primer caso, el votante con papel está chequeando su voto en el momento en que lo elige (no hay necesidad de doble instancia); en el segundo, con máquinas caídas y la necesidad de compartirlas entre todas las mesas, no solo para votar sino para escrutar, se termina con el único beneficio que el voto electrónico presenta frente al sistema de papel referido a la celeridad.

Sobre la posible "modernización" del sistema electoral argentino

Los casos analizados nos permiten extraer algunas enseñanzas y desafíos de cara al futuro para tratar temas vinculados a la "modernización" del sistema electoral argentino:

1) todos los procesos de implementación de tecnología se hicieron con amplios debates de reforma legislativa y posteriores pruebas piloto en circunscripciones pequeñas;

2) en todos los casos, se crearon comisiones evaluadoras antes y después de la implementación, conformadas por especialistas en la materia. De allí surgen referencias explícitas a las vulnerabilidades de los sistemas y a la necesidad de crear marcos regulatorios que no deleguen decisiones en las empresas;

3) un dato relevante surge de la cuestión del respaldo en papel: el proyecto del gobierno argentino "resuelve" la cuestión de la seguridad informática asegurando que la impresión de la boleta termina con cualquier riesgo. Sin embargo, países como Holanda, Alemania o Australia, aun advertidos de esta posibilidad, consideraron mejor volver o seguir con la boleta de papel. Eso demuestra que los problemas de vulnerabilidad no empiezan ni terminan en el momento de emitir el voto. El caso norteamericano es el más claro al respecto: el respaldo en papel no es un santo grial que permite terminar con las vulnerabilidades sino apenas

el emparche a un sistema riesgoso que, a su vez, necesita de más resguardos. Sostener que "modernizar" el sistema de emisión del voto significa ir hacia un sistema emparchado resulta, cuanto menos, paradójico.

4) los controles y las auditorías fallaron en muchos países por el mismo motivo: el momento en que se pone en disputa el derecho de la empresa proveedora a resguardar su secreto comercial frente al derecho ciudadano a fiscalizar el sistema es un problema que aún no encontró solución;

5) la cuestión de los costos es uno de los principales motivos de debate en el mundo (no solo por la implementación sino por actualización y mantenimiento) y el proyecto argentino no tiene siquiera un estimativo acerca de cuáles serían esos costos para su implementación en todo el territorio.

El voto electrónico, está demostrado, introduce riesgos en la seguridad del voto y la vulnerabilidad del sistema, dos cuestiones que, a largo plazo, pueden generar el peor de los efectos: la desconfianza del electorado en un sistema al que solo pueden auditar por terceros. Es cierto, como se dice, que "todos los sistemas son vulnerables", incluso los de papel en todas sus modalidades. Sin embargo, la diferencia en la seguridad del voto electrónico y el de papel radica en que el primero abre la puerta a un tipo de vulnerabilidad que, entre otros problemas, es capaz de manipular el sistema sin dejar rastros. La diferencia es cualitativa y uno de los fundamentos por los cuales muchos países del mundo encontraron que entre garantizar la seguridad del voto y tener un sistema superficialmente "más moderno" conviene resguardar el principio básico que sostiene el sistema democrático: la transparencia y seguridad de lo que decide la voluntad de los ciudadanos.

El voto electrónico no es la solución[1]

Delia Ferreira Rubio

El ciclo electoral 2015, en nuestro país, ha dejado al descubierto falencias que han generado la desconfianza de la ciudadanía. El punto culminante fue el proceso electoral en Tucumán con su carga de clientelismo, violencia y trampas.[2] Ante este lamentable espectáculo surge el clamor por la adopción del sistema de voto electrónico, cuya tarjeta de presentación destaca la experiencia de la Ciudad de Buenos Aires.

Cada problema reclama una solución y no se ha inventado aún la máquina que resuelva todos los flancos débiles de

1 Una versión diferente de este artículo fue publicada originalmente en Digital Rights, 27/10/15, http://www.digitalrightslac.net/es/el-voto-electronico-no-es-la-solucion/

2 La autora se refiere a las irregularidades acontecidas en las elecciones a gobernador en la provincia de Tucumán durante agosto de 2015. Más información puede leerse en http://www.lanacion.com.ar/1821620-elecciones-tucuman

un sistema electoral como el argentino.[3] El clientelismo, el abuso de recursos públicos con fines proselitistas, la violencia contra las autoridades de mesa, la quema de urnas, el negocio de los fiscales de un partido que se dejan comprar para no cumplir su función, la entrega fraudulenta de documentos argentinos a ciudadanos de otros países, la manipulación del padrón electoral, la manipulación en la carga de datos del escrutinio provisorio, todo esto puede seguir pasando aunque se instrumente un sistema de voto electrónico.

La implementación de cualquier sistema de voto electrónico abre –además– nuevas ventanas de oportunidad para los "vivos" de siempre. En la Ciudad de Buenos Aires, por ejemplo, un grupo de especialistas en seguridad informática detectó problemas que la auditoría encargada por el Tribunal Superior había pasado por alto.[4] Llamativamente la reacción fue la persecución de quienes habían detectado las fallas.[5] La trasmisión de información a través de Internet puede ser objeto de interferencias indeseadas. La utilización de códigos y otras formas de información cifrada suma un espacio de opacidad. Una línea de programa en un software puede modificar los resultados, tal como se demostró en algunos estados de Estados Unidos[6] y también en el caso del sistema utilizado en Capital Federal.

---

3 El problema del robo de boletas se corrige con la boleta única, en la que constan todos los candidatos. El sistema de boleta única en papel implementado en Santa Fe (https://www.santafe.gov.ar/index.php/web/content/view/full/195312/(subtema)/195309) y Córdoba (http://www.justiciacordoba.gob.ar/bus/) ha funcionado bien y es más económico que el sistema de voto electrónico implementado en la Ciudad de Buenos Aires (https://eleccionesciudad.gob.ar/simulador/) o en Salta (http://simulador.electoralsalta.gob.ar/).

4 Más información al respecto en https://blog.smaldone.com.ar/2015/07/15/el-sistema-oculto-en-las-maquinas-de-vot-ar/

5 Bogado, David y Danny O'Brien,"Buenos Aires censors and raids the technologists fixing its flawed e-voting system", 15/07/2015, https://www.eff.org/es/node/86903

6 Véase el documental *Hacking democracy* (2006). Más información en http://www.hackingdemocracy.com/

La adopción de sistemas de voto electrónico –en cualquiera de sus variantes incluida la llamada "boleta única electrónica"– debe ser analizada con detenimiento no solo pensando en los problemas que supuestamente soluciona, sino en los que puede generar.

Moderno y rápido parecen ser los nuevos valores democráticos. Pero aun admitiendo que lo fueran, no se pueden dejar de lado otros valores prioritarios para la calidad de la democracia electoral:

-Moderno y rápido pero sin garantía del secreto del voto resulta una mala combinación. Venezuela y su sistema de voto electrónico es una buena prueba de ello.[7]

-Moderno y rápido pero no transparente tampoco contribuye a la legitimidad de las elecciones. El abandono del voto electrónico por decisión del Tribunal Constitucional Alemán[8] lo dejó bien claro.

-Moderno y rápido pero no auditable no contribuye a la integridad de las elecciones. Los estándares internacionales en la materia son unánimes en el sentido de que se debe permitir la auditoría profesional y política de todo el sistema.

-Moderno y rápido pero privatizado pone en riesgo de dependencia la operación fundante de la legitimidad democrática.

Por otro lado, el reciente escándalo de Volkswagen puso de relieve que la sola utilización de la electrónica no garantiza el cumplimiento de los parámetros normativos. La alteración del software hizo que millones de automóviles entraran al mercado violando los estándares de seguridad ambiental.[9]

---

7 Delgado, Antonio María, "Maduro admite que el voto no es secreto en Venezuela", 18/05/2013, El Nuevo Herald, http://www.elnuevoherald.com/noticias/mundo/america-latina/venezuela-es/article2023161.html

8 "Alemania: urnas electrónicas anticonstitucionales", 06/03/2009, http://www.vialibre.org.ar/2009/03/06/alemania-urnas-electronicas-anticonstitucionales/

9 "Dirty secrets. Volkswagen's falsification of pollution tests opens door to a very different car industry", 26/09/2015, The Economist, http://www.economist.com/news/leaders/21666226-volkswagens-falsification-pollution-tests-opens-door-very-different-car

Sucedió a lo largo de varios años y no hizo falta mucha gente para concretar la maniobra. ¿Podría pasar con los sistemas de voto electrónico? No cabe duda.

Así, el otro interrogante que surge es ¿cuentan con capacidad técnica suficiente los organismos electorales argentinos para controlar eficientemente el sistema? No, y en los distritos que han implementado el voto electrónico lo que se ha visto es la creciente privatización de las etapas del proceso electoral y la tercerización de los controles en entidades académicas que no han visto o no han querido ver las falencias del sistema. Tampoco los partidos políticos están en condiciones de defender eficientemente sus derechos. En algunos casos ni siquiera se les proporciona acceso a la información necesaria. La fiscalización de un sistema de voto electrónico no se satisface con la "presencia de un fiscal informático" viendo cómo se encienden las máquinas. En los sistemas de voto electrónico, la manipulación es menos visible y puede llevarse a cabo con la intervención y conocimiento de muy pocas personas.

Es muy probable que Argentina se enfrasque –en los próximos años– en la modificación del sistema electoral a nivel nacional. Para que la eventual reforma contribuya a mejorar la calidad y confiabilidad del sistema debería abarcar no solo el análisis del instrumento de emisión del voto –la boleta–, sino los otros elementos del proceso electoral desde la emisión de los documentos y la elaboración del padrón hasta el escrutinio definitivo. Especial atención debe ponerse en el escrutinio provisorio hoy bajo la responsabilidad del gobierno de turno quien lo terceriza en una empresa privada. Este escrutinio que es el que concentra la atención de la ciudadanía no tiene valor jurídico, pero tiene una gran importancia política.

Si solo se concentra la atención en la forma de emisión del voto, me temo que los problemas más serios de la democracia argentina seguirán sin cambio. Sería lamentable perder una vez más la ocasión de sumar transparencia y legitimidad. Sin embargo, podemos enfrentarnos a ese escenario de discusión reducida a voto electrónico sí o no. En tal caso, a mi

juicio, el debate debería girar en torno a una serie de garantías mínimas.[10]

En primer lugar, la discusión debe ser seria y no basada en falsos relatos. En la Ciudad de Buenos Aires, por ejemplo, la ley es clara al exigir que la adopción del voto electrónico pase por la Legislatura. No se hizo así. A lo que es sin duda un sistema de voto electrónico se le cambió el nombre y así se eludió la ley. La maniobra fue apañada por la Justicia con la honrosa excepción del entonces presidente del Tribunal Superior.[11]

Cualquier sistema de voto electrónico que se pretenda imponer debe garantizar efectivamente el secreto del voto. Esa garantía debe ser real a los ojos de cualquier elector, y efectiva desde el punto de vista tecnológico. Se debe evitar que, so pretexto de facilitar la emisión del voto, el acto de marcar la preferencia personal se transforme en una romería con electores frente a la máquina, acompañados de supuestos familiares, amigos, o auxiliares.

Se debe evitar la privatización del proceso electoral. La dependencia técnica de los organismos de control representa un grave riesgo para la limpieza de los comicios y la legitimidad de los electos. Los organismos de control electoral deben contar con la capacidad técnica y los recursos económicos necesarios para ejercer su función con plena independencia.

El sistema debe garantizar la más amplia auditoría por parte de los partidos políticos y la ciudadanía.[12] Si el sistema no es manipulable no hay problema alguno en hacerlo transparente. Los expertos en informática, las organizaciones de la sociedad civil o incluso los ciudadanos individualmente

---

10 Busaniche, Beatriz. "Voto electrónico. Los riesgos de una ilusión", 28/07/2011, La Nación, http://www.lanacion.com.ar/1392827-voto-electronico-los-riesgos-de-una-ilusion

11 Ferreira Rubio, Delia. "BUE es voto electrónico", 01/07/2015, Bastión digital, http://ar.bastiondigital.com/notas/bue-es-voto-electronico

12 Torres, Ariel. "Algunas reflexiones sobre el voto electrónico", 11/07/2015, La Nación, http://www.lanacion.com.ar/1809389-algunas-reflexiones-sobre-el-voto-electronico

tienen derecho a la información técnica. No solo a través de audiencias que son una mera formalidad, sino a través de la posibilidad de analizar el sistema en su integridad.

La transparencia y auditabilidad debe incluir el proceso de recuento de votos en la mesa de votación, en la carga de datos y contabilización del escrutinio provisorio y en el escrutinio definitivo. La información debe estar disponible para toda etapa del proceso en que se incorporen mecanismos electrónicos, sea para impresión y lectura de códigos, transmisión de datos, cómputo y publicación de los mismos.

La información sobre los resultados de mesa, escrutinio provisorio y definitivo debe permanecer disponible en Internet en forma accesible, amigable, en formato utilizable y en tiempo real. La importancia y utilidad de esta información no termina dos días después de la elección.

Creo que en la actualidad, lo más aconsejable sería ir a un sistema de boleta única en papel antes que embarcarnos en el negocio del voto electrónico. Pero más importante aún sería ocuparse de corregir el clientelismo y el abuso del poder con fines electoralistas. Si la forma de hacer política es el clientelismo (incluyo en ese rubro desde la entrega de bolsones de comida hasta el manejo político de los planes sociales), la máquina de votar no cambiará nada. Si no se garantiza la equidad en la campaña y solo se ponen límites a las fuerzas de oposición mientras el oficialismo utiliza los recursos del Estado para financiarse, la máquina de votar no cambiará nada. Si algunos políticos y sus seguidores están dispuestos a la violencia y la quema de urnas para ganar elecciones, la máquina de votar no cambiará nada, aunque sea rápida y moderna.

En síntesis, si se propicia la adopción del voto electrónico se deberían respetar algunas garantías mínimas:

a) Cualquier sistema de voto electrónico que se pretenda imponer debe garantizar efectivamente el secreto del voto. Esa garantía debe ser real a los ojos de cualquier elector, y efectiva desde el punto de vista tecnológico.

b) Se debe evitar la privatización del proceso electoral. La dependencia técnica de los organismos de control representa un grave riesgo para la limpieza de los comicios y la legitimidad de los electos. Los organismos de control electoral deben contar con la capacidad técnica y los recursos económicos necesarios para ejercer su función con plena independencia.

c) El sistema debe garantizar la más amplia auditoría por parte de los partidos políticos y la ciudadanía. Los expertos en informática, las organizaciones de la sociedad civil o incluso los ciudadanos individualmente tienen derecho a la información técnica necesaria para analizar el sistema en su integridad.

d) La transparencia y auditabilidad debe incluir el proceso de recuento de votos en la mesa de votación, en la carga de datos y contabilización del escrutinio provisorio y en el escrutinio definitivo. La información debe estar disponible para toda etapa del proceso en que se incorporen mecanismos electrónicos, sea para impresión y lectura de códigos, transmisión de datos, cómputo y publicación de los mismos.

e) La información sobre los resultados de mesa, escrutinio provisorio y definitivo deben permanecer disponibles en Internet en forma accesible, amigable, en formato utilizable y en tiempo real. La importancia y utilidad de esta información no termina dos días después de la elección.

El elemento de votación y el secreto del voto

Javier Smaldone

Por estos días en la Argentina se está discutiendo la reforma del sistema electoral. En particular, la del sistema de votación. Casualmente, acaban de cumplirse cien años de la primera elección realizada bajo la llamada Ley Sáenz Peña. Sin embargo, en persecución de una supuesta modernidad, muchos parecen olvidarse del aporte fundamental de esta ley al sistema democrático argentino: la garantía del secreto del voto.

Así se oponía el estanciero, ex ministro del autonomismo y profesor de Derecho Constitucional de la UBA, Carlos Rodríguez Larreta al punto más importante del proyecto de Sáenz Peña:

> Si mi peón hubiera tenido la misma acción que yo para resolver los problemas económicos internacionales, o políticos del país, habríamos estado viviendo bajo un régimen absurdo. No ha sido así, gracias a Dios, porque yo he dirigido a mi peón. Pero el voto secreto lo independiza, al privarlo de una influencia

saludable y legítima... Y lo malo es que a menudo no tenemos un solo peón sino varios, y que algunos tienen muchos.[1]

Y, dados los intereses que defendía, razón no le faltaba.

Por otro lado, de esta forma relató las consecuencias de la primera votación en un cuarto oscuro, con voto secreto, el historiador Félix Luna:

> Así llega el 7 de abril. Se vota con tranquilidad en todo el país. En la Capital Federal la Unión Nacional compra votos descaradamente. No pocas incidencias ocurren con este motivo. Los comités de la Unión Nacional están atestados de ciudadanos. En uno de ellos don Tomás de Anchorena pregunta uno por uno a los votantes:
> –¿Votaste bien, m'hijito...?
> –Sí, doctor –era la respuesta obligada.
> –Bueno, tomá diez pesos...
> En esas condiciones resultó inexplicable para muchos el resultado de la Capital: triunfo radical, minoría socialista... La oligarquía, los círculos oficiales no comprendían que el pueblo porteño, con su escondida picardía, se había dado el gusto de "burlar a los eternos burladores y al mismo tiempo, votar a la novia del corazón: Hipólito Yrigoyen...", como dice agudamente un escritor antiyrigoyenista.[2]

Tiempo después, en el Congreso, el presidente Roque Sáenz Peña resumiría magistralmente en una frase los efectos que causó la instauración del secreto del voto:

> Si hubo votos pagados, no hubo votos vendidos.[3]

---

1 Sampay, Arturo, *Constitución y pueblo*, Buenos Aires, Cuenca ediciones, 1974.

2 Luna, Félix, *Yrigoyen*, Buenos Aires, Sudamericana, 1999.

3 *Ibíd.*

Estancieros modernos

Desde las elecciones provinciales y nacionales de 2015, se han difundido numerosos informes periodísticos sobre el accionar de la versión moderna de don Tomás de Anchorena y sus esbirros: flotas de automóviles de alquiler –incluso motocicletas– usados como transporte de votantes, quienes reciben bolsones de alimentos, dinero en efectivo y hasta viviendas a cambio de "votar bien". El llamado "clientelismo político" sigue estando, un siglo después, a la orden del día.

Pero, ¿por qué funciona? Porque cuando el sistema de votación era novedoso desconcertó a quienes querían cometer fraude, pero con el paso del tiempo estos fueron "tomándole la mano". Lo mismo ocurre con cualquier sistema: cuando es puesto en funcionamiento, salvo fallas evidentes, todo marcha bien. Pero luego van apareciendo formas de explotar sus vulnerabilidades o de trampearlo. Y al sistema actual de votación se le han encontrado varias.

"Tomá esta boleta. Es la que tenés que poner en el sobre. Tiene una marquita aquí, ¿la ves?". "Nuestro fiscal va a firmar tu sobre de forma en que podamos saber a quién votaste. Más te vale que cumplas con el trato". Frases como estas son pronunciadas por los "punteros políticos" –delegados de la versión moderna de aquel estanciero– a los votantes al entregar el dinero en efectivo, el bolsón, o el plan social.

¿Podrá el fiscal identificar la boleta con la supuesta marca entre más de 200 que habrá en la urna? ¿Será cierto que tiene una forma de "firma codificada" para saber a qué votante pertenece cada sobre? Posiblemente no, pero... ¿estará dispuesto quien recibió un pago por su voto a correr el riesgo de traicionar al puntero? ¿O el voto comprado se transformará, ante la duda y el temor, en voto vendido? Dados los ingentes recursos que se destinan a estas maniobras, todo parece indicar que esto último es lo que en efecto sucede. La coerción resulta efectiva.

La garantía del secreto

Para que el secreto del voto ocasione el efecto deseado –nada menos que la libertad de elegir– es el votante quien debe estar seguro de su garantía. Y el sistema debe permitírselo. Si quien es presionado no puede asegurarse por sus propios medios de que nadie puede saber cómo votó, la presión surtirá efecto. En esto, el sistema electoral es como la esposa de Julio César: "Además de ser honesta, debe parecerlo".

