



**VOTO
ELECTRÓNICO
EN PARAGUAY**

**El encierro de la
democracia en una
caja negra**

Beatriz Busaniche

VOTO ELECTRÓNICO EN PARAGUAY

El encierro de la democracia en una caja negra

Beatriz Busaniche

Un *white paper* es un informe o guía que informa de manera concisa y extensa sobre un tema complejo y presenta la filosofía y marco teórico al respecto.

Este *white paper* fue realizado por TEDIC en el marco de un proyecto financiado por el National Endowment for Democracy (NED) y forma parte de una serie de publicaciones que busca guiar e informar sobre el voto electrónico desde un enfoque político, legal, filosófico, técnico, social y cultural.



TECNOLOGÍA &
COMUNIDAD

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

Coordinación: Maricarmen Sequera

Diseño de portada: Betania Ruttia

Diagramación: Horacio Oteiza

Corrección: Luis Pablo Alonzo Fulchi

DICIEMBRE 2020



Esta obra está disponible bajo licencia
Creative Commons Attribution 4.0 Internacional (CC BY SA 4.0)
<https://creativecommons.org/licenses/by-sa/4.0/deed.es>

Tabla de contenidos

1. Introducción	5
2. Una breve historia del sistema de boleta electrónica/voto electrónico en la región	6
3. ¿Qué garantías debe tener un sistema electoral?	9
3.1. Secreto del voto	9
3.2. Integridad	11
3.3. Auditabilidad y transparencia	12
4. El problema de la propiedad intelectual y la privatización del sistema electoral	14

El encierro de la democracia en una caja negra

por Beatriz Busaniche¹

«El voto es secreto, pero el escrutinio es público»
Artículo 221 del Nuevo Código Electoral de Paraguay

La frase que sirve de introducción a texto es, paradójicamente, la clave fundamental de los problemas que vamos a trabajar a lo largo de las próximas líneas.

1. Introducción

En un período histórico caracterizado por la creciente polarización política a nivel global, la inestabilidad de las democracias de la región y la falta de confianza en los sistemas de partidos políticos, el sistema electoral se vuelve un elemento central para la construcción de procesos institucionales sólidos, confiables, que devuelvan a la ciudadanía la capacidad de construir nuevos procesos institucionales que refuercen los consensos democráticos.

Una democracia no es sólo el sistema electoral, pero este sistema debe funcionar de modo transparente y especialmente confiable para dotar a los representantes electos de la legitimidad que sólo la voluntad popular puede sostener.

Un sistema electoral debe cumplir dos funciones centrales: asegurar un ganador y convencer a un perdedor de que efectivamente ese ha sido el resultado de la contienda electoral. Se trata de una misión así de simple y de compleja a la vez. Para que un sistema electoral sea confiable, la transparencia y auditabilidad de los procesos y la participación ciudadana son factores indispensables.

A lo largo de las próximas páginas vamos a analizar las definiciones y características del sistema de votación electrónico que se prevé usar en Paraguay, su trayectoria en Argentina y las indispensables salvaguardas para una implementación de esta naturaleza.

¹ Beatriz Busaniche es Presidente de la Fundación Vía Libre, organización civil sin fines de lucro que trabaja en defensa de derechos ciudadanos en entornos mediados por tecnologías de información y comunicación. Desde 2003, la Fundación se ha dedicado a investigar y promover debates en torno al uso de tecnologías en los procesos electorales en la región. Todo el trabajo de la Fundación Vía Libre sobre Voto Electrónico se encuentra disponible en <https://www.vialibre.org.ar/category/voto-electronico/>

2. Una breve historia del sistema de boleta electrónica/voto electrónico en la región

El sistema de voto electrónico que se eligió tras el proceso de licitación pública en Paraguay fue diseñado por la firma argentina Magic Software, una empresa local con sede en la Ciudad Autónoma de Buenos Aires, que trabaja desde hace años en tecnologías vinculadas a la impresión de entradas para espectáculos y teatros, entre otros temas. Su llegada al mundo de los sistemas electorales se produjo en el primer tramo de los años 2000, de la mano de una oleada de propuestas de promoción de modernización en los procesos electorales.

