

ARTÍCULO MONOGRÁFICO

# **Voto electrónico: un peligro para la democracia\***

## **[Electronic voting: a danger for democracy]**

**GUNNAR EYAL WOLF-ISZAEVICH<sup>1</sup>**

**RECIBO: 25.08.2010 - AJUSTE: 20.09.2010 - AJUSTE: 17.11.2010 - APROBACIÓN: 27.11.2010**

### **Resumen**

*En varios países de Latinoamérica, las autoridades electorales están comenzando a voltear hacia las urnas de votación electrónicas. Los argumentos con los cuales presentan estas urnas a la población se centran particularmente en la disminución de costos del proceso electoral, una mayor agilidad en la obtención de resultados, y en poder tener más confianza en que las personas involucradas no engañen a la población con resultados ilegítimos, enfermedad de la cual Latinoamérica ha sufrido largamente.*

*Las urnas electrónicas no son ya una novedad. Han sido utilizadas por varios países, desde las primeras pruebas en la India en 1982 hasta una amplia base en la última década. Sin embargo, un análisis sobre las experiencias vividas en ellos dista de ser positiva - y dista de ser homogénea.*

*En el presente artículo serán analizados los desarrollos de estas tres líneas argumentativas resultan huecos, en el mejor de los casos, o directamente falaces. Se hace además una revisión de algunos casos emblemáticos de fallas que han llevado al replanteamiento -llegando incluso a la prohibición legal en algunos casos- del voto electrónico alrededor del mundo.*

**Palabras clave:** E-voto, voto electrónico, sociedad, democracia, experiencias internacionales

---

\* Modelo para citación de este artículo:  
WOLF ISZAEVICH, Gunnar Eyal (2010). Voto Electrónico: Un peligro para la democracia. En: Ventana Informática. No. 23 (jul.-dic., 2010). Manizales (Colombia): Universidad de Manizales. p. 181-195. ISSN: 0123-9678

1 B.Sc. Computer Science.  
Técnico Académico Asociado C de Tiempo Completo, Instituto de Investigaciones Económicas, Universidad Nacional Autónoma de México, México. Correos electrónicos: gwolf@iiec.unam.mx, gwolf@gwolf.org.

## Abstract

*Electoral authorities in several Latin American countries are turning their heads towards electronic voting booths. The arguments through which electronic voting is being presented to the population are mailed centered around reducing the costs of the electoral process, achieving better turnaround times for publishing electoral results, and being able to better trust that the involved actors do not cheat the population with illegitimate results, a disease Latin America has long suffered.*

*Electronic voting booths are not new. They have been used in several different countries, since the early implementations in India in 1982, and its usage has widely spread during the past decade. However, an analysis on the international experiences yields results far from optimistic -and far from homogeneous.*

*In this article, the outcome from the three above mentioned argumentative lines is analyzed, showing they are not sound, in the best case, or directly misleading. Some emblematic cases of failures around the world that have led to a serious reevaluation –and up to legal rulings banning its use– around the world are reviewed as well.*

**Keywords:** *E-voting, electronic voting, society, democracy, international experiences.*

## Introducción

Los promotores de las diferentes vertientes del Conocimiento Libre son los primeros en recalcar los tremendos fallos -de concepción y de implementación- que hacen que las estaciones computarizadas de emisión y contabilización de votos sean, desde su planteamiento, una causa perdida (Heinz, 2006) - Ninguna de las numerosas implementaciones a la fecha han salido airoosas ante el escrutinio (incluso casual) de expertos en seguridad (Felten, 2008a), a veces con resultados verdaderamente nefastos (Balzarotti, et. al., 2008a y 2008b). Los escrutinios generalmente han sido dirigidos por grupos de activistas independientes buscando señalar las deficiencias del proceso, con la muy notable excepción del ejemplo puesto por el Tribunal Superior Electoral de Brasil, el cual será abordado más adelante.