La reforma electoral impulsada desde el gobierno actual –y que cuenta con el apoyo mayoritario de fuerzas políticas y el público en general– introduce un nuevo elemento entre el votante y la expresión de su voluntad: un sistema informático. El procedimiento de emisión del voto parece bastante robusto desde el punto de vista de asegurar que el escrutinio reflejará la selección realizada por el ciudadano frente a la computadora. La máquina permite seleccionar los candidatos en la pantalla, y luego imprime voto en una boleta de papel, y lo almacena en un chip de identificación por radiofrecuencia (RFID) contenido en la misma. El votante tiene la posibilidad de leer lo impreso, y hasta de ver lo que está grabado –en realidad, lo que la máquina le dice que está grabado– en el circuito electrónico embutido en el papel. Luego, en el escrutinio, los votos deberán contarse para poder verificar que lo impreso coincida con lo almacenado digitalmente. Ante la discrepancia o la duda deberá prevalecer lo escrito en el papel (en una instancia posterior, ya que el resultado de la mesa se basará no en lo que sus integrantes puedan leer, sino en lo que la computadora pueda contar).

Más allá de las particularidades técnicas de este sistema propuesto llamado "boleta única electrónica" –del cual existe solo una implementación en el mundo, perteneciente a una empresa privada–, ¿cómo puede el votante estar seguro de que su voto es secreto, cuando debe emitirlo mediante una computadora? La respuesta corta es: *no puede*.

Y aquí de nada sirven las auditorías (menuda tarea, si acaso posible, para un sistema de tal complejidad). El solo hecho de

que el medio de votación requiera de auditorías especializadas demuestra que el mismo no puede ser controlado por el votante, y esto debería disparar todas las alarmas. No se trata de si un grupo de personas con los conocimientos técnicos y los recursos apropiados puede –dado un tiempo razonable– asegurarse de que el sistema garantiza el secreto. Se trata de que el votante, parado frente a una computadora, pueda estar seguro de que la amenaza del puntero –"votá bien, porque tenemos las computadoras tocadas y vamos a saber a quién votaste"– no tiene asidero. Lamentablemente, esa seguridad del votante no es posible.

¿Cómo puede violarse el secreto mediante una computadora de votación? Las formas son variadas y sorprendentes. Desde la decodificación de emisiones electromagnéticas[4] (técnica conocida como *interferencia de Van Eck*),[5] hasta la utilización de componentes no previstos ni auditados[6] que permitan almacenar el orden y la composición de cada voto. Y en el caso de usar chips como el de la "boleta única electrónica", existe incluso la posibilidad de leer el contenido de la boleta desde cierta distancia.[7] Ni qué decir de las nuevas formas en que se puede obligar a un votante a demostrar si "votó bien", algunas tan simples como la utilización de un celular oculto.[8]

Puede argüirse –en un ejercicio de ingenuidad– que estas prácticas son demasiado complejas o rebuscadas. Ante cada posibilidad de vulnerar el secreto puede ofrecerse una solución a modo de paliativo. Pero el hecho es que el ciudadano común (y aun el experto en informática) no podrá,

---

4 Este video ilustra cómo funciona dicha decodificación: https://www.youtube.com/watch?v=hwz1BLRgTgo

5 Más información sobre esta técnica en https://es.wikipedia.org/wiki/Interferencia_de_Van_Eck

6 "El sistema oculto en las máquinas Vot.ar", 15/07/2015, https://blog.smaldone.com.ar/2015/07/15/el-sistema-oculto-en-las-maquinas-de-vot-ar/

7 "Sobre el chip RFID de la 'boleta única electrónica'", 08/01/2016, https://blog.smaldone.com.ar/2016/01/08/sobre-el-chip-rfid-de-la-boleta-unica-electronica/

8 "Comprando votos con la boleta única electrónica", 03/09/2015, https://blog.smaldone.com.ar/2015/09/03/comprando-votos-con-la-boleta-unica-electronica/

parado frente a una computadora en el momento de elegir a sus representantes, saber a ciencia cierta que nadie lo está espiando a través de ese sistema.

Fácil y rápido, como antes de 1912

Antes de la Ley Sáenz Peña, votar era muy simple. No había discusiones sobre boletas, sobres, ni máquinas de ningún tipo. Los ciudadanos desfilaban ante la mesa, expresaban su voluntad de viva voz y las autoridades de la misma tomaban nota (en 1873, se cambió el voto oral por el escrito, pero seguía siendo público). Los resultados estaban disponibles ni bien finalizaba el comicio, sin demoras. Y nadie podía sospechar que se había cambiado su voto, ya que todo estaba a la vista. Pero llegó el secreto, y cambió de raíz el sistema de votación.

Estamos a más de cien años de ese cambio, y celebramos que gracias a él pudimos finalmente tener elecciones libres y justas, aun tolerando ciertas demoras en conocer los resultados. Y también, sabemos que es posible que algunos votos sean adulterados, pero también podemos buscar la forma de mejorar el sistema (y la fiscalización) para minimizar esos casos.

Hoy se nos propone votar usando computadoras. Con la promesa de tener resultados provisorios más rápidamente, con la esperanza de que sea más difícil adulterar el resultado de la votación (esperanza que muchas veces radica en una forma de pensamiento mágico).[9] A cambio, la posibilidad del votante de cerciorarse de que su voto es secreto se ve severamente comprometida. ¿Puede alguien que esté bajo presión correr el riesgo de creer en la palabra autorizada de un grupo de auditores que le asegura que todo se hace correctamente? ¿Debe un ciudadano confiar en una élite al realizar el acto vital y primigenio de una democracia republicana? Claramente, no.

---

9 "Magia electrónica", 01/08/2015, https://blog.smaldone.com.ar/2015/08/01/magia-electronica/

Sobre cómo mejorar el sistema

El sistema actual tiene problemas, eso es evidente. Pero en la búsqueda de la solución, no debe debilitarse el pilar del secreto del voto. ¿Hay robo de boletas o boletas falsas en el cuarto oscuro? Usemos boletas únicas –como la mayoría de los países del mundo–, papeles con grillas donde aparezcan todas las opciones, que sean retiradas de la mesa de votación por el votante (lo que también elimina el "voto cadena"). ¿Alguien duda sobre la posibilidad de boletas marcadas? Que la boleta única sea retirada por el ciudadano de una pila colocada al lado del presidente de mesa, eligiendo la que más le plazca. ¿Se adulteran boletas en el escrutinio? Pensemos en medidas de seguridad para evitarlo (no, ninguna funcionará sin fiscalización, por más que usemos los sistemas electrónicos más rebuscados). ¿Las actas confeccionadas manualmente tienen errores o resultan ilegibles? Usemos sistemas de impresión dispuestos en los centros de votación. ¿El escrutinio provisorio parece una "caja negra" en donde pueden alterarse los resultados? Usemos los medios que proveen la informática y las telecomunicaciones para abrirlo a la ciudadanía, de modo que todos podamos controlar, desalentando por lo tanto las manipulaciones.

En la mejora del sistema de votación, debemos buscar más transparencia. Debemos dar más control al votante sobre su voto, y no menos. Interponer entre el votante y su voluntad un elemento tan opaco (u oscuro) como una computadora va exactamente en el sentido opuesto: no ofrece transparencia, necesita auditorías; no brinda confianza, la requiere.

La experiencia mundial así lo evidencia: el uso de computadoras para emitir el voto, luego de más de cuatro décadas de investigación, desarrollo y pruebas, está en franco retroceso en la inmensa mayoría de los países. Actualmente, solo en Brasil, Venezuela, India y la mitad de Bélgica se vota usando computadoras. En los EE. UU., pionero mundial del uso de máquinas –inicialmente mecánicas, luego electrónicas– para votar, cada vez son más los estados que se vuelcan al uso de boletas de papel. En 2010, Israel descartó el uso de

un sistema muy similar al de la "boleta única electrónica". Finalmente, en el caso extremo de países como Alemania, los Países Bajos, Irlanda y el Reino Unido, después de probar en mayor o menor grado alternativas de este tipo, erradicaron completamente las máquinas.

Es particularmente esclarecedor el fallo de 2009 de la Corte Constitucional de Alemania, que declaró inconstitucional el uso de computadoras para votar (el énfasis es agregado):

> 1. El principio de la publicidad de la elección del artículo 38 en relación con el art. 20 párrafo 1 y párrafo 2 ordena que *todos los pasos esenciales de la elección están sujetos al control público*, en la medida en que otros intereses constitucionales no justifiquen una excepción.
>
> 2. En la utilización de aparatos electorales electrónicos, *el ciudadano debe poder controlar los pasos esenciales del acto electoral y la determinación del resultado de manera fiable y sin conocimientos técnicos especiales*.[10]

La garantía del secreto del voto es esencial. Es vital fortalecerla, para seguir preservando la máxima de Sáenz Peña, y que un voto comprado no pueda transformarse en un voto vendido, si el votante así lo dispone.

---

10 Sentencia 2 BVC 3/07 - 2 BVC 4/07, Corte Constitucional Alemana (traducción de Manfredo Koessl).

Vot no[1]

Nicolás D'Ippolito

Hablemos de las elecciones. Hablemos de la boleta única electrónica.

Sin preámbulos ni entrada en calor, hablemos de la posibilidad de que alguien pueda manipular las máquinas que usaríamos para votar. Podemos empezar por prestar atención al siguiente fragmento de código:

```
[…]
    read_unlock(&tasklist_lock);
    if (flag) {
    retval = 0;
    if (options & WNOHANG)
```

1 Este artículo fue publicado originalmente en el sitio *El Gato y la Caja*. Se puede leer el original que incluye algunas imágenes y videos en https://elgatoylacaja.com.ar/vot-no/

```
    goto end_wait4;
    retval = -ERESTARTSYS;
    if (signal_pending(current))
    goto end_wait4;
    schedule();
    goto repeat;
    }
   if ((options == (__WCLONE|__WALL)) && (current-
>uid == 0))
    retval = -EINVAL;
   else
    retval = -ECHILD;
   end_wait4:
    current->state = TASK_RUNNING;
    remove_wait_queue(&current->wait_chldexit,&wait);
    return retval;
   }
```

Es importante verlo detenidamente, sé que parece tedioso pero vale la pena el esfuerzo. Acá va de nuevo:

```
   […]
    read_unlock(&tasklist_lock);
    if (flag) {
    retval = 0;
    if (options & WNOHANG)
    goto end_wait4;
    retval = -ERESTARTSYS;
    if (signal_pending(current))
    goto end_wait4;
    schedule();
    goto repeat;
    }
   if ((options == (__WCLONE|__WALL)) && (current-
>uid = 0))
    retval = -EINVAL;
   else
```

```
 retval = -ECHILD;
end_wait4:
 current->state = TASK_RUNNING;
 remove_wait_queue(&current->wait_chldexit,&wait);
 return retval;
}
```

¿Qué es lo importante de este código? Que no es uno, son dos distintos, con una pequeña diferencia: uno de ellos tiene un signo '=' de menos. Es la única diferencia, dos miserables rayitas, pero con una implicancia no menor: si el segundo estuviese corriendo en una computadora, esta podría ser hackeada con facilidad. Se trata de un caso real del año 2003, de código que se encuentra en la parte central del sistema operativo Linux.[2] La diferencia entre la versión correcta y la que te hace sonar es tan sutil que es muy difícil de detectar, incluso por expertos (para ser riguroso, este caso se detectó con facilidad porque se trató de una modificación a un código ya existente y hay herramientas que muestran solo aquellas líneas que cambiaron, que en este caso eran solo dos, cuando hay que auditar una pieza de software desde cero no se cuenta con esa ventaja).

Me adelanto a la objeción: si fuera tan difícil, ¿cómo saben las empresas que venden software que sus productos no tienen fallas? La respuesta es muy sencilla: no lo saben. Y no se trata de que en su ansia desmedida por apropiarse de la renta saquen productos a medio cocinar. Bueno, a veces un poquito sí, pero hay dificultades mucho más de fondo.

Seguro es el que probó y confió

Ahora, podríamos probar con probar, ¿no? Es decir, si uno quiere saber si una pieza de software falla en algún caso,

---

2 Felten, Ed. "The Linux backdoor attempt of 2003", 09/10/2013, http://freedom-to-tinker.com/2013/10/09/the-linux-backdoor-attempt-of-2003/

puede probarla y con eso alcanza, ¿no? No, la verdad es que con probar no alcanza. El testing es la disciplina informática encargada de probar una pieza de software buscando incrementar la confianza que se tiene en que opera como debe. Funciona así: uno prepara una batería de casos de prueba, que son descripciones paso a paso de qué hacer con el sistema, y compara el resultado obtenido con el esperado. Si no son iguales, acabamos de encontrar un defecto (lo que coloquialmente se llama 'un bug').

Por otro lado, si sí lo son, la única garantía que tenemos es que esa interacción (y no otra, y mucho menos todas) funcionó bien la vez que la probamos, pero tampoco es que estamos tan seguros. Aun si corremos otra vez exactamente la misma secuencia, este segundo intento podría fallar porque no sabemos si el programa en cuestión tiene en cuenta alguna 'variable invisible', como por ejemplo la hora de la computadora, y entonces se comporta de una forma cuando esa variable es una (digamos, a las 9:13 de un martes), y de forma distinta en otra (por ejemplo, a las 4:12 de la madrugada del sábado). El que no se comporte distinto a las 4:12 del sábado, que tire la primera piedra.

Aun si tuviésemos el código y pudiésemos mirar todas las variables involucradas, las alternativas crecen exponencialmente y los caminos posibles a probar son millones de millones. Es decir, el testing es un paso fundamental para asegurar la calidad del software, y cuando encuentra un defecto, hay que arreglarlo; pero el testing nunca puede asegurar la ausencia de defectos.

Existen métodos automáticos que también ayudan a aumentar la confianza en que el software funcione como se espera. Algunos son muy buenos, pero tampoco son infalibles. La cosa se complica aún más si estamos haciendo testing de seguridad, ya que en ese caso el comportarse correctamente implica que no solo haga lo que tiene que hacer, sino que no haga nada 'extra'. Un ejemplo puede ser el caso del acceso a un home banking: no solo debe dejarme entrar solamente con la contraseña correcta, sino que siempre

debe transportarla por la red de manera encriptada y un largo etcétera de requisitos que hacen a la fortaleza y seguridad del sistema.

Pero hay más: no solo debe cumplir con estos requisitos, sino que no debe tener ningún tipo de agujero de seguridad, de esos que aprovechan los virus y los hackers para subvertir un sistema y hacer que sucedan cosas no contempladas. En un sistema informático, es muy, muy difícil encontrar fallas sutiles (a modo de ejemplo, un bug de seguridad en un software de código abierto muy usado estuvo presente 20 años hasta que fue hallado u otro que se detectó hace pocos días y estuvo latente por 11 años y presente en las máquinas con las que se votó en la CABA), y ni hablar de aquellas que son introducidas a propósito con la intención de que no puedan hallarse. Valga como ejemplo el bug introducido intencionalmente en el año 2006 en la especificación de (prepárense que parece chino lo que sigue, pero es algo importante) el generador de números al azar 'Dual_EC_DBRG', que es una parte central de muchos algoritmos criptográficos. Posteriormente, varios fabricantes implementaron el estándar viciado en sus productos y por ende muchísima información sensible que debía ser protegida por mecanismos criptográficos quedaba al desnudo para el autor del bug, que muchos sospechan que se trataba de la NSA. El incidente recién salió a la luz pública en el año 2013.

Algo que sabemos hace mucho en el mundo del software es que uno no puede tener garantías de que no hay fallas, y a lo que debe apuntar es a tener un muy alto nivel de confianza en que el sistema en cuestión funcione como se espera.

¿Qué tan grave es que falle el software? Bueno, si falla Tinder, tal vez nuestros genes no se propaguen (quién te dice, terminamos haciendo un bien a la humanidad). Ahora, si falla un marcapasos, uno pensaría que es bastante más grave. Pero, ¿y si el software altera o permite alterar un resultado electoral? Como el marcapasos, pero de escala país. A eso se lo conoce como la *criticidad*, es decir, qué tan graves son las consecuencias de que falle un sistema.

Cuando se trata de software crítico a lo que debe apuntarse es a hacer nuestro mejor esfuerzo para disminuir la chance de que ese software tenga fallas. Cabría preguntarse por qué se usa software en esos casos si no puede garantizarse que sea seguro. La respuesta es simple: porque las otras alternativas que podrían cumplir las mismas funciones o bien no existen o también pueden fallar.

Tener un alto grado de confianza en un sistema tan crítico como el que interviene en una elección requiere de mucho tiempo de trabajo por parte de un grupo de expertos, que utilizará técnicas como inspección ocular, revisión entre pares, testing, análisis estático y dinámico de código, penetration testing (no relacionado con Tinder) y un largo etcétera durante un periodo prolongado de tiempo. Los hallazgos de ese trabajo realimentarán el proceso de diseño y programación del sistema, y el proceso de prueba deberá recomenzar. Pero, ¿qué pasa en el caso de una elección? ¿Es posible que todos estos controles no sean suficientes? Sí.

Para nosotros que lo miramos por TV

Para entender por qué, imaginemos el próximo proceso electoral de nuestro país: una compra así de grande debe hacerse por licitación, supongamos que se hace mañana, que procede sin dificultades y se evalúa en tiempo récord.

[Pausa para recuperarse de la risa]

El 1° de enero de 2017 la empresa concesionaria termina por completo de desarrollar los sistemas que intervendrán en la elección, los prueba, los analiza y determina que funcionan correctamente. No estamos hablando de desarrollar una app chiquita; se trata de un sistema muy grande, que incluye mucho código desarrollado por la propia empresa, mucho código desarrollado por terceros, e incluso un sistema operativo o parte de él (que puede tener fallas como

las que describimos al comienzo del artículo). Todas y cada una de esas partes deben chequearse profundamente porque funcionan de manera encadenada y el resultado final puede alterarse en cualquiera de ellas. En definitiva, el sistema entero es tan fuerte como la parte más débil de la cadena.

Ese 1° de enero, ya curada la resaca, expertos de todos los partidos se reúnen y analizan el sistema utilizando todas las técnicas que mencionamos anteriormente. El sistema completo a probar es muy complejo, dado que contiene hardware (lo que se puede patear) y software (lo que solo se puede putear), así que les toma 6 meses. Menos tiempo, no es realista; más tiempo, se dificulta llegar a agosto con las máquinas repartidas por los más de 3 millones de km cuadrados de nuestro territorio. Entonces se juntan y en un éxtasis de felicidad brindan porque todas las fallas que fueron encontrando se fueron arreglando (lo cual solo significa que no encontraron más fallas, no que no existan).

La primera pregunta es: ¿cómo saben que todos auditaron el mismo sistema? Eso es fácil de resolver con el software porque uno puede calcular una firma digital del código del sistema, y si las firmas coinciden es que auditaron el mismo software. ¿Y el hardware? Bueno, no existe tal cosa como la firma digital del hardware, así que realmente no hay forma de saber que probaron con el mismo hardware, y eso es importante porque lo que determina qué va a pasar es la combinación de hardware y software. Y sí, se pueden poner "virus" por hardware.

Pero supongamos que decidimos pasar por alto ese "detalle" y, en un acto de fe ciega, suponemos que todas las computadoras que se van a usar en la elección fueron bendecidas por Santo Tomás de los Pines en persona y por ende suponemos que el hardware simplemente ejecuta el software en forma fiel, sin interferir con su funcionamiento (insisto con esto: en un acto de fe). ¿Cómo sabemos que el software que se va a ejecutar es el que fue auditado? Deberían reunirse todos, todos, todos, frente a otra de esas computadoras bendecidas y compilarlo ahí mismo (*compilar* es el proceso por el que se

pasa de un texto escrito en un lenguaje de programación a esa secuencia de ceros y unos llamada código de máquina, que es lo único que "entiende" una computadora realmente). De nuevo, necesitamos otro acto de fe para ignorar el artículo de Ken Thompson, laureado en 1984 con el Premio Turing (aka "el Nobel de la Computación"), llamado "Reflections on Trusting Trust", que explica cómo el propio compilador puede ser saboteado para, a partir de un programa sin problemas, producir código de máquina malicioso.[3]

Supongamos que también ignoramos eso, así como el trabajo posterior que lo muestra en la práctica. Tenemos nuestro código de máquina compilado delante de todos, que suponemos que no tiene trampas. Calculamos una firma digital de ese código de máquina y se la pasamos a todos nuestros fiscales. Y ojo acá, que cabe recordar que ya venimos acumulando dos actos de fe, uno por el hardware, otro por el compilador.