En Argentina, la primera experiencia de voto electrónico tuvo lugar en la ciudad de Ushuaia, en la provincia de Tierra del Fuego, en el año 2003 y estuvo a cargo de la firma española Indra. En aquel momento, la empresa proveyó equipamiento para elecciones municipales de manera gratuita, a modo de prueba piloto para convencer a las autoridades fueguinas de las bondades del sistema. Aquellos sistemas eran mecanismos de Registro Directo, sistemas conocidos como DRE y no emitían comprobante en papel.

Un trabajo intenso de organizaciones de la sociedad civil, unido a la cooperación de la comunidad de Software Libre local logró que los legisladores de la ciudad estuvieran advertidos de lo que implicaban estos sistemas. Cuando se reguló la utilización del voto electrónico mediante ordenanza municipal y ante la exigencia de resguardos de seguridad para el votante, Ushuaia no volvió a utilizar voto electrónico porque la propia firma indicó que los requerimientos exigidos no estaban a su alcance.

Años más tarde, la legislatura de la provincia de Tierra del Fuego comenzó a discutir una legislación que habilite el uso de máquinas para votar, pero finalmente el debate naufragó ante las duras críticas de la comunidad técnica y la evidencia irrefutable de la fragilidad de esos sistemas.² Las dos firmas involucradas en ese tramo del proceso de cabildeo fueron Smartmatic y MSA.

El arribo a la región de tecnologías de votación electrónica parecía inexorable en aquellos primeros años del presente siglo y la participación de firmas extranjeras como Indra eran un paso casi obvio. Para la misma época, varios países habían ya dado sus primeros pasos en el uso de máquinas para votar.

Brasil fue el pionero en la región, con una introducción de los sistemas de voto electrónico parcial para mediados de los años noventa. Y su difusión generalizada a toda la ciudadanía con derecho a voto para los 2000. Hoy es uno de los pocos países de la región que sostiene esta práctica. El sistema de voto electrónico utilizado en Brasil tiene la particularidad, a diferencia de las otras ofertas en la región, de ser un desarrollo propio del estado Brasileño y bajo control de la máxima autoridad electoral de ese país, el Tribunal Supremo de Justicia Electoral. A su vez, es un sistema que ha ido evolucionando con el correr de los años hasta incorporar el sistema de identificación biométrico en la propia urna electrónica.

2 Vale recordar que durante la exposición de una de las firmas proveedoras de servicios, el sistema de votación electrónica que fue presentado ante los legisladores falló en la misma demostración. Véase el registro en video de la sesión de la legislatura provincial en la cual se presentó el dispositivo en <https://www.youtube.com/watch?v=w7le8PCaKos> (Visitado el 29 de septiembre de 2020).

En Brasil, la discusión sobre el sistema electoral es mínima y está virtualmente relegada a expertos en seguridad de los sistemas de información que regularmente discuten y advierten sobre las vulnerabilidades y problemas del sistema. Recientemente se planteó la posibilidad de sumar papeleta impresa al sistema, pero el Tribunal Superior de Justicia rechazó esa posibilidad porque esa opción que contribuiría a resguardar la integridad de la elección sería contraria al secreto del voto.

Recordemos que el sistema de Brasil, a diferencia de la mayoría de los sistemas que comercializan las empresas privadas en la región, es el único que no deja el voto emitido en soporte impreso de papel, imposibilitando así cualquier auditoría y recuento *ex-post*. El sistema electoral de Brasil es uno de los más frágiles del mundo en términos de seguridad y ha sido puesto a prueba y vulnerado en diversas oportunidades a lo largo de los últimos años³. Aun así, el debate sobre el voto electrónico y el sistema electoral no ha cobrado la fuerza necesaria para implementar mejoras o buscar estrategias que permitan implementar un sistema más confiable. Lamentablemente, en Brasil, la discusión sobre la integridad del sistema electoral cayó en la polarización y fue promovida por partidarios de la extrema derecha, lo que contribuyó a socavar la capacidad de la sociedad civil de ofrecer un debate riguroso basado en evidencias.

Finalmente, lo que queda de manifiesto en el caso de Brasil es que la confianza cívica sólo está construida alrededor del sistema institucional que lo sostiene y no del sistema de votación en sí mismo.