Llega el día de la elección, viene el empleado del correo con una de esas máquinas que por acto(s) de fe suponemos que no tienen problemas. Trae también su CD o pendrive con el código de máquina que es lo que define qué pasará realmente con ella, y cada uno de los fiscales partidarios chequea con su computadora (que tienen, porque la VAN a necesitar, así que asumimos que hay una computadora para CADA fiscal) si la firma digital de ese CD o pendrive coincide con el que fue compilado delante de todos. Esto es absolutamente indispensable, porque si los fiscales no pueden corroborar individualmente que el software que se instala en cada máquina es el auditado, no solo existe la posibilidad real de que se instale otro, sino que además se deja abierta una puerta para que cualquiera disconforme con el resultado lo atribuya a una adulteración y tenga un punto muy fuerte a su favor.

---

3 El artículo en inglés se puede leer en esta página: http://dl.acm.org/citation.cfm?id=358210

Todo esto supone además que no hay que hacer ninguna modificación de último momento (como que la justicia autorice algún cambio en las listas o en la forma de presentarlas, algo que es muy usual), porque habría que repetir todo el proceso de nuevo, ya que cambia el código fuente, el código de máquina y la firma digital.

Nada puede malir sal

¿Qué podría pasar si las máquinas de votación estuvieran "comprometidas"? La verdad, de todo. Recordemos que, en el formato 'boleta electrónica', el ciudadano elige a sus candidatos y la máquina debe grabar su elección de forma digital y además imprimirlo en formato legible. Una máquina comprometida o adulterada podría imprimir al candidato A en letras y grabar digitalmente al B.

No tiene que hacerlo siempre, que sería muy obvio, puede hacerlo en una cantidad estadísticamente pequeña de casos, lo suficiente como para asignarle una banca de más o de menos a algún partido, o definir un ballotage muy parejo para una presidencia (pongámosle un 51 a 49 hipotético, o recordemos también el referéndum en Colombia[4] donde el No ganó con 50,2% de los votos).

Si de variaciones estadísticas se trata, también podría pasar que el orden al azar en el que aparecen los candidatos no sea tan al azar, dándole prevalencia a alguno. No vamos a hacer un listado exhaustivo, pero analicemos un poco más.

Unos investigadores independientes reportaron un defecto en el sistema usado en la CABA para las elecciones para Jefe de Gobierno de 2015: permitía cargar varios votos a la vez,

4 Se refiere al referéndum sobre las FARC. Este artículo amplía el tema mencionado: "Referéndum con sorpresa: los colombianos rechazar el acuerdo de paz con las FARC", Clarín, 03/10/2016, http://www.clarin.com/mundo/referendum-sorpresa-colombianos-rechazan-farc_0_r1stzByo.html

algo que ninguna de las auditorías oficiales había notado.[5] Otro investigador descubrió un manejo poco seguro del mecanismo de encriptación utilizado, lo que permitía que cualquiera mandara al centro de cómputos resultados como si fuesen oficiales. Lo reportó antes de las elecciones y por supuesto que fue automáticamente respetado y tratado con cuidado… O no: fue allanado y enfrentó un proceso judicial que duró casi un año[6] (así como al pasar, durante ese proceso se determinó que los servidores de la empresa que brindó el servicio habían sido hackeados), con altos costos, hasta que finalmente la justicia determinó que no había cometido ningún delito (y hasta que había dado una genuina mano identificando los problemas). Porque si hay algo que querés cuando reportás un bug en un sistema público crítico es que te traten como un peligroso delincuente y te secuestren todos los aparatos electrónicos, incluyendo compu, laptop, Kindle, y una licuadora que parece que miraba fijo a uno de los gendarmes.

Pero, si es electrónico, tiene que ser fantástico

Una objeción que se escucha con frecuencia es que está previsto el escrutinio manual. Analicemos esta posibilidad basándonos en los datos duros del informe final de la Defensoría del Pueblo de la CABA sobre la elección para Jefe de Gobierno de 2015. Según este informe, "una vez cerrada la mesa, el 83,9% de los presidentes pudo realizar el escrutinio sin inconvenientes. Durante el conteo de votos, solo el 10,1% de las mesas contó con fiscales que realizaron algún reclamo". Esto significa que hubo cerca de 730 mesas con

---

5 Cf. Video "Multivoto: sumando múltiples votos con una boleta en el sistema vot.ar", https://www.youtube.com/watch?v=CTOCspLn6Zk

6 Para ampliar sobre el caso de Joaquín Sorianello, se puede leer este artículo: http://www.clarin.com/politica/allanan-detecto-vulnerabilidades-sistema-electronico_0_HkBRiUKwml.html

reclamos. A 300 votantes por mesa, hay unos 219000 votos en cuestión, muy por encima de los 54000 que definieron la elección en CABA y peligrosamente cerca de los 300000 votos de diferencia que definieron el ballotage presidencial de ese mismo año. De ese informe surge también que un 26,2% de los votantes dijo no haber verificado que el voto impreso coincidiera con lo que había elegido.

Pero además, aun en el caso en que todas las mesas electorales corroboraran el escrutinio electrónico con uno manual, el manual es solo corroboración de una planilla que se graba digitalmente en otra boleta electrónica. De nuevo, un software malicioso podría hacer que la grabación tenga cifras adulteradas incluso cuando la propia máquina las siga mostrando como correctas. O tal vez la manipulación podría hacerla la máquina que lee la tarjeta y manda la información a través de Internet hacia el centro de cómputos (que a su vez podría tener software adulterado o hackeado como el de CABA en 2015). No sé cómo vienen ustedes, pero a esta altura ya perdí la cuenta sobre la cantidad de saltos de fe.

Memoria y "países serios"

El pueblo argentino se ganó el voto universal, secreto y obligatorio en cuotas. Primero nos ganamos el voto (de entrada solamente los varoncitos, aunque ellas conquistaron la universalidad un par de cuotas más tarde), varias dictaduras nos lo sacaron y hubo que reconquistarlo. En el medio de esas peleas, conquistamos el voto secreto, y lo consagramos en la Ley Sáenz Peña.

Entonces teníamos la posibilidad de que nadie supiera a quién votaste, para que no pudieran chantajearte, presionarte, comprarte o vengarse de vos si no les gustaba tu decisión. Esto se manifiesta de manera muy clara cuando tenemos la posibilidad de poner nuestro voto en un sobre idéntico a todos los sobres para después abrir la urna y contar (y sí, hay maneras de manipular y de romper el secreto de voto, pero

son fácilmente identificables y auditables por ciudadanos comunes).

Hay que tener memoria, algo que las computadoras también tienen. Justamente el tema de la memoria es central en el argumento de la Corte Suprema de Alemania que, en el año 2009, prohibió el uso de urnas electrónicas porque contradice el principio de que todos los pasos de la elección estén sometidos al escrutinio público sin requerir conocimientos técnicos especiales.

Si pudiera elegir un solo párrafo para ser recordado de todo este texto (que intenta ser exhaustivo respecto de las múltiples aristas a considerar en la adopción o no del voto electrónico y sus variantes), sería éste: si dependemos de un proceso técnicamente inaccesible para la enorme mayoría de nosotros (salvo los expertos en desarrollo de sistemas de votación electrónica), la transparencia del sistema para el ciudadano común desaparece.

Con el voto electrónico y sus variantes, a la democracia la vemos pasar, la miramos por TV. Nos cuentan y tenemos que creer o reventar. El pilar de nuestra construcción democrática, la elección, se transforma en algo que no entendemos, que no podemos auditar. No es un detalle menor que el voto sea secreto. Es esencial y nadie nos lo regaló, hubo que luchar mucho para conseguirlo. Con el voto electrónico y sus variantes, puede dejar de serlo. Lo que es peor aún, no sabemos si es o no secreto, y sembrar esa duda (que se vuelve razonable porque el sistema es tan opaco que no hay forma de saber la verdad), alcanza para que alguien pueda manipular nuestra decisión. El voto no solamente tiene que SER secreto, sino que tiene que LUCIR secreto, para poder ser ejercido sin presiones.

De imprentas e impresoras

El sistema actual no es perfecto: es cierto que es problemático y costoso distribuir las boletas a todos los cuartos oscuros,

y que sería muy bienvenida una alternativa superadora a semejante desafío logístico, especialmente para los partidos chicos. Pero superadora de verdad, no solo aparentemente. Si vamos a informatizar, pensemos en lo que pasa después de votar, desde hacer un conteo asistido de los votos hechos en papel a cosas mínimas como disponer de un procesador de texto y una impresora en los cuartos oscuros para que las actas no sean manuscritas y haya menos errores de transcripción.

Muchas veces se revolea el argumento de que las máquinas de votación son solamente impresoras. Es un argumento casi gracioso porque las impresoras de hoy en día son solamente otro tipo de computadoras y, como tales, también tienen memoria. Y pueden usar esa memoria para registrar que, por ejemplo, el primer votante votó por A, el segundo por B, el tercero por A de nuevo, y así siguiendo. Con el simple expediente de ir contando, todos los fiscales partidarios pueden saber quién votó primero, quién segundo, etcétera. No solo los fiscales, basta con poner a un chabón a fumar en la puerta del cuarto oscuro. Es decir, no alcanza con que el sistema no manipule los resultados, también hay que garantizar que no registre información de más.

Y la verdad es que en este caso hace falta poca memoria, o casi ninguna: en cada cuarto oscuro votan unas 300 personas; ese número se codifica con solo 9 bits.

Si no te resulta obvio que el número 300 se codifica con 9 bits, es un claro ejemplo de cómo el sistema que estamos discutiendo también te dejó afuera a vos, una persona probablemente educada, curiosa e informada, pero que no tiene conocimientos específicos sobre computación. Qué loco pensar que con esas mismas condiciones sí podrías auditar todo el proceso de voto en papel: saber leer, ser curioso y educarte respecto del proceso de fiscalización (algo que demora minutos).

Decíamos que alcanza con 9 bits, 9 puntitos escondidos en cualquier parte de la boleta en papel para saber a quién votó cada persona. Si alguien va contando en qué orden vota cada uno de los electores, luego, cuando recuperan las boletas en

papel, se miran esos 9 puntitos mínimos, escondidos con algo de cautela, tal vez en el borde de una letra, tal vez simulando ser una mancha de tinta, y se puede reconstruir a quién votó cada elector. ¡En tu cara, Sáenz Peña!

Comparando

El sistema electoral actual no es perfecto y tiene mucho para mejorar. Pero es mucho mejor de lo que se nos quiere hacer creer repetidas veces. Si una fuerza política quiere gobernar una ciudad debe concitar las voluntades de la mayor parte de los electores de la ciudad, pero el requisito previo es que tenga un núcleo de personas con un nivel mayor de adhesión, realmente entusiasmados por la propuesta, que estén dispuestos a ser fiscales durante un día. ¿Con qué requisitos? Los básicos: prestar atención, saber leer, sumar y restar, condiciones que en líneas generales cualquier adulto puede cumplir. Sería razonable que las fuerzas políticas que tienen una ambición mayor, como la de gobernar una provincia, tuvieran una cantidad de entusiastas proporcional al tamaño de la provincia. Si no, es muy difícil pensar que la van a poder gobernar. El mismo razonamiento cabe si quieren gobernar un país. Por supuesto que no es fácil, pero gobernar tampoco lo es. Si no podés resolver el problema de conseguir veinte fiscales para ser intendente de tu ciudad, difícilmente puedas resolver los problemas que conlleva la propia intendencia, donde son muchas más las voluntades que deben alinearse, durante mucho más tiempo que un par de domingos cada dos años. Lo mismo si querés gobernar un país.

Por otra parte, es poco verosímil y hasta peligroso que una fuerza política acepte dejar la máquina de votación sin supervisión, con lo que la implementación de mecanismos electrónicos tampoco elimina la necesidad de fiscales.

Para los fiscales, el sistema actual podría mejorarse en varios puntos, pero el hecho de poder entrar por la web y ver si el telegrama escaneado tiene tu firma y si la planilla

electrónica coincide con lo que está escrito a mano y con tu copia del acta es un punto de control muy fuerte.

Dada la propuesta actual de voto electrónico, con tener fiscales no alcanza, porque en definitiva los puntos de control establecidos de nada sirven si se pierde el secreto del voto, si lo que se graba en la boleta no refleja la voluntad del elector en todos los casos, o si luego esa información es nuevamente volcada a otra computadora que puede manipularla en el proceso.

No es menor decir que este análisis no parte de ser un romántico de los viejos tiempos o un férreo opositor a la ciencia y la tecnología. Lejos estoy de serles fóbico o de no comprenderlas. Es más bien lo contrario en este caso: entender cómo funciona la tecnología digital nos da herramientas para poder mirarla con ojos críticos. Justamente por eso entendemos sus limitaciones, como lo hacen casi todos los países desarrollados (para nada tecnofóbicos), que siguen votando en papel.

De hecho, si lo que se busca es boleta única, existe la boleta única en papel: en un mismo cacho de árbol tenés a todos los candidatos de todos los partidos y le ponés una cruz a los que prefieras (la única dificultad es que hay que explicarles a los adolescentes que se elige solo con una cruz y no vale usar otros emoticones).

Decía más arriba que con la boleta electrónica la transparencia se pierde, y es importante recalcar que no reaparece si, en lugar de implementarse a las apuradas, se hiciese con tiempo suficiente.

El sistema está intrínsecamente viciado porque el piso mínimo necesario para entender el proceso electoral electrónico, auditarlo y participar de su control, se vuelve prácticamente inalcanzable. Pasa de requerir habilidades que se adquieren en la escolaridad básica a volverse una discusión de expertos, cerrada, críptica, y por ende, excluyente.

Somos los ciudadanos y ciudadanas comunes, los que armamos ese nosotros bien grande que trasciende lo que nos aúna y lo que nos separa, los que queremos poder votar de

forma secreta y segura, y que nuestro voto se escuche. Que se escuche cristalino, sin intermediarios, dudas o mugre.

Que se escuche exactamente como lo manifestamos, aun cuando el resultado no nos guste, pero sabiendo que genuinamente nos representa.

2.
nuestro enfoque

Objeciones a los sistemas de voto electrónico[1]

Enrique A. Chaparro

Si bien es cierto que la democracia debe ser más que elecciones libres, también es cierto que no puede ser menos.
Kofi Annan

Preliminar: definiciones

Adoptamos en este trabajo la definición de "voto electrónico" de Alvarez y Hall (2010, 9–10):[2] la acción del votante que convierte su selección en una cadena de señales electrónicas define la condición de voto electrónico. Esta, por lo demás, es consistente con la opinión generalizada tanto jurídica como técnica.[3] Los sistemas denominados comercialmente "boleta única electrónica" (BUE), como los usados en las elecciones

1 Una versión extendida de este trabajo académico con más referencias bibliográficas y otras precisiones puede leerse en https://www.vialibre.org.ar/wp-content/uploads/2016/06/ECh_VE_3CADE_ponencia.pdf

2 Las referencias bibliográficas de este ensayo pueden reponerse en la sección "Bibliografía general" de este libro.

3 Para un breve análisis comparado, véase Chaparro (2015, 36–47). Para una taxonomía de los sistemas de voto electrónico, véase Franklin y Myers (2012).

locales de 2015 en la Ciudad de Buenos Aires y en la provincia de Salta, pertenecen pues a esta clasificación: es un sistema de registro electrónico, puesto que las opciones escogidas por el votante se registran directamente en una memoria electrónica incluida en la BUE, e incluye un comprobante impreso verificable por el elector. Para el caso, carece de significación que el registro electrónico se realice en un dispositivo distinto de la misma especie para cada voto, o que se acumule en una única unidad de memoria incorporada al dispositivo en el cual se lleva a cabo la emisión del voto, puesto que la lógica implícita es la misma. Tampoco hace diferencia que el proceso de totalización se lleve a cabo con cierto diferimiento o en simultaneidad con la emisión del voto, porque en ambos casos la operación involucrada implica leer del dispositivo de memoria (distribuido en dispositivos individuales en el caso de la BUE o sistemas similares, o consolidado en otros sistemas) mediante un programa y acumular los resultados parciales hasta obtener el escrutinio provisorio.

Los procesos automatizados a través del voto electrónico son entonces el de emisión, el de registro y el de conteo (o escrutinio primario). Definiremos como *emisión* al proceso por el cual el elector expresa su voluntad; *registro*, a aquel por el cual la voluntad expresada por el elector es fijada en un medio permanente y, al mismo tiempo, se torna imposible correlacionar la identidad del votante con su voto; y *conteo* al proceso por el cual se contabilizan los votos emitidos, asignándolos a las diversas candidaturas o propuestas. El objetivo, entonces, de un sistema electoral es que los votos sean emitidos como expresión fiel de la voluntad del votante (*cast as intended*), registrados tal como fueran emitidos (*recorded as cast*) y contados como fueran registrados (*tallied as recorded*).

Como mecanismo adicional contra la coerción, algunos sistemas electorales establecen salvaguardas complementarias; las más usuales son que no se emita recibo que permita identificar qué votó el elector, y que el resultado no pueda ser conocido antes de un momento prefijado y posterior a

la finalización del período establecido para que los electores puedan emitir sus votos.

I. El voto electrónico

El acto de votar para elegir representantes o establecer opinión es central a las formas democráticas de gobierno. Toda soberanía emana del pueblo, como bien señala nuestra Constitución Nacional, y es mediante ese acto fundamental que los representes del pueblo, y por extensión todo el sistema de gobierno, obtienen su legitimidad. En las palabras de Thomas Paine (1795), un protagonista destacado de las dos grandes revoluciones del siglo XVIII que darán forma a los modernos estados democráticos, "el derecho al voto es el derecho primario con el cual se protegen todos lo demás". El eco de las palabras de Paine resuena en Alberdi (1920): el voto es "la primera y la más fundamental de las libertades".

La Argentina tuvo un largo y complejo tránsito hacia el voto libre, universal, igual y secreto, y prueba de ello es que la legislación electoral nacional, basada en la ley 8871 por la que el nombre de Roque Sáenz Peña ha pasado a la historia, es extraordinariamente puntillosa, hasta en los detalles aparentemente menos relevantes, respecto de los procedimientos de garantía del sufragio.

En esencia, la cadena de legitimidad se construye a partir de la confianza del elector[4] en que su intención de voto va a ser computada fielmente. Es importante notar que nos referimos a la intención y no a la expresión de esa intención (es decir, el documento de cualquier tipo que la refleja): la diferencia radica en que es un requisito fundamental del sistema electoral garantizar el reflejo fidedigno de la intención

4 Usamos el género gramatical masculino para el genérico, tal como es norma en la gramática de nuestra lengua. No obstante este mecanismo de economía de expresión, debe entenderse que nos referimos a personas sin distinción de género biopolítico.

en el vehículo que la documenta. Los sistemas manuales de emisión y conteo primario que se utilizan en la mayoría de los países del mundo, bajo la forma de boleta única (conocida también como "boleta australiana" en los países de habla inglesa)[5] o boleta partidaria, están en general bien probados, ajustados por la experiencia de muchos años, y todos sus pasos son sencillamente verificables por percepción directa de los sentidos; la emisión implica un acto claro y directo de manifestación de la voluntad del elector haciendo una marca o escogiendo una papeleta, y el conteo primario es de sencillez tal que cualquier persona con conocimientos rudimentarios de aritmética puede realizarlo o verificar que se efectúa correctamente. En los sistemas electorales de muchos países se permite la observación pública del conteo primario; en los que eso no sucede, se garantiza el control público mediante la presencia de representantes de los partidos que intervienen en la elección, que ejercen control recíproco por oposición de intereses, y normalmente cualquier ciudadano puede registrarse como voluntario en el partido de su preferencia para ejercer esta función.

La informatización del sufragio

La introducción de tecnologías informatizadas en el proceso de emisión del voto y en el conteo provisorio que sigue inmediatamente al comicio, sin embargo, trae consigo interrogantes nuevos sobre la preservación de las garantías. Es habitual que la tecnología se mueva más rápidamente que el sistema legal; no obstante ello, la evolución tecnológica debe ser siempre procurada como un medio para mejorar la vida humana y no como un fin en sí misma. En este sentido,

---

5 La primera legislación electoral del mundo que preveía voto secreto con cédulas de papel en que aparecían los nombres de todos los candidatos fue sancionada en Tasmania el 4 de febrero de 1856. Al poco tiempo siguieron Australia del Sur (12 de febrero) y Victoria (13 de marzo). La primera elección con el nuevo método se llevó a cabo en el este último territorio el 27 de agosto del mismo año.

todo desarrollo tecnológico, y en particular cuando directa o indirectamente afecta principios fundamentales, debe ser cuidadosamente revisado centrando la atención en determinar su contribución hacia una sociedad mejor (Mitrou et al., 2002). Como bien señala Pellegrini (2014),

> el buen desarrollo del proceso electoral se acredita por medio de cadenas de confianza, que se rompen con la introducción de dispositivos opacos, concebidos y aplicados por terceros.

La certeza sobre la intención del votante se vuelve más difusa por la existencia de un mecanismo de expresión controlado por un programa informático que el votante desconoce (y es a veces desconocido también para las autoridades electorales), y que es imposible analizar sin un conjunto de conocimientos altamente especializados. Las tareas de control de las personas encargadas de verificar pasos esenciales del proceso electoral quedan reducidas a la mera visualización, o a actuar como dispositivos periféricos de alimentación de datos a un sistema informático que en esencia se desconoce.

A pesar de estas limitaciones problemáticas, que ponen en cuestión algunos de los atributos fundamentales del voto, a finales del siglo pasado y comienzos del actual, hubo una marcada propensión a considerar las percibidas ventajas de los sistemas de voto electrónico que llevó a muchos gobiernos a experimentarlo y ponerlo en práctica.

Los Estados Unidos fueron un país pionero en la implantación de sistemas de voto electrónico en los últimos dos decenios del siglo pasado, principalmente debido a tres razones: las particularidades de su sistema electoral, que hacen muy complicada la cuenta manual, el desarrollo de su industria informática y una prolongada tradición en el uso de dispositivos primero mecánicos y luego electromecánicos que se remonta a finales del siglo XIX.[6] El primer sistema de

6 Para una historia de la tecnología electoral en Estados Unidos, véase por ejemplo Jones y Simons (2012).

voto electrónico con selección por pantalla fue patentado en 1974 (McKay et al. 1974).

En Europa, la adopción temprana tuvo lugar en los Países Bajos y Bélgica; Alemania contó tempranamente con disposiciones legales habilitantes, pero el empleo de sistemas de voto electrónico no fue significativo hasta entrada la primera década del siglo XXI. Este impulso inicial, sin embargo, no parece haber logrado los alcances inicialmente imaginados. En 2015, tomando en cuenta hasta la última elección general en cada caso, los sistemas automatizados de emisión conocidos genéricamente como "voto electrónico" eran utilizados por la mayoría de los electores en solo cuatro países del mundo: Bélgica,[7] Brasil, la India y Venezuela. En los Estados Unidos es el segundo sistema más usado, después del basado en lectura óptica de boletas marcadas por el elector.

Mientras tanto, países que lo habían adoptado o realizado pruebas piloto fueron abandonándolo: los Países Bajos, donde la cantidad de votantes que utilizaban voto electrónico era superior al 90%, retornaron al voto en papel con cuenta manual en 2008, después de que se detectase fraude en las elecciones comunales de una pequeña localidad, de que la asociación civil *Wij vertrouwen stemcomputers niet* demostrase graves fallas de seguridad en el sistema empleado (Gonggrijp y Hengeveld 2007) y de que el tribunal superior de Amsterdam anulara en octubre de 2007 la certificación de las máquinas Nedap. Por su parte, el Tribunal Constitucional Federal alemán declaró la inconstitucionalidad del sistema de voto electrónico usado en ese país en 2009; el tribunal constitucional de Austria, donde se había llevado a cabo una elección experimental pero vinculante para la Federación de Estudiantes la declaró nula y fijó normas muy estrictas para futuros intentos; en enero de 2010 el Ministerio de Justicia de Finlandia comunicó que el gobierno de ese país

7 Ante la acumulación de fallas de seguridad y el costo desproporcionado, el parlamento valón solicitó al parlamento federal en 2015 la supresión del voto electrónico, y en 2016 decidió retornar al voto en papel para todas las elecciones futuras en la región valona (comunidades de habla francesa y alemana).

desistía de sus proyectos luego de que el Supremo Tribunal Administrativo (*Korkein hallinto- oikeu*) declarara nulas y ordenara rehacer por medios convencionales las elecciones en que se había experimentado en tres municipalidades en 2008; y, finalmente, la corte constitucional de Bulgaria declaró inconstitucionales ciertas provisiones del código electoral que autorizaban el uso del voto electrónico.

En Francia el uso de *machines à voter* fue autorizado por la ley 69-419 del 10 de mayo de 1969 modificatoria del Código Electoral. Las máquinas electromecánicas nunca se extendieron demasiado, y pronto cayeron en desuso, pero en 2002 una nueva ola de modernización llevó a instalar en forma experimental sistemas de voto electrónico en tres comunas, incrementándose progresivamente el número hasta 2007. La instalación de sistemas de voto electrónico se encuentra en moratoria de facto, porque desde finales de 2007 el Ministerio del Interior no ha dado nuevas autorizaciones a las comunas para incorporar este tipo de equipamiento, el uso ha disminuido desde su máximo de 82 comunas y 1,5 millones de electores en 2007 (5% del padrón electoral nacional) a 64 comunas y 1 millón de electores en 2012, y se han presentado varios proyectos de ley para su erradicación definitiva.[8]

Irlanda planeó introducir un sistema de voto electrónico para las elecciones de 2004 para lo que adquirió equipamiento entre 2002 y 2003, pero nunca llegó a efectivizarlo por resistencia de los electores e importantes sectores académicos, abandonando el proyecto en 2009 y finalmente destruyendo las máquinas en 2012; en Lituania las intenciones de la autoridad electoral para introducir voto electrónico han sido sistemáticamente rechazadas por el parlamento; Noruega realizó un estudio de factibilidad en 2006, una prueba piloto en diez municipalidades en 2010 y otra en 2013, para finalmente anunciar oficialmente el abandono de todas las pruebas en

8 En el caso francés, es interesante notar que las tasas de error en los sistemas de voto electrónico superan largamente las del voto manual, por un factor entre 5 y 7. Véase Enguehard (2012).

junio de 2014; el Reino Unido realizó varios pilotos entre 2000 y 2007, pero tomando en cuenta los resultados negativos en otros países y las críticas de la Comisión Electoral no se han hecho nuevos intentos desde entonces; y en noviembre de 2011 el gobierno de Kazajstán decidió abandonar el sistema Sailau que había iniciado en 2004, en razón de que la preferencia de los votantes por el papel, la desconfianza de los partidos y el costo.

Finalmente, en Paraguay, que venía adoptando gradualmente el sistema brasileño desde 2001 y que para 2006 había alcanzado prácticamente la cobertura completa del padrón electoral, el Tribunal Superior de Justicia Electoral dispuso el retorno al voto manual en papel en las elecciones generales de 2008.

Factores de adopción de los sistemas de voto electrónico

Sencillez del conteo. Los sistemas de voto electrónico se han introducido para hacer más simple la cuenta de votos y el cómputo de los resultados. Esta consideración es importante, pero solo se aplica a un número pequeño de elecciones complejas, basadas en preferencias (como el voto alternativo o el voto único transferible), o las que implican un gran número de categorías y cuestiones sometidas a referéndum,[9] y en ellas la cuenta manual puede requerir mucho tiempo y estar sujeta a error. No es el caso general de las elecciones en la Argentina, donde aún en el caso extremo de que coincidieran elecciones nacionales, provinciales y municipales

9 Elecciones en las que haya que decidir sobre más de una docena de cuestiones no son infrecuentes, por ejemplo, en los Estados Unidos. Las elecciones de 2006 en el condado de Marin, California, tenían 30 *races* con 98 candidatos en total más 30 decisiones plebiscitarias (*propositions*). En las elecciones parlamentarias holandesas, los votantes deben elegir entre cientos de candidatos. En Irlanda, Australia, Bosnia-Herzegovina y Taiwan se aplican sistemas de preferencia con transferencia de voto.

la convocatoria involucra a lo sumo ocho categorías, y no existen casos de voto preferencial o condicional.

Facilidad de emisión. La confusión puede efectivamente alterar el ejercicio del derecho al voto, especialmente cuando se trata de los electores más vulnerables (personas de edad, iletradas o con discapacidades). Las tecnologías de registro electrónico prometen reducir estos niveles haciendo imposibles los votos nulos y difíciles, los votos en blanco no intencionales. El Caltech/MIT Voting Technology Project ha argumentado que el empleo de tecnología puede reducir los votos "perdidos" en una variedad de formas, y la capacidad de generar interfaces más adecuadas puede potencialmente resolver problemas para personas con discapacidades o hablantes de lenguas minoritarias.

Sin embargo, al minimizar la posibilidad de algunos errores los sistemas de voto electrónico pueden incrementar la de otros. Es posible que los votantes no familiarizados con las computadoras no emitan ya votos nulos, pero pueden emitir votos que no reflejen adecuadamente sus preferencias; es posible también que la asistencia a los votantes iletrados o con discapacidades resulte confusa, errónea, insuficiente o inhabilitante, o que la interfaz genere nuevos problemas para personas con discapacidades que en un sistema manual podían emitir su voto sin inconvenientes.[10] La presunción de mayor *usabilidad*[11] no ha sido probada rigurosamente para la mayoría de los sistemas. Ni las autoridades electorales de la India ni las de Brasil, los países de uso más extenso del voto electrónico, han publicado estudios científicamente válidos de la interacción de los votantes con su tecnología. Sin estudios serios, es difícil establecer tanto la utilidad del voto

10 El caso más típico es el de personas con dificultades neuromotrices enfrentadas a una pantalla táctil.

11 Aplicamos aquí el término "usabilidad" en el sentido canónico en que lo define la Organización Internacional para la Normalización (ISO) en la norma iso 9241: la efectividad, eficiencia y satisfacción con que un usuario dado logra objetivos especificados en un ambiente particular.

electrónico cuanto la correcta aproximación a la educación de los votantes. La importancia de las pruebas de usabilidad de los sistemas es crucial, y en general se ha observado que, como en los casos testigo en la Argentina, no se realizan.[12]

Prevención del fraude. Las autoridades electorales frecuentemente han argumentado que las tecnologías electrónicas pueden combatir y hasta prevenir el fraude. Sin embargo, no existe evidencia convincente y sistemática sobre la veracidad de estas afirmaciones. Como señala Lehoucq (2003), los métodos de fraude son variados y complejos y la investigación científica sobre la cuestión, escasa. Algunas formas fraudulentas características de los sistemas de boleta partidaria, como el robo de papeletas o su sustitución, se revierten por mérito de la implantación de sistemas de boleta única, con independencia de la aplicación de tecnologías electrónicas. El "secuestro" de lugares de votación o el rellenado de urnas dependen de factores ajenos a la tecnología empleada. Más importante aún es el hecho de que los sistemas de voto electrónico crean nuevas y peligrosas posibilidades de fraude o de alegaciones de fraude que disminuyen sensiblemente la confianza en el sistema electoral. A diferencia de los sistemas convencionales, la opacidad de los sistemas de voto electrónico, su complejidad técnica y la de la logística asociada, y el efecto multiplicador de la replicación del software, tienen un triple efecto negativo: por un lado, la superficie de ataque al sistema se expande enormemente; por otro, los efectos de una intervención maliciosa o una falla accidental se multiplican a todos los lugares de votación de manera muy eficiente; y finalmente, el número de partes en colusión requeridas para una intervención maliciosa se reduce considerablemente, basta un solo programador malintencionado para introducir

12 Por otra parte, numerosos estudios de usabilidad proporcionan evidencia concluyente de nuevos problemas, entre ellos cómo la voluntad del votante puede ser influenciada por la interfaz en que realiza la selección y otros factores de entorno, y cómo determinadas formas de presentación afectan negativamente a los votantes de capacidades más limitadas y aun a aquellos sin aparentes limitaciones.

código que afecte la veracidad del resultado de una elección. Por otro lado, la generación de registros impresos comprobables visualmente por el elector no es eficaz para contrarrestar este riesgo, por razones que discutimos en otro apartado.

Reducción de costos. Con frecuencia se aduce que el voto electrónico reduce costos de administración electoral. Este argumento suena creíble por cuanto estamos acostumbrados a que el empleo de tecnologías de información aumenta la eficiencia de los procesos a los que se aplica y por lo tanto reduce costos en las actividades gubernamentales o del sector privado. Pero usualmente estas estimaciones se hacen en función de proyecciones de mediano y largo plazo, y no hay ningún estudio longitudinal que las confirme. En el caso del sistema adoptado para la Ciudad de Buenos Aires, se ha aducido que se generará una significativa economía relacionada con el costo de impresión y distribución de boletas partidarias, pero cabe notar que esta reducción es consecuencia de la implantación del sistema de boleta única y no de la automatización. Existen pocos estudios comparativos rigurosos entre los costos por voto emitido de boleta única en papel y su equivalente electrónico. Existen en cambio datos sobre el costo por elector de diversos sistemas electorales; reduciéndolos a una divisa común y actualizándolos, hallamos que para algunas democracias estables los valores son: Australia US$ 4,97, España US$ 5,14, solo la gestión electoral sin incluir el registro de electores, Suecia US$ 7,60. Comparativamente, hemos estimado el costo para la primera vuelta de las elecciones locales de 2015 del sistema escogido para la Ciudad de Buenos Aires en 80,36 pesos por voto emitido, lo que a la fecha de ajuste de la orden de pago respectiva equivalía a US$ 9,05, solo para las etapas de emisión y escrutinio y sin contemplar otros costos logísticos, como las compensaciones a las autoridades de mesa y a los delegados de la autoridad electoral.[13]

13 Nuestro cálculo se basa en el precio pactado ajustado por resolución 218/mjys-

Status. Un factor de adopción pocas veces considerado en la literatura es el del "prestigio tecnológico", una confusión de métodos y fines que supone que el uso de medios tecnológicos avanzados obra mágicamente para modernizar una democracia, o implica una aseveración sobre la modernidad de un gobierno o una autoridad electoral más que la solución a una necesidad específica. En la cadena de decisión y sustento del voto electrónico, puede ocurrir un fenómeno de introducción de error sistemático conocido como *sesgo cognitivo*, por la sobreapreciación de la tecnología: la fe en la tecnología puede enceguecer a los funcionarios públicos respecto de las cualidades negativas de las innovaciones, llevándolos a preferir una tecnología novedosa y compleja que puede ser inferior a una solución más antigua, más barata o más simple. Si la fe en la tecnología es un sesgo extendido y consistente entre los funcionarios públicos, será apropiado alentar una visión más pragmática, o aun pesimista, como contrapeso. Como mínimo, los decisores políticos generalmente proclives hacia la tecnología deberían intentar tomar esto explícitamente en cuenta cuando deciden respecto de la adopción de tecnología.

Riesgos de la adopción

La discusión precedente ha dejado en claro que muchas de las reivindicaciones sobre las ventajas de los sistemas de voto electrónico carecen de fundamento. Contra estas relativas ventajas, deben señalarse cuatro desventajas de mayor porte.

Daños a la confiabilidad y a la credibilidad. Todo programa informático puede tener errores no intencionales no detectados (bugs). Todo programa informático puede ser

gc/15 (Boletín Oficial de la Ciudad de Buenos Aires 4614: 40, 10 de abril 2015), el número estimado de votantes proyectado a partir del número en las primarias abiertas y con la tasa de incremento de las elecciones nacionales de 2013 en el distrito, y la cotización del dólar estadounidense para la fecha de publicación de la resolución referida.

cambiado en forma maliciosa en una forma indetectable *a posteriori*. Estas afirmaciones son verdaderas para cualquier software. Adicionalmente, toda computadora de propósitos generales (como las que normalmente constituyen la base de los sistemas de voto electrónico con pantalla táctil) es susceptible de explotación maliciosa, y la verificación del software en tiempo de ejecución es un problema de tal complejidad que su implementación resulta prohibitiva. Hay medidas que pueden reducir las vulnerabilidades de un sistema de voto electrónico, incluyendo la seguridad informática, la seguridad física, las pruebas y los análisis de los sistemas y el código,[14] y buenos procedimientos electorales; pero ninguno de estos pasos, y ninguna combinación de ellos, puede cambiar la irreductible vulnerabilidad de los sistemas informáticos. Un texto ya clásico de Ken Thompson (1984) alerta sobre la cuestión.

Esta vulnerabilidad implica que los resultados de una elección pueden ser manipulados, y también crea el peligro de que resultados legítimos de una elección no sean aceptados, porque es imposible refutar de manera concluyente las acusaciones de manipulación. En 2004, Venezuela tuvo un referéndum por la destitución presidencial. El entonces presidente Hugo Chávez se impuso cómodamente, con un 58% de los votos, y los observadores internacionales en general acordaron en que no se había observado fraude. Pero, considerando que el 90% de los votos había sido emitido a través de un nuevo sistema de voto electrónico, la oposición no estaba convencida, y con buenas razones: los observadores no pudieron certificar la confiabilidad de los sistemas de voto electrónico. El sistema venezolano emite un comprobante impreso verificable por el elector, pero la falta de procedimientos rigurosos de verificación y recuento hizo que la oposición no aceptara la veracidad de las verificaciones *ad hoc* llevadas a cabo después de la elección, e investigaciones

14 Las medidas sistémicas de defensa resultan, en principio, más eficaces que las aplicadas a nivel de programa.

estadísticas posteriores realizadas por académicos de Harvard y el MIT confirmaron la falta de confiabilidad del proceso. En general, los estudios indican que no puede descartarse en el caso la posibilidad de fraude (Martín 2011; Pericchi y Torres 2011).

Lo que se alegue sobre los resultados electorales basados en sistemas de voto electrónico puede corroer rápidamente la confianza en las elecciones, pues aquellos no pueden ser adecuadamente probados ni refutados. Una encuesta de *The New York Times* y CBS mostraba en 2006 que el 64% de los votantes demócratas y el 40% de los definidos independientes creía que en las elecciones presidenciales de 2004 en el estado se había cometido fraude.[15]

Se ha postulado que algunos de los problemas del voto electrónico pueden ser salvados empleando comprobantes verificables por el votante *vvpat o*, pues estos permitirían al votante confirmar sus preferencias en un medio permanente y recontable. Para ser efectivos, deberían cumplir con un conjunto de criterios: no comprometer el secreto del voto; ser legibles; estar insertos en un procedimiento que aliente a los votantes a confirmar su contenido; y ser parte de un proceso que prevea la realización de recuentos manuales extensivos sobre muestras al azar estadísticamente correctas después del escrutinio provisorio. Sin embargo, la utilidad de los comprobantes impresos como elemento de confirmación de la voluntad del elector es cuanto menos discutible, puede ayudar a convalidar resultados fraudulentos, y los impresos traen sus propios problemas, incluyendo la adición de más elementos propensos a fallar y la falsa sensación de certeza que pueden crear si no se establecen procedimientos claros sobre cómo emplear los comprobantes para determinar o verificar el resultado de la elección. Es significativo que la Dra. Rebecca Mercuri, quien desarrolló originalmente la idea, sostenga:

---

15 En 2004 George W. Bush ganó el estado de Ohio por un pequeño margen, y con ello su reelección como presidente.

> desde 2003, debido a los problemas irresolubles de implementación y despliegue de [estos] sistemas [...] y las dificultades experimentadas en usar los comprobantes para los recuento, he recomendado (y sigo recomendando) contra la adquisición de estos dispositivos. Los votos deben ser preparados en papel (no en computadoras) y contados del papel (preferentemente por humanos) (Mercuri, 2007).

La confianza de los votantes en el proceso electoral es fundamental en las democracias, porque las elecciones establecen un vínculo entre los ciudadanos y sus servidores públicos elegidos. Si los electores tienen dudas acerca de lo fidedigno del escrutinio, sentirán que los resultados no reflejan la voluntad expresada por la mayoría; esta duda socava el aspecto más fundamental de las democracias modernas: la elección de los representantes del pueblo soberano. La legitimidad de los individuos elegidos, y la de los cuerpos colegiados, se debilita cuando surgen estos cuestionamientos; esto puede llevar a minar las fortalezas del proceso democrático y de las instituciones. La mayoría de las democracias modernas ha tenido épocas de cuestionamiento del proceso electoral (Lehoucq 2002). En democracias consolidadas, puede suceder que sin haber pérdida de confianza en las elecciones la haya respecto de la tecnología usada. Es inevitable coincidir con McGaley y Gibson (2003):

> aparte del obvio requerimiento de que los votos sean computados correctamente, es vital que los votos se vean como computados correctamente. Un sistema de votación es solamente tan bueno como el público cree que lo sea.