Venezuela se convirtió pronto en otro país de la región en utilizar voto electrónico. Esta vez con un sistema desarrollado por una empresa originalmente local llamada Smartmatic, firma que fue cambiando de capital accionario y con intereses, filiales y subsidiarias en diversos países del mundo.⁴

El sistema de votación de Venezuela se caracteriza por tener dos partes diferentes de implementación. En primer lugar, se utiliza un sistema de validación biométrica de la identidad de los y las votantes que, luego de ser habilitados por el sistema informático, pasan al sistema de emisión de sufragio basado en tecnologías de registro directo con comprobante en papel. El escrutinio se basa en el registro electrónico y se utiliza el papel para validar estadísticamente la integridad de la elección.

En el año 2017, la firma Smartmatic rompió sus relaciones abruptamente con el gobierno de Nicolás Maduro tras presentar denuncias públicas de que su sistema de votación había sido corrompido por el gobierno venezolano en el marco de la elección para el Constituyente de ese año.⁵

En la actualidad, Smartmatic se presenta como una de las oferentes de servicios de tecnologías electorales más activas de la región y ha brindado servicios en diversas regiones y países, desde Filipinas, Italia y ahora en el estado de California en los EE. UU.

3 Véase la presentación del experto en seguridad de sistemas de la información Diego Aranha en Ekoparty 2017 <https://www.youtube.com/watch?v=5JoOxriSh7o> (Visitado el 28 de septiembre de 2020).

4 Véase <https://www.bbc.com/mundo/noticias-america-latina-40808557>

5 Véase <https://www.bbc.com/mundo/noticias-america-latina-40804551> (visitado el 28 de septiembre de 2020).

En Argentina, la avanzada del voto electrónico se caracterizó por la utilización de los sistemas de la firma Magic Software que en el año 2004 realizó un registro de patentes sobre su método de votación basado en la incorporación de una boleta de voto electrónico que trae un chip RFID. En ese año, la empresa obtuvo una patente sobre esta tecnología, pero la perdió años más tarde por no pagar la tasa de renovación anual que es obligatoria en la oficina de propiedad industrial de Argentina. La patente sobre el sistema y método de votación registrado por la Firma MSA S.A. se encuentra hoy en dominio público.⁶ De la lectura de la memoria descriptiva de la patente se desprenden numerosas características que hoy son negadas por los proveedores del sistema, entre ellas la posibilidad de contabilizar los votos ingresados a una urna aún a cierta distancia y sin necesidad de abrir la misma. Esto se debe al sistema de chips RFID integrados a las boletas de votación, que son, según el análisis de los expertos en seguridad de la información, un punto de vulnerabilidad directo del secreto del sufragio.

La empresa MSA ha sido la principal beneficiaria de las licitaciones en las diversas implementaciones de voto electrónico en la República Argentina, especialmente en las provincias de Salta, Neuquén y en la Ciudad Autónoma de Buenos Aires. Es, a su vez, la empresa seleccionada para el próximo proceso electoral en Paraguay. Mientras tanto, Smartmatic ha estado intentando ingresar al mercado argentino con tecnologías y ha podido vender al Estado sistemas de identificación biométricos para la validación de identidad en las mesas electorales en las elecciones de medio término en 2017 y en las presidenciales de 2019. Estos sistemas no fueron usados en todo el país sino en la región del Noroeste y Noreste de la República Argentina, en particular en las provincias fronterizas.⁷

A lo largo de los últimos años hubo intentos de avanzar con sistemas de voto electrónico en Ecuador y Chile, pero tras diversos debates, idas y vueltas, finalmente en ninguno de esos países se logró modificar el sistema de emisión de sufragios.

El próximo paso en materia de voto electrónico en la región está enfocado en Paraguay. Antes de avanzar con esa iniciativa, es indispensable aprovechar la experiencia de lo sucedido en Argentina con el sistema que nuestro país está exportando como innovación y sobre el que consideramos no están dadas las garantías básicas y razonables del sistema democrático.

6 Una copia de la memoria descriptiva de la mencionada patente está disponible para consulta en el sitio web de la Fundación Vía Libre en <https://www.vialibre.org.ar/wp-content/uploads/2015/05/memoria.descriptiva.patente.votoelectronico.pdf> (visitado el 21 de Septiembre de 2020).

7 Véase <https://www.vialibre.org.ar/2017/08/04/sistema-de-identificacion-biometrica-en-elecciones-suma-de-problemas-y-ninguna-solucion/> (Visitado el 29 de septiembre de 2020)

3. ¿Qué garantías debe tener un sistema electoral?

El sistema electoral debe cumplir con tres requisitos indispensables que están fijados en las Constituciones Nacionales de cada uno de nuestros países y en los tratados internacionales de derechos civiles y políticos.