Si bien los gobiernos, especialmente a partir de las décadas de 1980 y 1990, han tendido a confiar al sector privado la ejecución bajo contrato de algunas actividades relacionadas con las tecnologías de información, los procesos electorales son especiales por su significación y sus consecuencias, y no pueden ser completamente tercerizados a proveedores del sector privado (Xenakis y Macintosh 2005). Como señala

Lehoucq (2002), los estados latinoamericanos realizaron una gran contribución a la democracia constitucional con el surgimiento de autoridades electorales independientes de los poderes ejecutivo y legislativo, que incrementaron la confianza pública en las elecciones. Pero si estas entidades de control independientes pierden la capacidad efectiva de supervisar todos los detalles del proceso electoral, su rol de garantes de la transparencia ya no podrá ser cumplido cabalmente. ¿Cómo se comportará un contratista privado a cargo de un aspecto crítico de una elección cuyo resultado afecta sus intereses? Aun si se comportara con absoluta neutralidad, ¿cómo podrían aventarse las sospechas si la opción favorecida por el contratista resulta ganadora? Las fallas, accidentales o intencionales, de un sistema de voto electrónico tienen profundas consecuencias para la confiabilidad del sistema electoral y la confianza pública en él (Moynihan 2004).

Cabe señalar a manera de ejemplo que la adopción del sistema de voto electrónico de la Ciudad de Buenos Aires en 2015 parece compartir una característica común con un número de iniciativas de informatización electoral tomadas en otros lugares: aparenta haber sido conducido por posibilidades tecnológicas y conveniencia burocrática, en lugar de por una determinación de utilidad social democráticamente debatida.[16] Cuando aquellos criterios prevalecen, como sucede en muchos casos de *outsourcing* de aspectos importantes de actividades del sector público, la eficiencia choca con la obligación de rendir cuentas y socava los valores democráticos. Para acrecentar la transparencia de los procesos electorales hacia la ciudadanía, los partidos políticos y las propias autoridades electorales, es necesario que se incorporen las capacidades técnicas necesarias, mantengan el control, asuman plena responsabilidad y promuevan un rol activo de los ciudadanos en todos los procesos que llevan a la decisión

16 Se omitió, por ejemplo, la aprobación legislativa exigida por el artículo 25 del anexo II de la ley 4894.

sobre tecnologías electorales. La absoluta transparencia del sistema a utilizar es un indispensable primer paso.

Seguridad en los sistemas de información. En cualquier sistema de voto electrónico, tanto la experiencia como la teoría indican que una cosa es segura: el sistema contiene errores, y algunos de ellos son explotables por un adversario. Hasta el presente, todo sistema de voto electrónico sometido a análisis exhaustivo por especialistas en seguridad ha mostrado fallas, y sería una singularidad improbable que uno nuevo no las tuviera. Como sostiene Rivest (2008), la historia de los sistemas informáticos muestra que dados los incrementos e innovaciones en tecnología y velocidad, el software es capaz de hacer más cosas y en consecuencia su complejidad se acrecienta. La capacidad de demostrar que un software es correcto disminuye rápidamente a medida que el software se vuelve más complejo, y resulta efectivamente imposible probar adecuadamente los sistemas de votación actuales (y futuros) respecto de fallas y defectos inducidos, por lo que estos sistemas siempre serán sospechables respecto de su capacidad de procesar los votos con seguridad y exactitud.

Los análisis serios de seguridad requieren trabajo exhaustivo y especializado: el análisis del código fuente del software de las máquinas de voto electrónico Diebold AccuVote TS requirió de casi dos semanas a tiempo completo de cuatro notables expertos en seguridad informática. También es necesario notar que una inspección, por detallada que sea, no necesariamente encontrará todos los errores en un conjunto de programas, en algunos casos porque la técnica de ataque no es aún generalmente conocida. Ocultar de la vista pública los detalles es una muy mala práctica en términos de seguridad de la información, porque retrasa el ciclo de reparación de defectos y disminuye la confianza en el sistema o la reduce a un acto de fe incompatible con la certeza racional.

La problemática de seguridad de un sistema de voto electrónico debe ser vista desde la perspectiva general de la seguridad de la información, esto es, el cumplimiento de los atributos canónicos de confidencialidad, integridad y disponibilidad.[17] No obstante ello, la cuestión trasciende los límites puramente tecnológicos ya que, como señalan Oostveen y van den Besselaar (2004a; 2004b), "las complejas cuestiones técnicas relativas a la seguridad (...) deben ser respondidas antes de que los sistemas vayan a ser usados en elecciones gubernamentales de cualquier nivel", pero también deben tomarse en cuenta el entorno social y las consideraciones sociopolíticas, la percepción de la seguridad por parte del público, porque ya no existe una fe ciega en la objetividad científica y los "expertos".

Es necesario notar que desde el punto de vista de la seguridad informática, los sistemas de voto electrónico plantean problemas especiales, no solamente por las graves consecuencias institucionales de los resultados erróneos. En efecto, estos sistemas plantean la singular demanda de satisfacer simultáneamente tres condiciones que se contraponen: por un lado, que el elector pueda asegurarse de que su intención de voto ha sido correctamente computada; por otro, que no tenga forma de probar ante terceros cuál fue el contenido de su voto (porque ello da lugar a compra de votos o intimidación); y, finalmente, que se conserve perfecto anonimato para garantizar el secreto del sufragio. La inexistencia hasta el presente de modelos formales de seguridad de sistemas de voto que cubran efectivamente el amplio espectro de modelos de amenazas, ha llevado a plantear la noción de "sistemas independientes del software" (Rivest, 2008): un sistema de voto es "independiente del software" si un cambio o error no detectados en el software no pueden causar un cambio o error

17 Cfr. ISO/IEC 27000:2009 (E). Information technology – Security techniques – Information security management systems – Overview and vocabulary. Ginebra: International Organization for Standardization e International Electrotechnical Commission.

no detectables en el resultado de la elección. De ello surge el marco teórico de "verificabilidad de extremo a extremo" (*end-to-end verifiability*) (Benaloh et al., 2015); pero si bien este marco es formalmente correcto, se ha probado que los sistemas que lo implementan tienen graves problemas de usabilidad que conducen a bajos porcentajes de éxito en la emisión y la verificación del voto.

Como se ha expuesto más arriba, todo sistema informático es suceptible de error o de intervención maliciosa. La notable complejidad del conjunto presenta una enorme superficie vulnerable: aun cuando pudiera obtenerse un razonable grado de aseguramiento respecto del software de aplicación empleado, por debajo de este yacen numerosas capas de software y hardware, cada una de ellas sujeta a problemas de seguridad. Los sistemas de voto electrónico son particularmente frágiles: ninguno ha sido formalmente verificado, y todos los que han sido sometidos a análisis exhaustivo por expertos independientes han mostrado fallas explotables por adversarios, como el de Brasil (Aranha et al. 2014) o el de la India (Wolchok et al. 2010). Incluso análisis fragmentarios han hallado fallas muy graves, como en el caso del sistema Vot.ar utilizado en la Ciudad de Buenos Aires y en Salta.

Las cuestiones centrales de seguridad radican en la preservación de la integridad y el secreto del voto. Cuando se utilizan sistemas de registro directo electrónico sin ningún comprobante verificable por el elector, el logro de estas condiciones es imposible de demostrar. Para la primera cuestión, como señalábamos más arriba, se ha intentado generar un elemento que el elector pueda verificar por sí mismo. Sin embargo, la observación empírica y el resultado de pruebas controladas proporcionan amplia evidencia de que la mayoría de los electores generalmente no verifican los comprobantes impresos (ni siquiera cuando ese control es un paso indispensable para completar la transacción) y, cuando los controlan, de todos modos se deslizan altas tasas de error. En un experimento, Everett (2007) halla que más del 60% de los votantes no detecta los errores introducidos (algunos

de ellos muy burdos, como la supresión de una categoría completa). Campbell y Byrne (2009) repiten el experimento de Everett mejorando la capacitación de los votantes y la usabilidad de la interfaz de pantalla, pero tampoco logran mejorar los niveles de detección más allá del 50%. La baja detección de error se atribuye a la disonancia perceptiva entre la información presentada en pantalla respecto de la registrada en un medio impreso. El bajo nivel de reporte, inferior en todos los casos a lo detectado, corresponde a un fenómeno bien estudiado: la atribución de "credibilidad" a las computadoras; por lo tanto los errores no pueden ser sino del elector, que se siente avergonzado de reconocerlos. Cabe agregar, por otra parte, que el texto legible no dice nada respecto de los datos almacenados en la memoria, que son los que se utilizarán para el conteo. Además los comprobantes generados producen dificultades cuando debe realizarse un recuento manual, con tasas de error mucho mayores a las de las boletas completadas a mano por el votante (Goggin et al. 2008).

La preservación del secreto es un problema aún más serio. El uso de cualquier identificador único (como el número de serie de los dispositivos RFID del sistema usado en 2015 en Salta y la Ciudad de Buenos Aires) deja abierta la posibilidad de asociarla con el votante individual.

No es objeto de este trabajo hacer una enumeración de las posibles fallas de seguridad, que requeriría mucha mayor extensión y sería necesariamente provisional. Pero es necesario dejar en claro que los sistemas de voto electrónico son particularmente frágiles ante amenazas internas (*insider threat*) y que el medio informatizado permite una escala de ataques inimaginable con medios convencionales.

Obstáculos en los procesos de implantación y despliegue. Aun si se lograran en el software de los sistemas de voto informatizado niveles de seguridad comparables con los de los mecanismos convencionales, el aseguramiento de todos los procesos involucrados en la elección es pieza clave de su

fiabilidad. Uno de los problemas más difíciles de resolver es el de la complejidad de la cadena de suministro, porque una falla accidental o inducida en cualquiera de los pasos se propaga hasta el resultado final. En general, hay una marcada insuficiencia en los procedimientos establecidos por la autoridad electoral que eleva los riesgos. Por ejemplo, no suelen establecerse correctamente mecanismos para asegurar efectivamente que la versión del software a ejecutar durante la elección se corresponde con una versión previamente verificada, un problema que por cierto presenta dificultades extremas. Tampoco suele haber mecanismos para asegurar que el hardware se corresponde exactamente con algún modelo de referencia exhaustivamente verificado, ni se prevén acciones de verificación independiente y control por oposición, y la logística de distribución suele ser débil y susceptible de ataques internos y externos.

Adicionalmente, se requiere establecer procedimientos de control de conteo que permitan validar, mediante una muestra estadísticamente significativa, los resultados del escrutinio provisorio realizado mediante medios electrónicos.

II. ¿Quién supervisa la elección?

La perspectiva tecnicista. Algunas lógicas de empleo del voto electrónico suponen como inevitable el desplazamiento de la capacidad de control sobre los procesos electorales. Así, la mediación informatizada de aspectos críticos de una elección no habría de verse de modo diferente al empleo de computadoras en otras actividades que también revisten importancia significativa para las personas. En esta aproximación ingenieril, la cuestión no sería diferente de otras en que los usuarios carecen de información de detalle sobre el funcionamiento real del sistema, y no tienen sobre él capacidades de supervisión inmediata pero depositan confianza en procesos de control llevados a cabo por terceros; característicamente, se ha equiparado esta cuestión a los procesos informatizados bancarios.

En los sistemas bancarios (donde además aparece la analogía entre los dispositivos de emisión del voto y los cajeros automáticos), en los sistemas electorales, o en cualquier otro entorno informatizado, la auditoría previa y posterior constituye, entonces, un factor decisivo para la fiabilidad. Pero este recurso queda fuera del alcance de los usuarios, que carecen de los saberes requeridos; y tampoco los necesitarían, pues su intervención es irrelevante en tanto su confianza no debería basarse en el conocimiento de los detalles técnicos sino en la convicción de que el conjunto de medidas procedimentales adoptadas incluye las salvaguardas necesarias. En este sentido, no habría diferencia con otros productos industriales sometidos a procesos de certificación; aunque en la mayoría de los casos los resultados de estos procesos solo serán conocidos por la autoridad electoral y la empresa proveedora.

Pero es fundamental señalar que las elecciones presentan notables diferencias con otras áreas de uso de la informática. Una de las diferencias centrales es expresada sintéticamente por Richard M. Stallman: "el software de las máquinas de votación es un caso especial porque el mayor peligro para la seguridad proviene de la gente que se supone sea responsable por ella" (citado en Anderson 2010, 707).

La comparación con los sistemas bancarios es falaz (Loeber 2008): en primer lugar, en estos no hay necesidad de una obligación pública de rendir cuentas y basta con una auditoría independiente. En las elecciones, en cambio, cada votante debería ser capaz de verificar que el sistema funciona correctamente, porque si esto no fuera posible la confianza en las elecciones, y por ende la confianza en los representantes elegidos, declinaría. Por otra parte, en los sistemas de banca electrónica un banco puede permitirse cada tanto un problema menor en el sistema; los errores causados por estos problemas pueden ser enmendados sin mayores consecuencias, y con buena probabilidad serán detectados porque los titulares de cuentas pueden verificar sus extractos, y la mayoría lo hace. En las elecciones no hay

posibilidad de enmienda, y cualquier error menor, aun si se lo detecta, puede tener un impacto significativo sobre la cuestión de quien ejercerá la representación popular por los próximos cuatro años. Una pequeña cantidad de estos errores y la confianza se disolverá en el aire, con consecuencias desastrosas.

La perspectiva de las garantías fundamentales. Hay, sin embargo, una significativa línea de pensamiento que advierte que las condiciones fundamentales del proceso electoral deben preservarse con independencia del empleo de recursos tecnológicos. En ese sentido, el Tribunal Constitucional Federal de Alemania (BVerfG) resolvió favorablemente en 2009 una impugnación sobre el uso de sistemas de voto electrónico,[18] declarando inconstitucional la Ordenanza Federal sobre Máquinas de Votación (*Bundeswahlgeräteverordnung*) de 3 de septiembre de 1975 en su versión modificada por la Ordenanza Modificatoria del 20 de abril de 1999 (*Verordnung zur Änderung der Bundeswahlgeräteverordnung und der Europawahlordnung*). El valor teórico de esta resolución se acrecienta si tenemos en cuenta las similitudes de marco constitucional. El fallo establece dos principios esenciales: las elecciones como acto público (*principio de publicidad*),[19] y el derecho del elector a comprender todos los pasos esenciales de la elección y el escrutinio sin conocimiento experto (*principio de entendimiento*).

---

18 Bundesverfassungsgericht. 2009. Leitsätze zum Urteil des Zweiten Senats vom 3. März 2009 – 2 BvC 3/07, 2 BvC 4/07. (Sentencia del Segundo Senado del 3 de marzo de 2009) ECLI:DE:BVerfG:2009:cs20090303.2bvc000307

19 Siendo un acto fundacional de lo público, es inevitable que esto sea así. Si todos los actos de gobierno son públicos, con más razón son públicos los únicos actos de los que emana la legitimidad de ese gobierno. Esta característica ineludible de las elecciones no colisiona con el secreto del voto de cada elector, porque el secreto del sufragio individual no es un elemento constitutivo del derecho a votar, sino una garantía, ciertamente indispensable, de que la expresión de la ciudadanía no estará sujeta a ninguna forma de coerción.

Respecto del primer principio, el alto tribunal halla que

> La publicidad de las elecciones es condición fundamental para la construcción de una voluntad política democrática. Asegura la regularidad y transparencia del proceso electoral y se configura, con ello, como condición esencial para una confianza fundamentada de los ciudadanos en el correcto desarrollo de la elección. (§ 106)

Aunque la exigencia no esté expresada directamente en el texto de la Ley Fundamental (*Grundgesetz für die Bundesrepublik Deutschland - GG*), la interpretación sistemática de los artículos 38 y 20.2 asegura que se trata de un principio irrenunciable. El primer artículo refiere a las elecciones del parlamento (*Bundestag*) y menciona las características del sufragio (libre, universal, igual, directo y secreto), mientras que el segundo proclama el origen popular de los poderes públicos. Compárese el primero con los artículos 37 de la Constitución Nacional, lo prescripto por los tratados de derechos humanos de jerarquía constitucional conforme al artículo 75 inc. 22 de la CN (artículo 21.3 de la Declaración Universal de Derechos Humanos, artículo 25.b del Pacto Internacional de Derechos Civiles y Políticos, artículo 23.1.b de la Convención Americana sobre Derechos Humanos); y el segundo con el principio de la soberanía del pueblo del 32 CN. La exigencia de publicidad no es expresa en la norma constitucional alemana, pero el tribunal llega a la necesaria conclusión de que solamente las elecciones públicas son garantía de la legitimidad democrática de los representantes del pueblo.

Ahora bien, de ese carácter público sigue necesariamente el segundo principio:

> En una república, las elecciones son cuestión de todo el pueblo y preocupación común de todos los ciudadanos. En consecuencia, el control del procedimiento electoral también debe ser cuestión y deber del ciudadano. Cada ciudadano ha de poder seguir y entender de forma fiable las etapas centrales de la elección sin conocimientos técnicos especiales. (§ 109)

> El votante por sí mismo debe ser capaz de verificar –también sin un conocimiento informático detallado– si su voto es registrado fielmente como base para el conteo o, si los votos son inicialmente contados con ayuda tecnológica, cuando menos como base para un subsiguiente recuento. No es suficiente si debe confiar en la funcionalidad de un sistema sin posibilidad de inspección personal. (§ 119)

> La naturaleza pública de las elecciones requiere, en el despliegue de máquinas de votar controladas por computadora, que los pasos esenciales del acto electoral y la certeza de los resultados puedan ser revisados confiablemente y sin conocimiento experto especial. (§ 146)

Esta capacidad de observar y controlar no debe entenderse meramente como la garantía del acto físico de visualizar, sino que exige que el proceso electoral sea completamente inteligible para todos los involucrados, y en particular para los titulares del derecho al sufragio activo. En el caso del voto electrónico, las consecuencias de este principio adquieren particular relevancia porque no hay una garantía de comprensión plena de las acciones por más que estas se produzcan en público.

Cierto es que el uso de sistemas de voto electrónico puede ir acompañado de cautelas compensatorias, como por ejemplo las certificaciones del equipamiento o auditorías informáticas previas, pero nada de esto puede justificar que el resultado final sea un proceso incomprensible, y por lo tanto incontrolable, por los ciudadanos:

> Las limitaciones sobre el control ciudadano del proceso electoral no se pueden compensar a través de prototipos en el contexto del proceso de homologación, ni en la selección de máquinas de votar que, antes de su uso en una elección concreta, hayan sido examinadas por una institución oficial y evaluadas conformes a determinadas exigencias de seguridad y de integridad técnica. El control de las fases esenciales de la elección solo promueve fundada confianza sobre la regularidad de la elección si se

> ofrece de tal forma que los ciudadanos puedan seguir por ellos mismos el proceso electoral de manera fiable. (§ 123)

El tribunal refiere, a título de ejemplo, algunas de estas medidas compensatorias técnicas u organizativas que no ofrecen contrapeso suficiente a la perdida de capacidad de supervisión ciudadana. Entre ellas menciona el monitoreo constante y salvaguarda de los dispositivos, la comparación en cualquier momento de los dispositivos utilizables contra una muestra oficialmente verificada, y la responsabilidad penal respecto del fraude electoral (§ 124). Menciona también la participación de todo el público interesado en los procesos de examen o aprobación de los dispositivos, la publicación de informes de examen o del código fuente (§ 125), y señala que

> Los exámenes técnicos y los procedimientos oficiales de aprobación, que en cualquier caso solo pueden ser evaluados de manera experta por especialistas interesados, se relacionan con una etapa del procedimiento que precede por mucho a la elección. (§ 125)

En síntesis, la supervisión basada en el conocimiento del votante sin que requiera asistencia experta es insustituible.

La sentencia señala que solo es posible admitir excepciones a estos principios cuando se justifiquen en función de la protección de otras garantías constitucionales; pero no encuentra que haya principios constitucionales opuestos que ameriten menoscabar los de carácter público y de supervisión con plena comprensión para el caso de máquinas de votación controladas por computadora (§ 126). Destaca además que ciertos justificativos usuales para la adopción de sistemas de voto electrónico, como la disminución de los errores involuntarios del votante (votos nulos o que llevan a interpretación incorrecta de la voluntad del elector, § 127), los errores aritméticos del escrutinio provisional (*íd.*), o la rapidez en la disponibilidad de los resultados (§ 130), no son argumentos de valor para abandonar, siquiera parcialmente, los principios fundamentales.