El sistema de votación debe asegurar secreto del voto, integridad de la elección y auditabilidad y transparencia del proceso. Esos son los tres requerimientos que debe arbitrar todo sistema electoral para cumplir con las garantías constitucionales vigentes.⁸

3.1. Secreto del voto

Toda elección legítima en un sistema democrático requiere que se mantenga la característica de una persona/un voto. Es necesario que se corrobore la identidad de cada votante para que ejerza ese derecho una sola vez y para que su voto no sea suplantado por terceras partes malintencionadas. Es por eso que se debe llevar un registro de votantes —padrón electoral— que debe corroborar que cada persona ha ejercido su derecho de manera apropiada sólo una vez. Pero, a la vez, se debe custodiar el secreto del voto, instrumento fundamental para asegurar la autonomía y libre voluntad de quien elige a sus representantes.

En América Latina hemos escuchado muchas veces la preocupación por el fenómeno del clientelismo político. Este elemento que se atribuye de forma regular a los partidos más populares y que ha generado numerosas investigaciones tanto académicas como judiciales sobre manipulaciones electorales, es uno de los elementos centrales de la crítica al actual sistema electoral en nuestros países. Se utiliza el concepto de clientelismo para denigrar procesos democráticos basados en el sistema tradicional de papeleta al que se asocia con lo antiguo y lo arcaico, frente a la promesa de modernidad y eficiencia del sistema de votación mediado por computadoras.

Sin embargo, lo que poco se explica es que la mejor herramienta que el sistema electoral tiene para morigerar los impactos del clientelismo político es el secreto del voto, que ofrece a la ciudadanía ese espacio de intimidad y resguardo para manifestar en las urnas su voluntad, libre de presiones de todo tipo.⁹ El sistema de cuartos oscuros o entornos de votación aislados y a resguardo de la mirada ajena junto con la posibilidad de elegir entre una diversidad de boletas en papel o de opciones en una boleta única impresa es un resguardo de esa selección frente al sistema digitalizado de votación.

8 Artículo 25 del Pacto Internacional de Derechos Civiles y Políticos
<https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx>

9 La posible vulneración del secreto del voto es uno de los elementos más certeros de ataque sobre sistemas informatizados. En general, es el mecanismo más común usado para atacar cualquiera de los sistemas y se ha corroborado la fragilidad de los mismos a la hora de custodiar el secreto de manera apropiada. De hecho, el propio Nicolás Maduro reconoció públicamente tener la lista de quienes votaron contra su gobierno en las elecciones de 2013, con el consiguiente condicionamiento y la amenaza a quienes pueden ser víctimas de represalias de todo tipo por su elección política. Véase <https://www.youtube.com/watch?v=AjG42CMOodk> (Visitado el 29 de septiembre de 2020).

Es claro que el clientelismo es un problema multidimensional y multicausal, pero si hay un resguardo clave justamente ese es el secreto del sufragio. Cualquier ataque al sistema de secreto del voto impacta de lleno en la autonomía de los y las votantes y torna ilegítimo el proceso.

Sin ánimo de entrar en tecnicismos, los sistemas informáticos utilizados en los procesos electorales tienen baja o nula capacidad de resguardar el secreto del sufragio, ya que la forma en la que administran y gestionan la información que procesan deja rastros y huellas que un atacante puede explotar incluso de manera remota.

El sistema de MSA que se atribuyó la licitación pública en Paraguay es uno de los más vulnerables en este sentido. En Argentina se han realizado diversas pruebas de concepto sobre ataques que resultaron exitosos, en particular por la característica propia del sistema que se basa en el almacenamiento del voto de forma distribuida en las boletas electrónicas dotadas de chips de identificación por radiofrecuencia.

El chip RFID es un sistema de almacenamiento y recuperación de datos remotos que se utilizan para transmitir la identidad de un objeto mediante ondas de radio. Cada chip tiene a su vez un número de serie único y puede ser leído a cierta distancia con mecanismos básicos y tecnologías muy rudimentarias y accesibles. Son tecnologías sencillas de múltiples usos, desarrolladas hace muchos años y puestas en producción en diversas áreas, son especialmente usados en sistemas de control de stocks en grandes cadenas de comercialización y en algunos sistemas de administración y gestión de ganado en el negocio agropecuario, entre miles de otros usos diversos. Su característica central es que pueden ser leídos a distancia.