El Tribunal Constitucional Alemán reafirma, profundiza y precisa un principio ya establecido en la Recomendación REC(2004)11 del Consejo de Europa (2005): la obligación de los estados de garantizar que los votantes "entienden el sistema de voto electrónico y tienen confianza en él" (anexo 1, § 20) y la disponibilidad pública general de "información sobre el *funcionamiento* del sistema" (íd. §21, el destacado es nuestro). Si bien estos términos pueden tener interpretaciones diversas, el Memorándum Explicativo de la recomendación se encarga de precisarlos: "la plena comprensión del sistema de voto electrónico es la base" de la confianza (§ 55) y recuerda, como señalábamos más arriba, que

> los métodos de votación tradicionales son simples y han sido bien probados y ensayados... (l)os votantes están familiarizados con los sistemas de sufragio que usan papeletas y urnas y entienden las reglas generales que gobiernan cómo deben votar y cómo su voto es recogido y contado sin alteraciones (§ 56).

Conforme al fallo analizado, entonces, si bien el uso de recursos informatizados en la emisión del voto no es inconstitucional *per se*, ningún sistema de esa especie está exento de garantizar los principios fundamentales de publicidad y comprensión.

III. A modo de conclusión

Este brevísimo recorrido plantea entonces tres niveles de objeción al voto electrónico. En primer lugar, el razonamiento del *Bundesverfassungsgericht* alemán, perfectamente aplicable en nuestro entorno constitucional: el imperativo de que el votante pueda asegurarse por sí mismo y sin necesidad de recurrir a ayuda experta que su voto expresa correctamente su voluntad, y que se registra y cuenta debidamente. Ahora bien, el correcto entendimiento de esta exigencia plantea un problema irresoluble en el actual estado de la ciencia

informática. En segundo plano, se hallan las objeciones técnicas en sí: no es posible construir un sistema seguro que proporcione esas garantías, y aun cuando fuera admisible un ligero menoscabo de ellas, el sistema resultante presentaría serios problemas de usabilidad. Finalmente, los procedimientos necesarios para asegurar un correcto despliegue son extremadamente gravosos.

A las presuntas ventajas de mayor celeridad y exactitud en el conteo, se oponen problemas de tal magnitud que hacen desaconsejable la implantación de cualquier sistema de voto electrónico. Si bien se reconocen problemas en el sistema electoral vigente, no existe razón para suponer que estos no puedan ser resueltos por medios más eficientes. Debería ser un llamado de atención que, cuarenta años después de los primeros ensayos, los sistemas de voto electrónico en el mundo no han ganado impulso sino que, por el contrario, muchas democracias desarrolladas han decidido no adoptarlo, y en algunos casos rechazarlo después de haberlo empleado de modo significativo.

3.
exposiciones sobre el voto electrónico

Plenario de Comisiones
en Cámara de Diputados
04 de agosto de 2016

En este apartado, se transcriben las intervenciones de distintos especialistas que se oponen a la implementación del voto electrónico y que expresaron sus argumentos en el Plenario de Comisiones de Asuntos Institucionales; Justicia; Presupuesto y Hacienda en la Honorable Cámara de Diputados de la Nación. En las transcripciones se modifican algunas expresiones y repeticiones propias del habla oral para lograr una mayor cohesión en el texto escrito.
Recomendamos, también, observar los videos en Youtube de cada participación ya que en ellos se podrán escuchar, además del discurso, algunas preguntas realizadas a los expositores. Se pueden escanear los códigos QR correspondientes para acceder a las grabaciones en la Cámara de Diputados.

"En el proyecto de ley sobre voto electrónico, hay aspectos contradictorios"

Daniel Penazzi

Mi nombre es Daniel Penazzi, soy Doctor en Matemática con el título en la Universidad de Minnesota y Licenciado en Matemática y en este momento soy profesor en la Universidad Nacional de Córdoba en la Facultad de Matemática, Astronomía, Física y Computación. Si bien mi título es de matemática, justamente como hay computación desde hace 17 años enseño esta materia. Me he dedicado a la criptografía y tengo dos *papers* publicados en voto electrónico. Como el tiempo es poco le voy a dar una pequeñísima clase de cómo son los sistemas de voto electrónico en general.

Hay sistemas de voto electrónico que usualmente se llaman *sistemas* DRE, que significa en inglés *direct recording electronic machines*, en donde los actos de generar el voto y de contarlo están en el misma máquina. Esos sistemas pueden o no tener un registro en papel y son muy peligrosos. Quince años o más de ataques demostraron que estos sistemas no deben usarse.

Otro sistema alternativo llamado *sistema IRE* por *indirect recording electronic voting machines* intenta imitar lo que uno hace cuando vota a mano. Es decir, el votante genera un voto, ese voto se deposita de alguna forma, se plasma en algún objeto físico y ese objeto físico se deposita en una urna en donde se anonimiza y, luego, se cuenta aparte. Esos sistemas son muchos más seguros que los sistemas de DRE con o sin papel.

Acá el problema no es que haya un registro en papel –porque, por ejemplo, en Venezuela tienen un registro en papel–, tener un registro en papel solo ataca el problema de integridad y de verificabilidad. Los DRE son peligrosos por otro problema: vulneran el secreto del voto. ¿Por qué vulneran el secreto del voto? Porque dado que la misma máquina que genera cuenta, el votante por su parte no puede saber si su voto no va a ser revelado de alguna forma. Entonces los sistemas IRE son mejores pero eso no significa que no se puedan hacer mal.

Lo que yo quería aclarar es que en este proyecto de ley hay aspectos contradictorios. En el articulo 15, por ejemplo, en donde se define lo que es sistema de emisión de sufragio con boleta electrónica, lo que se está definiendo es un sistema DRE con papel. Sin embargo, en los artículos 31, 33, 37 y 38 lo que se está definiendo es un sistema IRE. O sea en la misma ley se contradice. Obviamente los que hicieron este proyecto están pensando en un sistema parecido al de MSA [Magic Software Argentina], o sea un sistema IRE. La diferencia entre esos dos sistemas no consiste en que haya un registro en papel sino que en el sistema IRE no debe quedar ningún registro en la máquina que genera el voto de lo que el votante voto.

En este sentido, por más que digamos "bueno, vamos a corregir el artículo 15 porque está medio mal escrito, para tratar de reflejar lo que dicen el 31, 33, 37 y 38" no es suficiente, sigue faltando precisión. Debe estar explícito que el sistema que genera el voto no guarda ningún registro, porque si no ocurren situaciones como en Brasil. Hace poco, Brasil fue "hackeado" por un investigador llamado Diego Aranha, quien reveló que, por una mala implementación de algoritmos

criptográficos, se puede conocer quién voto a qué candidato, es decir, conocer todo el orden de las votaciones de los votantes, cliqueando en qué momento voto y saber qué voto.

Entonces es importante que estos aspectos cambien en esta ley. Por supuesto que mejor sería no proponer un sistema de voto electrónico. Como mucha gente ha dicho, el sistema de boleta única en papel contada a mano es mucho mejor desde el punto de vista de seguridad que este sistema. Y si lo que quieren es rapidez, están los sistemas electrónicos que pueden utilizarse en el conteo solamente. Es decir, uno genera el voto a mano, con lo cual resuelve todos los problemas de seguridad que hay en los sistemas de generación de votos electrónicos y luego sí, se cuenta electrónicamente y por supuesto hay que tener una auditoría post-elección como está señalado en el artículo 111 bis. Pero ahí lo que uno hace es aislar los dos problemas.

El mayor problema de seguridad está en la generación del voto porque la máquina está en contacto con la persona que está votando y existe un derecho fundamental, un derecho del votante. Este derecho no es solo que el voto sea secreto, sino que el ciudadano sepa por su cuenta que el voto no está siendo revelado. En el sistema propuesto por MSA y en la ley no queda claro que se le ofrezca esa garantía al votante. Hay métodos propuestos por bibliografía específica, aunque no todos el 100% seguros, para intentar que el votante tenga alguna seguridad por su cuenta, sin tener que depender del personal de la compañía ni de los que van a auditar el voto. En cambio, en la ley, la redacción de los artículos 31, 33, 37 y 38 no parecería dejar lugar a ese tipo de sistemas.

Igual, si bien hay sugerencias en la bibliografía específica sobre el voto electrónico es bastante costoso –en términos de dinero– y posiblemente tiene otros problemas, así que en general quizá de acá a un par de años se puedan hacer. Yo no las recomendaría. Por ejemplo, muchos de esos sistemas usan criptografía como la encriptación homomórfica, *zero knowledge proof*, y un montón de otras cosas que sería difícil explicárselas al común de la gente.

Es decir, por más que uno pueda diseñar un sistema que, en abstracto, sea bueno, explicárselo a millones de personas no va a ser fácil. En este sentido, la International Association for Criptological Research (IACR) tiene un sistema de voto no solo electrónico sino a distancia y lo usan. Pero ellos mismos dicen: "esto sirve para nosotros que somos criptógrafos y sabemos los que estamos haciendo, este no es un sistema que se pueda adaptar masivamente". Entonces, aun cuando se pudiera de forma técnica resolver estos problemas que menciono, siempre quedaría el problema de cómo explicárselo a millones de personas. Por eso, en general, lo que la gente recomienda por ahora es o todo manual o por lo menos que la generación del voto sea manual y si después se quiere hacer un conteo electrónico se hace.

Para terminar, me gustaría hacer una pequeña analogía: hay gente que se opone a las centrales nucleares y gente que está a favor de las centrales nucleares. Y en general uno hace un análisis de costo, riesgo y beneficios y estará de un lado o de otro. Pero aun la gente que está a favor de las centrales nucleares no tiene la locura de diseñar una central nuclear como si fuera una central termoeléctrica común. Muchos de los que estamos acá hacemos la relación costo, riesgo y beneficios del voto electrónico y concluimos: mejor no, mejor quedarnos con el papel. Algunos de ustedes por ahí dicen que les parece que la ecuación da por el lado de los beneficios, bien. Ustedes son los legisladores y si ustedes quieren adoptar el voto electrónico, bien, pero por lo menos diséñenlo bien. No dejen todos estos huecos que hay acá porque va a ser un desastre.

Muchos me dijeron "bueno, pero hay que demostrar…"; no, no hay que demostrar nada. Nosotros no tenemos que demostrar nada. La persona o compañía que introduzca el sistema, que proponga el sistema, ellos tienen que dar una serie de afirmaciones de seguridad y demostrar que esas afirmaciones se cumplen. No estoy diciendo que prueben que el sistema es 100% seguro. Si dicen que la máquina que genera el voto no tiene ningún registro, que lo digan explícitamente;

y si, luego, se verifica que sí tiene un registro que lo guarda, tiene que haber penalidades, así como hay penalidades para el que se mete y vulnera el sistema. Tiene que haber sanciones penales y no solo económicas para el que dice que está prestando un sistema que no tiene ciertas características y después resulta que tiene vulnerabilidades.

El votante, como dije antes, tiene su derecho fundamental de saber que su secreto no será revelado y para que les quede otra analogía: el sistema debe ser tal que el votante piense "esta máquina con la que voy a interactuar para producir el voto, es mi enemiga, no mi amiga". Y sin embargo el protocolo que me están dando para que yo vote me permite burlarla y ganarla. Si no tiene eso, como no lo tiene esta ley y como no lo tiene el sistema de MSA, es un problema grave. Finalmente otra analogía: uno no construye un puente y dice: "Mire, el puente es seguro, ya pasó una semana y no se cayó ningún auto". La gente que construye puentes hace cálculos y demuestra que el puente está bien construido. Nada más. Gracias.

Para observar el video de la exposición de Daniel Penazzi, lea el código o acceda a esta página web: https://www.youtube.com/watch?v=m4iB1dgMZ34

“Hay que verificar, garantizar y demostrar matemáticamente que el sistema cumple con esas propiedades”

Iván Arce

Gracias por la invitación a todas las autoridades, a los diputados, a la comisión. Voy a tratar de ser lo más rápido posible, es difícil ser rápido, hablar en diez minutos de seguridad, TIC y voto electrónico. Yo me dedico a la seguridad TIC, lo he hecho los últimos veinte años en el sector público, en el sector privado, con la comunidad académica, con la comunidad de practicantes, en el ámbito nacional y en el internacional. Trabajé dieciséis años en el sector privado en una empresa de seguridad informática, trabajo actualmente en la Fundación Sadosky coordinando un programa de seguridad en TIC. Además, fui editor doce años de la revista *IEEE Seguridad y privacidad*. IEEE es una asociación profesional de ingenieros, electrónicos y electricistas, es una de las dos más importantes del mundo en la materia. Finalmente, soy fundador del Centro para el Diseño del Software Seguro de IEEE. Dicho todo esto aclaro que mis comentarios y observaciones son a título personal, ninguna de todas las instituciones que

mencioné fueron consultadas o participaron en el proyecto. Hablo en calidad de experto a título personal.

Voy a tratar de hacer referencia o tomar algunos puntos de algunos oradores anteriores que hablaron de cosas de las que yo tenía previsto hablar, empezando por lo que dijo la Dra. Tula cuando hablaba de los tres principios rectores que uno debería esperar del voto electrónico que están de hecho enunciados en el artículo 1 del proyecto de ley. Ella hablaba de integridad, auditabilidad y secreto como principios rectores, eso cuando se habla en un sistema informático se tiene que traducir a propiedades del sistema. Una cosa es hablar de estas cosas como principios o cosas que son deseables y otra cosa distinta es que un sistema tenga esas propiedades y se pueda garantizar que esas propiedades se cumplen y el sistema las brinda. Para garantizar esto a lo que se recurre generalmente en la ciencia de la computación es a la matemática. Hay que verificar, garantizar y demostrar matemáticamente que el sistema cumple con esas propiedades.

Enrique Chaparro suele hacer mención de un teorema del 2009 que precisamente te muestra matemáticamente que no se puede construir un sistema que satisfaga simultáneamente esas tres propiedades. Eso no es el fin del mundo y ahora les voy a explicar por qué pero la conclusión es que hay una demostración matemática que señala que no se puede construir un sistema que simultáneamente satisfaga las tres características –integridad, auditabilidad y secreto– al mismo tiempo. Ahora bien, es una demostración matemática, por lo que dista de la implementación práctica.

La seguridad en las tecnologías de información y comunicaciones trata de manejar el riesgo de sistemas tecnológicos imperfectos –no perfectos y demostrados matemáticamente que lo son, sino sistemas tecnológicos imperfectos en presencia de ataques o de adversarios. Eso es a lo que yo me dedico y ahí hay que hacer una nueva salvedad que es el tema de la presencia de los adversarios. La seguridad en TIC estudia los sistemas informáticos y tecnológicos desde el punto de vista no de los fenómenos naturales sino de la presencia de

actores, adversarios, con capacidades, es decir, agentes inteligentes que tienen recursos, tienen conocimientos y tienen incentivos o desincentivos y capacidad de acción variada. Hay que caracterizar correctamente cuál es el adversario.

En el contexto de un sistema electoral el adversario va desde un entusiasta de la informática que tiene intenciones de causar problemas o curiosidad, hasta una o varias agencias de inteligencia estatales nacionales o extranjeras. En el medio hay una gran variedad de potenciales adversarios. Las organizaciones delictivas nacionales e internacionales, el proveedor del sistema y toda su cadena de abastecimiento deben ser considerados como un potencial adversario; un grupo de activistas, un tipo como yo que sabe de informática y de seguridad o un conjunto de personas como yo que quieren hacer algo dañino también. Es por lo tanto necesario caracterizar a los adversarios adecuadamente y diseñar los sistemas para prevenir amenazas identificadas de cualquiera de estos. Hay que determinar cuál es el nivel de riesgo que uno quiere asumir en el uso de un sistema que, como dije, es imperfecto. Y hacerlo explícitamente. El proyecto de ley que estamos tratando habla de la seguridad en el artículo 1, enunciando principios, pero no habla de cuestiones precisas en todo el resto del proyecto. Por lo tanto deja un margen muy amplio, muy abierto a que puedan suceder cualquier tipo de cosas ya sean malas o buenas. En principio eso es preocupante porque lo que sucede generalmente en la práctica no es bueno, no es la situación ideal sino todo lo contrario.

Se ha mencionado en este debate el tema de la auditoría y de los plazos, particularmente si no me equivoco esto figura en el artículo 15 del proyecto y frente a eso tengo que hacer algunos comentarios. El primero y principal es que los plazos previstos en el artículo 15 hablan de la auditoría, de los 120 días anteriores a la elección, pero lo que hay que considerar desde el punto de vista de la seguridad informática o seguridad TIC, es todo el proceso de un sistema de desarrollo electoral. Desde su concepción, diseño, implementación, prueba en laboratorio, prueba de campo, puesta

en funcionamiento, mantenimiento en la elección y lo que sucede después. En el mundo de la seguridad informática, la seguridad de software, no es suficiente hacer la auditoría de artefactos, de códigos de programas sino que hay que tener una idea de las prácticas empleadas y las actividades. Hay un conjunto de prácticas conocidas tendientes a minimizar el riesgo durante todo el ciclo de vida de desarrollo de los sistemas tecnológicos y todos esos rasgos deben ser tenidos en cuenta a fin de minimizar el riesgo de seguridad en un sistema de esta naturaleza.

Independientemente de esto que les cuento, una auditoría de veinte días es insuficiente para lo que se está tratando y me podrían preguntar cuántos días son suficientes. La respuesta a eso sería: no les puedo decir porque no se cuál es el sistema, qué grado de complejidad tiene, cuáles son los componentes que usa, cuáles son los proveedores del proveedor y cuál es la práctica o la madurez en términos de seguridad que tiene cada uno de ellos. Solo es posible determinar cuáles son las necesidades de auditoría cuando se tiene alguna especificación o alguna indicación concreta sobre qué es lo que se quiere auditar. Así que creo que eso es algo que se debería considerar. Se debería considerar también quien determinaría esto. Porque evidentemente no se puede determinar en una ley de antemano y posiblemente no se puede determinar en una reglamentación tampoco, hay que considerarlo de una manera un poco más precisa.

El Dr. Tullio hablaba de las diferencias entre, si no me equivoco, auditoría y homologación. Sugiero retirar la palabra *homologación*. Se podría reemplazar por *certificación*. Tanto una certificación como una homologación se hacen respecto a algún criterio preestablecido de antemano. Y es muy difícil definir criterios de antemano. La autoridad de asistencia electoral en los Estados Unidos se tomó cinco años para definir los criterios de homologación de sistemas electorales tecnológicos, con dos periodos de 120 días abiertos a comentarios y sugerencias del público en general.

Para terminar, aunque tengo muchos más comentarios para hacer, me voy a enfocar en uno que me parece fundamental y que es un tanto preocupante en el proyecto de ley. Me refiero a los artículos 59 y 60. En el 60 se crea el *delito informático electoral*; el 59 habla de otros delitos. En ellos se mencionan cosas o prácticas que son frecuentes en la investigación y desarrollo en seguridad informática o seguridad TIC, para hacerlo más informal. Eso es preocupante porque el efecto de desincentivo o de temor que puede generar en la comunidad de investigación tanto de practicantes como académica por explorar e identificar problemas de seguridad en los sistemas de seguridad propuestos, va directamente en detrimento de la seguridad del sistema. En seguridad informática, el ataque y la defensa de un sistema se complementan y son ambos necesarios. Desde el año 800 esto se aplica en los sistemas criptográficos; desde 1950 en adelante (seguramente 1970), en la práctica de sistemas de seguridad modernos. Tanto el ataque como la defensa son necesarios y hay que incentivar a ambos. Solo se pueden solucionar los problemas de seguridad si hay gente activa sistemáticamente buscándolos para resolverlos y aquello que vaya en detrimento, con buena o mala intención, no importa, pero que vaya en detrimento de esa práctica en realidad presenta un potencial problema que puede redundar en mayor inseguridad y no mayor seguridad de los sistemas previstos. Les agradezco a todos su tiempo y su atención.