A su vez, los sistemas de registro directo de votación (DRE) en los cuales los y las votantes interactúan con una pantalla de una computadora registran numerosas vulnerabilidades en materia de privacidad. En Holanda, país pionero en materia de voto electrónico, los sistemas de emisión digital de sufragio se suspendieron definitivamente en 2008 después de que un grupo de activistas y hackers documentara la posibilidad de leer el voto de una persona mientras lo emitía a varios metros de distancia, vulnerando así el principio fundamental de la privacidad del sufragio.

El mismo experimento se llevó adelante con éxito en Brasil, donde quedó demostrado que la principal vulnerabilidad del sistema electoral de nuestro vecino país es la posibilidad de quebrar el secreto del voto.

Sin secreto del voto, o con baja o nula confianza en la posibilidad de resguardar la privacidad en el sistema electoral, es prácticamente imposible luchar contra las prácticas clientelares y construir democracias sólidas basadas en la voluntad libre y autónoma de cada ciudadano y ciudadana al votar.

3.2. Integridad

Los sistemas informáticos, contrariamente al imaginario popular, son altamente vulnerables a fallas y errores. Estos errores además pueden pasar inadvertidos, ya que se trata de sistemas de caja negra que muy pocas personas conocen y de las que no conocemos exactamente el funcionamiento. No todas las vulnerabilidades y errores de los sistemas informáticos están ahí por la malicia de algún atacante, sino que son características propias de todo sistema de este tipo. Todos los sistemas tienen vulnerabilidades, algunas ya conocidas y otras por conocer. A su vez, los sistemas implementados en elecciones son estructuras complejas que dependen de múltiples piezas de *hardware* y software producto muchas veces de múltiples proveedores de diversas partes del mundo. El proveedor del sistema no tiene necesariamente control sobre toda la cadena de montaje de todas las partes integradas, por lo que en muchos casos se arrastran errores, problemas y vulnerabilidades de diversa índole. En algunos casos pueden ser problemas de *hardware*, de controladores, de sistema operativo, de aplicaciones e incluso del *software* usado específicamente para la elección. No es trivial la realización de una auditoría sobre estos sistemas, ya que requieren equipos multidisciplinarios y un conjunto de saberes especializados para la tarea. Vale agregar que auditar una máquina no asegura la integridad de todas ellas.

Es por esto que confiar la integridad del proceso electoral a sistemas de este tipo es una apuesta riesgosa, en particular cuando se realiza sin márgenes amplios de escrutinio público y equipos ampliamente especializados. En algunos condados de los EE. UU. donde se utilizan máquinas de votación electrónica desde hace años, se enfrentan con la problemática de la antigüedad de los equipos, la falta de controles apropiados de seguridad en materia de *software* y la actualización permanente que requiere cualquier sistema de cómputo, especialmente sistemas de misión crítica como los equipos para votar.¹⁰

En términos electorales, hablar de la integridad del sistema no es sólo mencionar la seguridad de cada uno de los instrumentos de votación, sino de contabilizar los votos tal y como fueron emitidos por la ciudadanía, ya que se trata de la expresión de su voluntad política, un acto central para el sistema democrático.

Velar por la integridad de la elección es una de las tareas más complejas de las autoridades electorales. Cuando se incorporan sistemas de votación electrónica agregamos una gruesa capa extra de complejidad, ya que es imposible garantizar que los registros electrónicos de los votos no sean adulterados, modificados o incluso eliminados.

¹⁰ Introducimos aquí el concepto de sistemas de misión crítica en línea con el informe preparado por el Consejo de Investigaciones Conicet en Argentina, ante requerimiento de evaluación de factibilidad de la implementación de tecnologías en el proceso electoral, la primera declaración de los expertos que realizaron el reporte para el Gobierno Argentino es la definición de los sistemas de votación como sistemas de misión crítica. «El *hardware* y *software* que implementa cualquiera de las fases en las que se ha dividido el proceso de votación pertenecen a la categoría de sistemas de misión crítica (o *missioncritical software-reliant system*), debido principalmente a los atributos de calidad en juego y a la reducida ventana de operación donde el sistema debe funcionar “casi sin fallas” (Axelrod, 2012 y U.S. Election Assistance Commission, 2017) . El desarrollo se vuelve aún más sensible en caso de considerar la automatización de la fase de emisión del voto.» Véase https://www.conicet.gov.ar/wp-content/uploads/Analisis_factibilidad_implementacion_tecnologia_proceso_electoral.pdf

Es por esta razón que en los últimos años, salvo en Brasil, se ha impuesto visión de que un sistema de votación electrónico siempre debe arrojar un comprobante en papel que la ciudadanía pueda corroborar a la hora de emitir el voto. Sin embargo, la impresión de una pa-peleta tampoco representa una garantía para la integridad del sufragio. ¿Cómo se resuelve cualquier diferencia entre el conteo manual y el conteo informático? ¿Se asegura la validez legal del conteo en papel? ¿Si el sistema en papel es finalmente el que se dictamina válido, qué sentido tiene la incorporación de todo el sistema informático aledaño? Todos los pro-veedores, en mayor o menos medida, han reconocido que el único reaseguro de integridad de la elección es el comprobante en papel. Entonces, ¿cómo se justifica la incorporación de todo el sistema con los consiguientes puntos de ataque y vulnerabilidades existentes?

3.3. Auditabilidad y transparencia

Finalmente, un tercer aspecto fundamental del sistema electoral es la creación de confianza para así dotar de legitimidad a todo el proceso, base de la legitimidad del sistema político en su conjunto. Los sistemas de votación electrónica agregan una capa de complejidad a un proceso que ya de por sí supone una serie de características propias multidimensionales.

En las democracias latinoamericanas hemos construido sistemas electorales que se basan fundamentalmente en la participación ciudadana. Es la propia ciudadanía la que, ejerciendo su derecho ciudadano pero a la vez su deber constitucional, contribuye al proceso electoral controlando los procesos de elección. La ciudadanía participa activamente y es protagonista de la jornada electoral en la que no sólo ejerce su derecho al voto sino que actúa como fiscal en representación de su partido político de preferencia y en otros casos como autoridad electoral de mesa por voluntariado y/o por carga pública.

Esta fiscalización del proceso electoral por parte de ciudadanos comunes como cualquiera de nosotras, sin formación técnica específica ni especialización en sistemas de seguridad de la información, se torna absolutamente imposible.

De hecho, es este el argumento nodal del fallo que el Supremo Tribunal Constitucional de Alemania emitió en el año 2009 con el cual descartó la utilización de sistemas de vota-ción electrónica en elecciones vinculantes y lo declaró inconstitucional.¹¹ El argumento de la transparencia y la auditabilidad se impuso a muchos otros y constituye un precedente importante. El proceso electoral es un acto público en si mismo, es un acto fundamente del sistema republicano y democrático y como tal debe asegurar la transparencia y la potestad ciudadana de control. Si para el ejercicio de ese contralor se debe contar con una capacita-ción especial que no está al alcance de la media de la ciudadanía ni disponible en el sistema de educación básico elemental que el Estado debe garantizar, entonces ese derecho que es colectivo y de toda la ciudadanía se vuelve un derecho exclusivo de una elite técnica acotada y no representativa.

Si a estos problemas generales le sumamos las dificultades propias de nuestra región, el pro-blema de la transparencia y auditabilidad se vuelve crítico. Ninguno de los proveedores de

¹¹ Sobre este tema ha trabajado ampliamente el jurista experto en derecho electoral José M. Perez Corti, Véase «Los principios generales del derecho electoral y su gravitación en la inconstitucionalidad del régimen alemán de voto electrónico» disponible en http://joseperezcorti.com.ar/Archivos/Bibliografia_Digital/Electoral/Revistas_Publicaciones_Regulares/TRIFE_Revista_Justicia_Electoral/2010_1_juel_a6_n2_1.pdf

sistemas de voto electrónico que operan en el mercado ha sido afín a la apertura para auditorías serias y reales de sus sistemas. En este sentido, la empresa MSA no es la excepción. Su código fuente sólo fue auditado de manera extraoficial por sucesivas filtraciones anónimas del código en Internet, lo que permitió que la comunidad informática argentina pusiera un ojo sobre un código que fue históricamente calificado como de muy baja calidad y magros resguardos de seguridad. Es destacable que hay incluso un fallo de la justicia argentina que reconoce que la seguridad del sistema de MSA era 'vaga'.¹²