Para observar el video de la exposición de Iván Arce, lea el código o acceda a esta página web: https://www.youtube.com/watch?v=UK_Vm-W20Jg

“La auditoría de este sistema de voto es imposible”

Alfredo Ortega

Me presento: soy Alfredo Ortega, tengo un Doctorado en Matemática en el Instituto Tecnológico de Buenos Aires (ITBA) y, aparte de la experiencia académica, me especialicé en auditoría y seguridad de software por casi quince años. En estos años, estudié y trabajé en la creación de ataques de software y hardware en todo tipo de dispositivos: computadoras, dispositivos móviles como celulares e impresoras –porque también son computadoras–, y específicamente en el sistema de voto como el de boleta única electrónica, usado en 2015.

En primer lugar, todo sistema tiene ventajas y desventajas. Las ventajas están sobrerrepresentadas en el proyecto de voto y acá vinimos a hablar lamentablemente de las desventajas. Si uno tiene más desventajas que ventajas, hay que pensar si conviene o no implementar un sistema de este tipo. Como ya muchas personas dijeron, las tres características fundamentales que tiene que tener un sistema de voto que son auditabilidad, resistencia al fraude y secreto. Estas no se

garantizan en este sistema y, por ende, se presenta muy vulnerable a la coacción del votante.

Específicamente escuché que muchos hablaban de las posibilidades de auditar el sistema. Trabajé mucho tiempo en auditorías y es imposible auditar este sistema en el tiempo propuesto. Es bastante lógico si uno piensa que son decenas de personas desarrollando un sistema por diez años pero si uno lo quiere auditar en 180 días, es imposible hacerlo. Además uno puede auditar una máquina pero hay casi 90.000 maquinas que no necesariamente son las mismas. Entonces, la auditoría de este sistema de voto es imposible. No es extrapolable a nivel nacional, se lo puede hacer con una universidad con un equipo de fútbol pero no con un país.

Por esta razón, justamente, no se puede mantener el secreto del voto porque no se puede confiar en lo que hay adentro de una computadora. Nadie sabe a ciencia cierta todos los componentes, miles de componentes, que tiene una computadora adentro. El votante no puede confiar en algo que tenga componentes electrónicos, lamentablemente. Hay un dato interesante, la misma boleta electrónica tiene una computadora dentro. Lo escuché nombrar como *memoria* pero es una computadora. Insisto: la boleta misma tiene computadora dentro cuyo código nadie sabe quién lo escribió ni quién lo fabricó.

Además, me gustaría hablar sobre ataques específicos a los sistemas de voto. En cuanto a los ataques de los adversarios, uno se va a enfrentar con gente que está muy preparada, hay ataques que no se pueden detectar con auditorías. El sistema de boleta única electrónica pasó por muchas auditorías; muchas universidades –todas las que conozco– auditaron este sistema. Cada universidad encontró una falla distinta. Porque es una falacia que uno puede limpiar un sistema de vulnerabilidades. Uno jamás va a terminar de encontrar las en un sistema. Después de que todas las universidades hicieron su auditoría, lo vi yo personalmente y encontré otra vulnerabilidad, que permitía poner muchos votos de una misma persona en la boleta. Es algo básico en el conteo

de los votos pero se les pasó. Y no porque hayan sido malas personas sino porque es algo natural del software. No porque las máquinas no estén preparadas sino porque en una auditoría es imposible sacar todas las fallas de un sistema. Y lamentablemente el sistema de voto no tolera fallas, no es como un sistema de tarjetas de crédito, de cajero, que pueden ser tolerantes a fallas. Este sistema no tolera fallas. Porque una falla permite que haya un error en la elección, se elija a otra persona y no se pueda volver atrás. Con una tarjeta de crédito se puede volver atrás perfectamente en cualquier transacción.

También, me gustaría hablar de un dato muy interesante: los ataques prácticos –no teóricos– que sufrió el sistema de voto. El sistema de voto de boleta única electrónica sufrió ataques no a los meses sino a los días de ser implementado, es decir, antes de la votación ya sufrió cuatro ataques informáticos de los cuales hay registros por la policía. Uno de los "atacantes", a quien la policía allanó, justamente no se trataba de un ataque sino de una persona que avisó de los ataques.[1] Quiero centrarme en los demás, de los que nadie habla, de los dos ataques que la policía no pudo encontrar. No sé si saben de dónde salieron esos ataques. Uno salió de Texas y otro salió de New Jersey. Esto que parece tan tranquilo significa que la policía tiene evidencia del primer ataque internacional al voto electrónico; y no se puede hacer absolutamente nada porque se trata de otro país, de otra jurisdicción. Fue un ataque internacional, fue antes de que ocurriera siquiera la primera votación. Esto es importante explicarlo: en el ambiente de la informática y la electrónica, todos los países están atacando. Existe la *ciberseguridad*, un área moderna. Todos los países están tratando de atacarse constantemente. Son expertos en hacerlo. No por nada este ataque fue a días de estar el sistema online. La policía que

1 Se refiere a Joaquín Sorianello. Más información puede leerse en http://www.lanacion.com.ar/1807647-segun-un-programador-que-detecto-fallas-en-el-sistema-de-voto-electronico-allanaron-su-casa

es una policía realmente eficiente –no podemos decir que es una policía sin recursos porque a las dos personas que fueron de Argentina las individualizaron, al instante, en corto tiempo– no puede hacer absolutamente nada contra los ataques internacionales.

Ahora bien, la empresa dice que estos sistemas de votos no son vulnerables porque no están conectados a Internet. Eso es totalmente falso. Hay ataques famosos como el de Stuxnet que se han realizado sin que las máquinas estén conectadas a Internet. No se puede pelear contra un adversario que tiene diez o veinte años de experiencia en ataques de sistemas informáticos. Yo tengo esa cantidad de años en el área: uno puede creer que los ataques son cosas que les pasan a otras personas, que no van a suceder en este sistema electrónico y que se van a poder frenar y detectar. Los ataques efectivos son los que no se pueden detectar.

Por casualidad, me mandaron un mail para venir a este lugar como invitación, ese mail tenía un link al sitio de la Cámara de Diputados. A través de ese link, que tenía una falla, uno puede entrar a la base de datos y bajarse los datos de todos los empleados, los diputados, los pedidos de declaración jurada. Los tengo acá, los traje. Esta es exactamente la misma falla de los Panamá papers, no exactamente pero el mismo tipo de falla que permitió los Panamá papers y que permitió los leaks de Wikileaks. Es algo muy común y muy sencillo de hacer. Yo lo reporté, por supuesto, al sistema de seguridad informática que fue muy expeditivo en arreglar este problema; ya no existe, para que se queden tranquilos. Pero este tipo de fallas prevalece en la mayoría de los sistemas.

Por eso, como conclusión, quiero decir que es muy difícil hacer un sistema totalmente seguro y simple. El mundo se está moviendo para alejarse del sistema de voto electrónico. No quiere decir que en algún momento futuro se pueda llegar, pero hoy en día no se puede hacer. Y como prevención los países están alejándose del voto electrónico. Veo que Argentina justamente está yendo en contra de los países y no podemos

ir en contra otra vez del conocimiento mundial, por algo lo están haciendo, aprendamos de la gente con experiencia y tratemos de hacer el voto de alguna manera que no involucre ningún sistema informático. Gracias.

Para observar el video de la exposición de Alfredo Ortega, lea el código o acceda a esta página web: https://www.youtube.com/watch?v=4SlYHVYq1Vs

“La compra de votos no se elimina con este sistema”

Delia Ferreira Rubio

Lo primero que quiero señalar es que esta discusión no es “máquina sí, máquina no”, esta discusión es “rápido y moderno” (título de película) contra “seguro, íntegro y transparente”. Eso es lo que estamos discutiendo y como eso es lo que estamos discutiendo, estamos discutiendo sobre calidad de la democracia; sobre derechos y libertades de los ciudadanos y los electores; sobre los valores que dan sustento al sistema electoral; y sobre la legitimidad de ustedes, que son los electos. Ese es el resultado de un proceso electoral íntegro. La boleta única papel, que usa la mayoría de los países del mundo, es más barata, ofrece muchos más proveedores, evita los monopolios y soluciona el robo de boletas igual que la boleta única electrónica.

Respecto de la boleta única electrónica –y acá estoy llegando a la confusión total–, mal que les pese al señor ministro y a los funcionarios nacionales, es un sistema de voto electrónico. Hemos tenido acá el reconocimiento del Dr. Lozano que, luego de señalar en una sentencia como miembro del

Tribunal Superior de la Ciudad que no era voto electrónico, ahora ha dicho que en la ciudad se aplicó el voto electrónico. Así que me parece muy interesante este reconocimiento. Pero además, ¿para qué vamos a decir una cosa por otra en el Congreso de la Nación, donde no tenemos las restricciones que en la Ciudad Autónoma de Buenos Aires, donde justificaron que las autoridades dijeran una cosa por otra? Porque si reconocían que era voto electrónico tenían que volver a la Legislatura. Para saltarse la Legislatura inventaron la historia de que la boleta única electrónica no es voto electrónico. Acá no necesitamos esa cuestión así que sinceremos ya que estamos sincerando tanto en el país.

¿Qué hay detrás de la decisión de adoptar este sistema de voto electrónico? Veamos los argumentos, veamos si son ciertos. Un argumento es "este sistema es rápido y moderno". Cuidado con *lo moderno* porque estamos haciendo una ley que se supone que va a durar más de seis meses así que el año que viene, sobre todo en materia de tecnología, podríamos llegar a decir que esto es una antigualla. Pero me puse a mirar en los estándares internacionales en materia de sistemas electorales y en los tratados de derechos humanos que hablan de las elecciones libres y no encontré ningún tratado ni ningún estándar que diga que el principio electoral madre en una democracia es *rápido y moderno*. El problema con *moderno* es que si es tan moderno no me explico cómo puede ser que países mucho más desarrollados y modernos que Argentina no utilicen el sistema. A nivel internacional, solo tres países usan el sistema: la India, Brasil y Venezuela. La verdad es que creo que algo deben de estar haciendo bien con la boleta papel los países que son modernos y desarrollados y tienen mucha más tecnología que nosotros como Inglaterra, Alemania, Holanda y los países escandinavos, además de muchos lugares de países latinoamericanos. Entonces lo moderno hay que ponerlo en tela de juicio. También usan la boleta papel Corea y Corea del Sur y lo menciono porque ya voy a volver sobre el tema de si acá tenemos un problema de privatización del sistema electoral o tenemos un problema de extranjerización

del sistema electoral. Lo dejo planteado. Corea del Sur es el país elegido por el Ministerio de Modernización para realizar convenios en la materia.

Además, la otra gran ventaja de este sistema de voto electrónico serían los resultados rápidos. Vamos a ver los resultados rápidos, suponiendo que "rápido y furioso" fuera un valor democrático. El 5 de julio de 2015 se realizaron elecciones en la Ciudad de Buenos Aires, con boleta única electrónica, y en mi provincia, en toda la provincia de Córdoba, con boleta papel (con un modelo distinto del de Santa Fe pero modelo papel). Veamos que ahora supimos las cosas. Sobre la rapidez inicial: a las 19:27 –tengo todos los documentos bajados del escrutinio–, CABA informaba un porcentaje escrutado de 4,7% de las mesas; en Córdoba, a las 19:17, un porcentaje de 1,4% de las mesas. Efectivamente en la Capital iban más rápido. Las 23:55, hora en el que en el día de la elección presidencial todavía no sabíamos nada, en Córdoba teníamos escrutados con boleta única papel el 65% de las mesas y la tendencia no varió hasta después. Alrededor de las 02:00 am del día 6 de julio el escrutinio de Capital y de Córdoba iban cabeza a cabeza, 93,4 y 93,5%. Así iban funcionando. Eso es lo rápido y furioso.

Por otro lado, a mí me parece que rápido y con errores no es un buen negocio. En el caso del voto electrónico de la Capital Federal, ni la empresa, ni las autoridades, ni las auditorías detectaron algo que mencionó la diputada Stolbizer hace un momento. Un error en la carga de los resultados estaba dando más votos que votantes en algunas comunas. Por ejemplo en la comuna 14, 21:57 de la noche, cantidad de electores 147.100, cantidad de votos 147.363. O sea que habían votado más que el total de los electores de la comuna. A las 00:29, información oficial del sistema que la autoridad electoral dice que funcionó tan bien, seguía diciendo que esa comuna tenía a 170.000 electores y que habían votado 147.363. Recién se corrigió esto a las 02:00 am del día siguiente y se corrigió no porque la empresa lo detectó, no porque los autores lo detectaron, no porque las autoridades lo detectaron, se corrió

porque los que estábamos observando la elección desde nuestras respectivas casas –y hay muchos que estábamos esa madrugada siguiendo la elección–, empezamos a ver que había una discordancia total entre la cantidad de electores de las comunas y la cantidad de votos que habían recibido. Gracias a nuestro trabajo conjunto, descubrimos que todo el padrón electoral del distrito Ciudad de Buenos Aires estaba mal cargado en la base que se estaba utilizando para dar los resultados. Y gracias a que lo hicimos público en las redes sociales se corrigió a las 02:00 am del día siguiente. Lo mismo pasaba con la comuna 1, por ejemplo, que es un caso muy lindo. Esa comuna tenía 166.483 electores empadronados a las 21:00; pero a las 02:00 am, 181.207 empadronados. Así que se ve que había habido un proceso de empadronamiento, solo *El Cronista Comercial* mencionó esta irregularidad al día siguiente sobre la base de lo que habíamos dicho los que estábamos observando. Pero rápido y moderno evidentemente no es para mí lo que vale acá sino los valores fundamentales. Y me voy a referir solo a algunos.

Sobre el secreto del voto y la integridad de las elecciones, les voy a leer lo que dice la patente del sistema MSA, la lectura de la totalidad de los códigos puede hacerse dentro de la urna sin necesidad de tener que abrirla, evitando todo contacto manual con los votos. Se pueden leer todos los votos que están en la urna, también se pueden leer con un simple aplicativo que se demostró que funcionaba voto por voto para poder hacer el sistema de compra de votos. De manera tal que el sistema de votos se puede vulnerar con el sistema de boleta única electrónica, como se vulneró en Holanda que determinó la eliminación del sistema, como se vulneró en Brasil. Y también habría que recordar el discurso de Maduro cuando en Venezuela dijo al día siguiente de una elección, "tengo lista de todos los empleados públicos que votaron en contra del partido", previo a una purga. La compra de votos no se elimina con este sistema, lo que se hace es utilizar otro sistema para comprar los votos. Es graciosa la norma del proyecto que dice que no se podrá sacar fotos a la boleta,

porque están pensando en la boleta papel y no en cómo se puede probar en cómo ha votado una persona para el voto. El clientelismo que el gobierno dice que se elimina con esto tampoco se elimina evidentemente porque sino no habría clientelismo en Venezuela, Salta, en la Ciudad de Buenos Aires o en muchos otros países.

Un último punto, porque todo lo demás ya lo he escrito y publicado y lo pueden buscar en las redes, es que yo confio en que el que va a determinar el sistema electoral de la nación sea el Congreso de la Nación. Entonces, me pregunto si ya han pedido informes sobre el convenio celebrado por el Ministerio de Modernización con una empresa o con el estado coreano para el desarrollo del software y la provisión de las máquinas. Y me pregunto si les mostraron, de hecho es que no les mostraron porque estuve desde esta mañana acá, si les han mostrado el prototipo que ha llegado desde Corea y que el Ministerio de Modernización y el Ministerio del Interior le muestran a determinadas personas. Podrían pedirlo. Y me pregunto finalmente, lo último que me enteré ayer de un funcionario del gobierno que no sabía con quién estaba hablando, si es cierto que el gobierno de Corea ha ofrecido el regalo del software que se va a utilizar. Entonces la pregunta es: ¿privatización, tercerización o extranjerización del sistema electoral? Muchas gracias.

Para observar el video de la exposición de Delia Ferreira Rubio, lea el código o acceda a esta página web: https://www.youtube.com/watch?v=ebTS2_wFuQs

“¿Qué seguridad tiene un votante de estar seguro del secreto?”

Javier Smaldone

Mi nombre es Javier Smaldone, soy programador y administrador de redes de sistemas. No soy especialista en seguridad informática pero sé lo suficiente sobre el tema para sobrevivir en lo que hago. No pertenezco a ninguna entidad, a ningún organismo, ni club de fútbol, ni partido político, así que vengo a hablar acá como un ciudadano común. Por el poco tiempo que tenemos y lo cansados que estamos todos esta altura de la noche, me gustaría poner el foco en una cosa que se ha mencionado, sobre todo en los últimos discursos, pero en gran parte del día se ha pasado por arriba, y es el tema del secreto.

El énfasis siempre ha estado puesto mayormente en lo que es auditabilidad y verificabilidad. Saber que los resultados son correctos, saber que los conteos están bien hechos, tener forma de verificar si ese conteo electrónico coincide con un conteo manual, pero nos olvidamos de una cosa. Está probado que no se puede tener un sistema ni electrónico, ni manual,

ni de ningún tipo que permita a la vez garantizar el secreto, la auditabilidad y la verificabilidad. Aquí, en Argentina, tomamos una decisión hace mucho tiempo y pusimos el secreto por delante de todo, fue en el año 1912. Todas las complicaciones que tenemos de cómo diseñamos las boletas, de cómo hacemos el procedimiento para emitir el voto, de cómo escrutamos las mesas y los controles cruzados de escrutinio provisorio y definitivo, vienen de la necesidad de preservar el secreto del voto. Sino no habría este problema, habría otros.

¿Cómo garantizamos el secreto del voto hoy con boletas de papel? Sea con la boleta partidaria en un cuarto oscuro o con la boleta única como usamos en Córdoba y en Santa Fe. ¿Cómo hace el votante para estar seguro de que nadie sabe lo que está votando? Mirando. En el cuarto oscuro mirando que no haya nadie, llevando si quiere la boleta desde su casa guardada en un bolsillo. Él puede asegurarse de que nadie va a saber a quién voto. Hay algunos problemas con eso que ya los voy a detallar. Y con la boleta única de papel también, mirando. ¿Cómo hace el votante para asegurarse de que no se viola el secreto del voto cuando tiene que emitir su voto a través de una computadora? Creyendo lo que dicen en la auditoría. Creyendo, confiando: todo empieza con un acto de fe.

De las auditorías ya han hablado suficiente. Las auditorías nunca son suficientes, en particular en este sistema, en este proyecto de ley que es el sistema del MSA. Se ha probado que pasó por un montón de auditorías que detectaron la posibilidad de meter varios votos en una boleta, que se comieron que en esa carcasa de plástico no había una computadora sino que había dos y la segunda con su software no fueron ni siquiera mencionadas en las auditorías. Incluso la segunda violaba el decreto reglamentario de la ley electoral porque tenía capacidad de almacenamiento permanente. Memoria permanente, suficiente para almacenar todos los votos emitidos en una mesa y ni se nombró. Entonces, las auditorías.

¿Qué seguridad tiene un votante de estar seguro del secreto? Creer o no. Qué piensan ustedes, qué camino tomará

aquella persona para la que su trabajo, su plan social, su bolsón, sus $400 dependan de a quién vote. Creer en la auditoría o agachar la cabeza, apretar el botoncito que le dijeron que tiene que apretar y votar cómo lo mandaron a votar. Ya el solo hecho de que el elemento de votación requiera de auditorías lo invalida. No estamos hablando de que el procedimiento de votación permita hacer controles sino que el mismo elemento de votación requiera de una auditoría de una élite que le dice al votante "nadie va a saber cómo votaste", cuando a lo mejor hay un puntero que le dice "ojo, cómo votás porque vamos a saber". ¿Será cierto o no? Y después hay otra cosita más que es la violación voluntaria del secreto, la posibilidad de demostrar a quién se voto. Algo que debería estar imposibilitado por el sistema.

Con la boleta única de papel sí hay un problema, lo sufrimos en Córdoba y en Santa Fe y cada elección se tiene que controlar: el tema de las fotos. Es más, en Córdoba en particular, en mi ciudad, Rio Cuarto, se dieron cuenta en la mitad de una elección cuando alguien notó que andaban celulares dando vueltas por todos lados. Ya se había aprobado la reforma, ya se habían diseñado las boletas, ya se había hecho todo y en el medio de una elección los vivos de siempre ya sabían cómo hacerlo. En la auditoría, no nos dimos cuenta de que sacan fotos, le muestran al puntero la foto y les pagan. De ahí en más no se puede sacar foto. Pero cómo evito yo que alguien saque una foto cuando está poniendo cruz en una boleta a través de un tabique así. Mirando con mucho cuidado.

Ahora les voy a mostrar una cosa, espero que se vea la pantalla. Este es un celular, un Samsung S4, medio viejito, no es el último. Tengo una aplicación que funciona así: tengo dos boletas con votos. Supongamos que soy puntero del partido azul. Voy y voto con la boleta única electrónica, elijo las opciones, confirmo y la máquina me entrega esto. Este celular lo tengo en el bolsillo, esto no usa la cámara del celular, esto usa el lector de chips. Y lo que hago es esto, paso el chip cerca del celular, ven cómo cambio, está en amarillo,

leyó el voto maestro, leyó este voto. El celular se lo doy a un votante y le digo "ponetelo en el bolsillo y andá a votar. Cuando termines de votar saca la boleta y hacete el que estás leyendo y pasatelo al lado del bolsillo. Si el celular se pone en rojo, no cobrás, pero si el celular me lo traés en verde, cobrás". Y todo esto sin sacar el celular del bolsillo. ¿Cómo lo evitan? ¿Cachando votantes? La aplicación no, pero esta metodología la hicimos pública antes del 5 de julio en Capital Federal. Nadie dio bolilla. Después la publicamos para que se vea que es una pavada hacerla, funciona con celulares de $2000. Nada más, muchas gracias.

Para observar el video de la exposición de Javier Smaldone, lea el código o acceda a esta página web: https://www.youtube.com/watch?v=F4Gco-w_qRo

“La posibilidad de que se deslice un error es muy alta”

Enrique A. Chaparro

Estoy aquí no solo como miembro de la Fundación Vía Libre sino con algunos múltiples sombreros, como casi todos tenemos. Durante los últimos treinta años, mi actividad principal ha sido la seguridad de los sistemas de información. He pasado por algunas universidades y de algunas me he graduado y de otras me han echado. El último sombrero es el de mi condición de ciudadano de a pie. Trataré de combinarlos en los próximos diez minutos señalando algo que dos académicos irlandeses McGaley y Gibson señalaban en el momento en que Irlanda analizaba el paso a un sistema del voto electrónico. McGaley y Gibson decían que ningún sistema electoral es mejor que la confianza que los votantes tienen en él. Esta es una cuestión central porque independientemente de que discutamos meses sobre cuáles son las fallas reales o percibidas de nuestro sistema electoral, lo cierto es que hay una sensación en la ciudadanía de que hay fallas estructurales en el sistema electoral actual.

Ahora bien, una de las soluciones que propone el Poder Ejecutivo para resolver esta cuestión es una serie de cambios

en el método de votación. Nosotros nos oponemos ontológicamente al voto electrónico, ¿qué quiere decir? Esencialmente que no conocemos forma en que un sistema de voto electrónico pueda garantizar las condiciones fundamentales que nos impone por ejemplo el artículo 25 del Pacto Internacional de Derechos Civiles y Políticos. Es decir, elecciones genuinas con voto universal e igual protegidas por secreto. Esto se debe no a capricho, no a opinión, sino a cosas que sabemos en el plano de la teoría. Es imposible construir un sistema de voto que al mismo tiempo garantice verificabilidad, secreto e integridad. Eso es un teorema que se llama *teorema de Hosp y Vora*, resuelto en el año 2009. También sabemos que cualquier proclama de seguridad que hagamos es, en términos de conocimientos científicos, no falsable. Esto que quiere decir, que puedo demostrar que una condición de seguridad es necesaria pero jamás puedo demostrar que es suficiente. Por lo tanto además hay un error conceptual en uno de los ítems del artículo 14 bis propuesto que dice que la máxima seguridad solo existe en el infinito. Nuestra posición ontológica debería ser explicada largamente pero tenemos limitaciones de horario y estamos todos muy cansados.

Entonces, además, desearíamos apuntar algunas cuestiones que están ligadas al proyecto en particular. La justificación del proyecto propone que este sistema sugerido resolvería la cuestión que plantea el Tribunal Supremo Constitucional alemán en su fallo del 2009 302 y 402 del segundo senado del Bundesverfassungsgericht. Esto no es así y permítanme intentar el test por dos vías. En primer lugar, porque si imprimir el voto fuese la solución a la inconstitucionalidad que plantea el Tribunal Supremo Constitucional alemán, supongo que los alemanes no son tan estúpidos como para no haber agregado un pedacito de papel a su sistema. Y en segundo lugar, porque si uno hace un repaso a la doctrina alemana y a todos los comentaristas jurídicos alemanes a partir de ese fallo, van a encontrar mayoritariamente que la doctrina opina que el camino que deja abierto es muy estrecho. Nada autoriza a suponer que una copia impresa garantice que estamos efectivamente en ese camino estrecho. Porque de las copias impresas sabemos a partir de experiencias

de otros países, que el porcentaje de lectura es muy bajo, mucho más aún en un sistema cuyo modelo favorito del Ejecutivo es la provincia de Salta y la Ciudad de Buenos Aires, un sistema que no fuerza a leer la copia para obtener el voto, a diferencia de otros que implican apretar un botón por *sí* o por *no* después de haber visto la versión impresa. Y por otro lado por diferencias cognitivas que son típicas de nosotros, los humanos, nos cuesta mucho distinguir aquello que está en pantalla respecto de lo que tenemos en la mano. Yo acabo de escoger la foto en colores de una persona y me presentan en un papel impreso una lista de nombres. La posibilidad de que se deslice un error es muy alta. Los mejores estándares que tenemos de esto dicen que, por lo menos, la mitad de los votantes pasan por alto errores serios de diferencia entre lo que sucedió en pantalla y lo que ha sido mostrado impreso.

Ciertamente los problemas de índole técnica son muchas y hay algunos problemas graves de índole técnica en el proyecto. Por ejemplo, cuando se plantea la auditoría ex post del sistema. Con todo respeto lo digo, me parece que el Ministerio del Interior podría haber invertido una pequeña cantidad de dinero en preguntarle a algún estadístico en cómo se hace una muestra correcta. La muestra del 5% no tiene ninguna relación con lo que se pretenda muestrear. El tamaño de la muestra depende del tamaño de la diferencia. Entonces, con la norma tal como la prevé la ley, en este momento el presidente de la República podría ser otro y el jefe de gobierno podría ser otro y se ajustaría perfectamente a los términos de la ley. Pero además tenemos un problema, nosotros usamos para la asignación de los cargos de los cuerpos colegiados del sistema proporcional D'Hont y entonces cuando repartimos el último cargo la diferencia es muy pequeña. En términos comparativos, la banca 15 para el actual oficialismo o la octava para el principal partido de oposición en la Ciudad de Buenos Aires se definen por 531 votos. Persiste ampliamente en el conteo el error del 5% que plantea la ley y podemos tener casos más extremos.

Otro riesgo que enfrentamos –y que han señalado aquí algunos de los oradores que me precedieron– es el problema de la

privatización del sistema electoral. Holanda lo experimentó. Les recomiendo y no quiero ser particularmente aburrido sobre la cuestión, una publicación de Anne Marie Oostveen, quien analizó los efectos de la privatización del sistema holandés. Cuando los holandeses recuperaron la autonomía para manejar las elecciones, no sabían cómo hacerlas porque habían estado en el sector privado durante más de una década. Eso es la sabiduría fundamental de la maquinaria de la democracia. Si no sabemos cómo hacer elecciones, vamos a perderlas todas.

¿Cuánto vale el poder político de un país? No pregunto cuánto cuesta, me pregunto cuánto vale. ¿Cuántas voluntades están dispuestas a sacrificar cualquier cosa por el poder político de un país? Un columnista se preguntaba el otro día en el *Washington Post* cuánto vale la presidencia de los Estados Unidos. Bien, eso, lo que podamos imaginar que vale el poder político de un país es el presupuesto con el que cuenta el adversario y a grandes presupuestos, grandes ataques. Que no solo debemos pensar en términos del potencial fraude que un sistema electrónico multiplica maravillosamente, porque hay cambio de dos o tres líneas de códigos en un programa se replica en 95.000 mesas electorales del país a una escala que no podemos lograr con los procedimientos manuales. El problema es la pérdida del secreto o la amenaza de la pérdida del secreto y en tercer lugar, el problema del sabotaje.

Siempre estamos pensando que estamos compitiendo entre partidos que quieren llegar al poder por vía legitima y están dispuestos a ceder un poco éticamente para robarse unos votos. Pero ¿qué pasa si lo que yo quiero hacer es sabotear el sistema electoral? ¿Qué pasa si en el medio de la elección tenemos un evento catastrófico tal como un caballo de Troya que pare todas las maquinas de votación a las 00:35? Estamos sin red. El proyecto que plantea el Poder Ejecutivo no tiene ninguna alternativa. Si tenemos un evento catastrófico, tenemos un incendio en términos del sistema político. Suspender una elección. Y esto se logra con tres o cuatro líneas de código que eventualmente insertó un obrero en una factoría china dentro de un chip que está entre los miles de chips de una máquina.

No quisiera ser ave de mal agüero pero mi función desde el punto de vista de la sociedad civil es ser opositor independientemente de quién sea el oficialismo. Finalmente, quiero tomarme este último minuto para dedicarlo a las disonancias que existen en términos de régimen penal que se impone en el proyecto del Ejecutivo. Quiero señalar varias cosas, en primer lugar el que aparezcan tipos penales nuevos significa que el Poder Ejecutivo está evaluando que existen amenazas nuevas respecto de aquello que ya teníamos, porque a uno no se le ocurriría por ejemplo crear una figura penal por derribar aviones con el pensamiento, nadie va a crear un tipo penal relacionado con la tentativa supersticiosa. Entonces, ciertamente, lo que se está persiguiendo es que hay nuevas amenazas que necesitan un nuevo régimen penal y que las que existían siguen existiendo porque si no hubiéramos sustituido el régimen penal existente. Pero, además, quiero señalar que por ejemplo el proyecto se lleva puesto el criterio de proporcionalidad de la ley penal. Les voy a dar dos ejemplos simples. Por el artículo 134, si yo interrumpo a un empleado de correos que lleva un telegrama con los resultados, estoy condenado a una pena de prisión de entre seis meses y dos años. Ahora, si yo lo que hago es interrumpir el cable que comunica el lugar de captación de votos con el lugar de acopio la pena varía entre dos y seis años. Mismo delito, distinta figura dependiendo del medio comisivo. Quisiera señalar que algunos delitos electorales, que son delitos de intención, están planteados en términos más duros que el abuso sexual de personas menores de trece años. Muchas gracias.

Para observar el video de la exposición de Enrique A. Chaparro, lea el código o acceda a esta página web: https://www.youtube.com/watch?v=cc9aX2-PJn8

Sobre los autores

Tomás Aguerre es Licenciado en Ciencia Política de la Universidad de Buenos Aires (UBA) y co-editor del blog colectivo *artepolítica* (http://artepolitica.com).

Iván Arce es especialista en informática. Es co-fundador y ex Oficial Principal de Tecnología (CTO) de Core Security Technologies, una de las empresas de seguridad informática más importantes del mundo. Es miembro del Institute of Electrical and Electronics Engineers (IEEE) y de la Association for Computing Machinery (ACM), editor asociado de la revista especializada IEEE Security & Privacy. Además, es el director del Programa de Seguridad en TIC (STIC) en la Fundación Dr. Manuel Sadosky, dedicada a la investigación y desarrollo en TIC, creada por el Ministerio de Ciencia, Tecnología e Innovación Productiva

Ártica es un centro cultural online que desarrolla servicios de formación, consultoría e investigación para la implementación de proyectos artístico-culturales en Internet. Más información sobre sus actividades y objetivos, puede consultarse en http://www.articaonline.com/presentacion

Beatriz Busaniche es Licenciada en Comunicación Social por la Universidad Nacional de Rosario (UNR), Magíster en Propiedad Intelectual de FLACSO y Candidata al Doctorado en Ciencias Sociales en FLACSO. Además, es docente en grado y posgrado en la Universidad de Buenos Aires (UBA) y en FLACSO y presidente de la Fundación Vía Libre, organización civil sin fines de lucro dedicada a la defensa de derechos fundamentales en entornos mediados por tecnologías de información y comunicación. Ha escrito múltiples artículos sobre el voto electrónico y sus problemas. Es autora del libro *Propiedad intelectual y derechos humanos* (Tren en movimiento, 2016).

Enrique A. Chaparro es especialista en seguridad de los sistemas de información, devenido propagandista del software libre. Ha participado

en proyectos significativos de implantación de software libre en los sectores público y privado, y ha colaborado con proyectos legislativos sobre uso de software libre en el Estado en Argentina, Colombia y Perú. Es miembro de la International Association of Cryptologic Research, del Technical Committee on Security and Privacy de IEEE, y de la Fundación Vía Libre. Graduado en Matemáticas en la Universidad de Buenos Aires, con posgrados en Canadá e Inglaterra.

Nicolás D'Ippolito es Doctor en Computación, psicólogo aficionado, investigador y profesor de la UBA.

Delia Ferreira Rubio es abogada y Doctora en Derecho por la Universidad Complutense de Madrid. Entre 1990 y 2005, se desempeñó como Jefe de Asesores de Diputados y Senadores en el Congreso Nacional, trabajando con las Comisiones de Asuntos Constitucionales de ambas Cámaras del Congreso. Entre 2005 y 2007, cumplió el rol de Asesora de la Auditoría General de la Nación. A partir de 2007, trabaja como consultora independiente. Además, es investigadora de la Fundación CEPPA de Buenos Aires. Entre 2004 y 2010, fue miembro del *board* de Poder ciudadano y, entre 2008 y 2010, fue su Presidenta. También, fue miembro del *board* internacional de Transparency International por dos períodos consecutivos entre octubre de 2008 y octubre de 2014. Es autora de numerosas publicaciones sobre cultura democrática, instituciones políticas, política comparada, gobierno por decreto, ética pública y parlamentaria, financiamiento de los partidos políticos y sistemas electorales, entre otros temas.

Federico Heinz es programador y especialista en software libre. Fue cofundador de Fundación Vía Libre, en la que actualmente participa como colaborador.

Alfredo Ortega es Doctor en Informática por el Instituto Tecnológico de Buenos Aires (ITBA). Es especialista en auditoría y seguridad de software.

Daniel Penazzi es Doctor en Matemática por la Universidad de Minnesota (EE. UU.) y especialista en criptografía. Actualmente, es docente e investigador en la Facultad de Matemática, Astronomía y Física en la Universidad Nacional de Córdoba (UNC).

Javier Smaldone es programador y administrador de redes de sistemas. Se especializa en soluciones informáticas con software libre. Además, es consultor informático independiente. Hace varios años organiza el sitio blog.smaldone.com.ar y la cuenta de Twitter @mis2centavos.

Bibliografía general

Alvarez, R. Michael, y Thad E. Hall (2010). *Electronic elections: The perils and promises of digital democracy*, Princeton (NJ): Princeton University Press.

Anderson, Ross J. (2010). *Security Engineering*, New York: John Wiley & Sons. Disponible en https://www.cl.cam.ac.uk/~rja14/book.html

Aranha, Diego F., Marcelo M. Karam, André Miranda, y Felipe Scarel. 2014. "Software vulnerabilities in the Brazilian voting machine". En *Design, Development, and Use of Secure Electronic Voting Systems*, editado por Dimitrios Zissis y Dimitrios Lekkas, 149–175. Hershey, PA: IGI Global.

Benaloh, Josh, Ronald Rivest, Peter YA Ryan, Philip Stark, Vanessa Teague, y Poorvi Vora. 2015. "End-to-end verificability". arXiv preprint arXiv:1504.03778.

Campbell, Bryan A., y Michael D. Byrne. 2009. "Now do voters notice review screen anomalies? A look at voting system usability". En *Proceedings of the 2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*. USENIX Association.

Chaparro, Enrique A. 2015. "El sistema de voto electrónico de la Ciudad de Buenos Aires; una 'solución' en busca de problemas." Working Paper. Buenos Aires: Fundación Vía Libre.

Everett, Sarah P. 2007. "The usability of electronic voting machines and how votes can be changed without detection". Ph. D. thesis, Rice University.

Franklin, Joshua, y Jessica C. Myers. 2012. "Interpreting Babel: Classifying Electronic Voting Systems". En *Proceedings of the 5th International Conference on Electronic Voting 2012*, editado por Manuel J. Kripp, Melanie Volkamer, y Rüdiger Grimm, 244–256. Lecture Notes in Informatics 205. Bonn: Gesselschaft für Informatik.

Goggin, Stephen N., Michael D. Byrne, Juan E. Gilbert, Gregory Rogers, y Jerome McClendon. 2008. "Comparing the Auditability of

Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems." En *EVT 08*, 1–7. USENIX Association.

Jones, Douglas W., y B. Simons. 2012. "Broken ballots: will your vote count?". En CSLI lecture notes, no. 204. Stanford, Calif: CSLI Publications.

Lehoucq, Fabrice. 2002. "Can Parties Police Themselves? Electoral Governance and Democratization". *International Political Science Review* 23 (1): 29–46.

– 2003. "Electoral Fraud: Causes, Types, and Consequences". En *Annual Review of Political Science* 18 (6): 233–56.

Loeber, Leontine. 2008. "E-Voting in the Netherlands: from General Acceptance to General Doubt in Two Years". En *Electronic Voting 2008*, 21–31. Lecture Notes in Informatics 131. Bonn: Gesselschaft für Informatik.

McGaley, Margaret, y J. Paul Gibson. 2003. "Electronic Voting: A Safety Critical System". Technical Report NUIM-CS-TR-2003-02. Maynooth: National University of Ireland.

Mercuri, Rebecca. 2007. "Rebecca Mercuri's Statement on Electronic Voting". Notable Software. http://notablesoftware.com/RMstatement.html.

Mitrou, Lilian, Dimitris Gritzalis, y Sokratis Katsikas. 2002. "Revisiting legal and regulatory requirements for secure e-voting". En *Security in the Information Society: Visions and Perspectives*, editado por M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi, y Heba K. Aslan, 469–80. IFIP Advances in Information and Communication Technology 86. Dordrecht: Kluwer.

Moynihan, Donald P. 2004. "Building Secure Elections: E-Voting, Security, and Systems Theory". *Public Administration Review* 64 (5): 515–28.

Norden, Lawrence, Jeremy M. Creelan, David Kimball, y Whitney Quesenbery. 2006. "The machinery of democracy: Usability of voting systems". En *Voting Rights and Elections*. New York: Brennan Center for Justice at NYU School of Law.

Oostveen, Anne-Marie, y Peter van den Besselaar. 2004a. "Ask No Questions and Be Told No Lies: Security of Computer-Based Voting Systems, Users' Trust and Perceptions". En *EICAR 2004 Conference*, editado por U. E. Gattiker. Copenhague: EICAR E.V.

– 2004b. "Security as belief. User's perceptions on the security of electronic voting systems". En *Electronic Voting in Europe: Technology, Law, Politics and Society*, editado por A. Prosser y Robert Krimmer, 73–82. Lecture Notes in Informatics P47. Bonn: Gesselschaft für Informatik.

Pellegrini, François. 2014. "Chaînes de confiance et périmètres de certification: le cas des systèmes de' vote électronique'". *Research Report RR-8853*. Project-Team Bacchus. Talence: INRIA.

Rivest, Ronald L. 2008. "On the Notion of 'Software Independence' in Voting Systems". En *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 366 (1881): 3759–67.

Tula, María Inés (coord.). *Voto Electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales*, Buenos Aires, Ariel Ciencia Política - Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC), 2005.

Wolchok, Scott, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, y Rop Gonggrijp. 2010. "Security analysis of India's electronic voting machines". En *Proceedings of the 17th ACM conference on Computer and communications security*, 1–14. ACM.

Xenakis, Alexandros, y Ann Macintosh. 2005. "E-electoral administration: organizational lessons learned from the deployment of e-voting in the UK". En *Proceedings of dg.02005: the 6th National Conference on Digital Government Research*, Atlanta, Georgia, May 15-18, 2005, editado por Lois Delcambre y Genevieve Giuliano, 191–97. Marina del Rey, CA: Digital Government Research Center.

Índice

Este libro se terminó de imprimir en los talleres
de la cooperativa de trabajo Tricao ltda.
CABA, marzo 2017.