A eso se suma el hecho de que la propia firma inició acciones penales e impulsó el allanamiento del domicilio de un investigador de sistemas que les reportó vulnerabilidades evidentes en los servidores de la compañía a pocos días de la elección local para Jefe de Gobierno y Legisladores de la Ciudad Autónoma de Buenos Aires en 2015. Este hecho no sólo marca altos niveles de irresponsabilidad de la firma y las autoridades electorales sino especialmente de la justicia que ante la certeza de una vulnerabilidad grave documentada a dos días de las elecciones, en lugar de exigir medidas de mitigación a la empresa o evaluar el riesgo de la elección, optaron por allanar al mensajero.¹³

En el imaginario colectivo abunda una idea de que la fiscalización de los procesos electorales es una pesada obligación. Por el contrario, es un derecho. Sin este proceso de contralor ciudadano es muy difícil garantizar unas elecciones limpias y libres.

¹² Véase <http://www.noticiasurbanas.com.ar/noticias/la-justicia-admitio-que-fallo-el-sistema-de-voto-electronico/>

¹³ Véase la narración de Joaquín Soriano en su charla Ted en Bariloche en <https://www.youtube.com/watch?v=mVNzLoI5U3k> (visitado el 29 de septiembre de 2020)

4. El problema de la propiedad intelectual y la privatización del sistema electoral

«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 (...).»
Fallo del Supremo Tribunal Constitucional Alemán, 2009.

Un tema pocas veces explorado en los debates sobre implementación de voto electrónico en nuestros países de la región es el de la propiedad intelectual y los procesos de privatización del sistema electoral.

Si bien este último aspecto es clave y ha sido tratado en algunas ocasiones, no parece haber preocupación en la clase política sobre el impacto real de la privatización de un proceso central de cualquier democracia.

La integración de un proveedor privado de servicios esenciales para el proceso electoral es un aspecto que debe ser cuestionado severamente cuando se trata de una función elemental de la construcción de confianza en el sistema. Es posible que a lo largo de un proceso electoral haga falta contratar proveedores privados que puedan realizar desde consultorías hasta impresión de boletas de votación. Sin embargo, integrar un actor privado en el acto central del sistema como es la emisión del voto suma una problemática clave. ¿Quién es ese proveedor? ¿Quiénes son los accionistas de esa empresa? ¿Qué intereses tiene esa empresa en relación a los diferentes partidos políticos de la contienda? ¿Es una empresa pública, radicada en el país, con suficientes credenciales en términos de transparencia? ¿Cuál es su relación con el gobierno que ha llevado adelante la contratación?

Hace algunos años, la cadena de televisión HBO estrenó un documental llamado *Hacking Democracy*. En esa producción se mostraron los intereses compartidos de la firma Diebold con altos funcionarios del partido republicano¹⁴.

A su vez, los cables de Wikileaks dieron cuenta de la preocupación que el Departamento de Estado de los EE.UU. tenía por las operaciones de la firma subsidiaria de la venezolana Smartmatic, Sequoia Voting Systems en sus elecciones. El gobierno norteamericano vio como una amenaza la posible injerencia venezolana en sus sistemas electorales y la firma caribeña tuvo que desprenderse de sus acciones en Sequoia. Recién tras la ruptura de Smartmatic con el gobierno de Nicolás Maduro en 2017 pudo ingresar al mercado norteamericano de venta de sistemas electorales. Esta pequeña anécdota da cuenta de que no es una pregunta trivial saber de dónde vienen y a quién responden los capitales de las firmas proveedoras de sistemas de votación.

Pero debemos sumar otro aspecto a la cuestión de la privatización del sistema: el problema derivado de la propiedad intelectual.

14 Véase el documental *Hacking Democracy* de la cadena HBO. <https://www.youtube.com/watch?v=OligO7fSUpk>

A partir de la entrada en vigencia de los acuerdos sobre aspectos de propiedad intelectual aplicados al comercio, cada país integrante de la Organización Mundial de Comercio asumió el compromiso de regular el software y las bases de datos en el mismo sentido que las obras musicales y artísticas, es decir, bajo el sistema de copyright y derechos de autor.

Esto significa que legalmente, los sistemas de cómputo que se utilizan en las máquinas de votación están regulados por sistemas de propiedad intelectual. En algunos casos, como el de la empresa MSA, incluso realizaron un registro del sistema bajo patente de invención.

La problemática de la propiedad intelectual y su tensión con el interés público abarca múltiples aristas, desde el acceso a medicamentos y tratamientos esenciales hasta la posibilidad de acceder a investigación científica. La tensión entre la propiedad intelectual y el interés público en sistemas electorales es, probablemente, uno de los menos explorados por parte de la comunidad de expertos en derechos de autor y patentes. Sin embargo, aparece como una preocupación constante en la comunidad de practicantes de la seguridad de sistemas de información.

¿A qué se debe esto? A que en buena medida, la práctica de la seguridad de sistemas de información está íntimamente ligada a la necesidad de evaluar la seguridad, integridad y confiabilidad de un sistema de cómputo y para esto es indispensable realizar ingeniería inversa de esos sistemas.

Es por eso que numerosos investigadores de sistemas de voto electrónico han sido amenazados y hasta perseguidos penalmente por su tarea de evaluar y reportar vulnerabilidades. Esta es una práctica que debería ser adoptada, legitimada, protegida e incentivada por cualquier autoridad electoral que se comprometa con la transparencia de un proceso de esta naturaleza. Lamentablemente, todavía no tenemos una conciencia clara de lo que significa la frase que da inicio a esta sección y que fue emitida por el Tribunal Constitucional Alemán. La propiedad intelectual siempre debe estar supeditada al interés público, más cuando se trata de transparencia electoral.

La exigencia de disponibilidad pública de todos los componentes de un sistema de votación electrónica debería ser la demanda básica de cualquier autoridad legislativa y electoral que asuma el riesgo de incorporar sistemas de votación electrónica, aún contra todas las advertencias de seguridad, integridad y vulneración de derechos civiles y políticos.

La experiencia regional indica que en ningún caso las empresas proveedoras entregaron voluntariamente el código fuente y el detalle de toda la implementación de sus programas a las autoridades electorales. De hecho, aún en casos en los cuales la legislación establecía total transparencia para la auditabilidad del proceso, esto jamás ocurrió de una forma apropiada. En las diversas elecciones en las cuales la firma MSA participó de procesos electorales en Argentina, los procesos de auditoría y revisión del código por parte de los apoderados informáticos de los partidos políticos se parecieron más a una farsa que a una auditoría seria. En todos los casos, técnicos de la empresa proveedora mostraron partes del código de la aplicación de votación en una pantalla durante una presentación y en ningún caso se habilitó la posibilidad de hacer pruebas reales sobre equipos y acceso pleno al código fuente. Siempre se dieron argumentos basados en la idea de la seguridad por oscuridad.

En otros países, en particular en los Estados Unidos, la experiencia de los investigadores de seguridad informática no es mucho mejor. El investigador Ed Felten, a cargo de una de las auditorías oficiales encargadas por el estado de New Jersey sobre máquinas de votación que fallaban sistemáticamente en las elecciones de ese distrito, recibió notificaciones amenazantes de violación de propiedad intelectual en el caso de que decidiera avanzar con el análisis de fallas y vulnerabilidades de la firma Sequoia.¹⁵ En India, un investigador fue arrestado por las autoridades por denunciar vulnerabilidades del sistema.¹⁶

La amenaza legal es una de las principales herramientas que las empresas de votación utilizan para evitar que investigadores independientes realicen auditorías apropiadas sobre sus sistemas. Las regulaciones de propiedad intelectual funcionan como instrumentos para que la ciudadanía no tenga acceso a información fundamental a la hora de evaluar un sistema electoral.

Con regulaciones de propiedad intelectual estrictas, con tipificación penal de las técnicas de ingeniería inversa, con potenciales persecuciones por supuestos delitos informáticos, se amedrenta y desincentiva la investigación de seguridad indispensable para conocer cómo funciona y reportar vulnerabilidades de sistemas de votación electrónica.

Sin auditorías reales, el ejercicio de derechos civiles y políticos mediados por votación electrónica queda opacado por dispositivos que lejos de favorecer la democracia los encierran bajo llave en cajas negras.¹⁷

15 Véase <https://freedom-to-tinker.com/2008/03/17/interesting-email-sequoia/>

16 Véase <https://www.wired.com/2010/08/researcher-arrested-in-india/>

17 Véase Documental Caja Negra – Fundación Vía Libre Argentina (2017) https://www.youtube.com/watch?v=zhjVVrVHsrQ&feature=emb_logo (visitado el 30 de Septiembre de 2020).



Esta obra está bajo una
Licencia Creative Commons
Atribución-CompartirIgual 4.0
Internacional.