Obviamente, estos resultados no son del agrado de las compañías que buscan vender máquinas supuestamente seguras, diseñadas *ex-profeso* para el conteo de votos. Se han dado a conocer incluso amenazas he-

chas contra dichos equipos de investigadores (Felten, 2008b) por llevar a cabo estos análisis. En este caso, la demanda es que, en asuntos tan sensibles, relevantes y tan frágiles ante la intervención como la vida de una sociedad democrática, es sencillamente imposible asegurar los elementos básicos de *confiabilidad* y *auditabilidad*.

Cabe aclarar que la argumentación hecha en este capítulo no pone en duda los *fundamentos matemáticos* de diversos sistemas que serían aplicables a una votación electrónica, como las garantías descritas por Ruiz (2010), sino su *implementación*— Duda que se mantiene, como se ve más adelante, aún partiendo del supuesto de que el código está 100% disponible para su escrutinio. Lo que es más, algunos de los mecanismos descritos por Ruiz pueden ser empleados en contra del sistema democrático<sup>2</sup>.

Diversos argumentos han sido esgrimidos a favor del voto electrónico, pero pueden ser resumidos en tres:

- Disminución de costos: Un adecuado proceso democrático es caro. La papelería electoral debe ser impresa con mecanismos suficientes para asegurar su unicidad, deben proveerse mecanismos para garantizar que sólo los electores autorizados emitan su voto, y debe haber garantías de no manipulación para todos los componentes involucrados en el proceso. La automatización del proceso ayudaría a implementar estos candados a un menor costo.
- Agilidad en la obtención de resultados: No hay nada que genere mayor falta de confianza y suspicacia en los procesos que una demora en la publicación de los resultados. Se ha argumentado que a través del voto electrónico, los resultados pueden ser anunciados prácticamente de inmediato tras haberse cerrado la casilla.
- Confiabilidad de los actores: La experiencia de muchos países en torno a los fraudes electorales apunta dolorosamente a la falta de integridad de los actores involucrados en el proceso - Personas susceptibles ya sea a la compra de conciencias, a la extorsión, o directamente a la violencia física; si todo el proceso es controlado por computadoras, estos factores deberían perder peso.

---

2 Puede verse, como ejemplo, la prueba de la emisión de un voto basada en cero conocimientos: Si bien el esquema sugerido permitiría que cada votante individual verifique que su voto haya sido tomado en cuenta, sin divulgar el sentido de los votos de los demás, esta propiedad sería ideal para la compra de votos, tan tristemente común en América Latina. Si en una votación pudiera demostrarse el sentido del voto de determinado individuo, indudablemente habrá quien sepa exigirle a dicho individuo le demuestre que su voto fue realizado en el sentido “correcto”.

En las siguientes secciones se analiza por qué los tres argumentos caen ante un sencillo análisis.

## 1. Disminución de costos

La sociedad está acostumbrada a lidiar con los bemoles del voto *tradicional*, utilizando al papel como su medio primario. Una crítica muy común a éstos procesos, especialmente en los países cuyas democracias no están bien consolidadas (y que por tanto, requieren de mucho mayor inversión tanto en la vigilancia como en la promoción de la participación de las elecciones) es el costo.

En México, citando a un caso extremo (el sistema electoral más caro de América Latina (Urrutia y Martínez, 2009; Ojeda, Rueda y Chávez, 2010)), cada sufragio emitido tanto en las elecciones federales intermedias del 2009, como en las estatales del 2010, tuvo un costo superior a los 17 dólares, aunque hay estimaciones que lo llegan a ubicar en hasta 50 dólares, tomando en cuenta *gastos ocultos*. Como fue mencionado anteriormente, un rubro que en él, sin duda, podrían presentarse importantes ahorros es en la generación, el manejo y la custodia del material electoral. Sin embargo, como queda demostrado tras el estudio realizado por Feldman, Halderman y Felten (2007) a las estaciones de votación Diebold AccuVote-TS, las más difundidas en los Estados Unidos y que han sido responsables de la recopilación de votos de hasta uno de cada diez electores de dicho país, enfrentadas a un atacante con conocimiento técnico especializado, éstas máquinas presentan un nivel de confiabilidad ante ataques verdaderamente bajo, y permiten -requiriendo de un tiempo mínimo de acceso- la reprogramación resultando en resultados fraudulentos que serían prácticamente imposibles de lograr en una elección tradicional sin recurrir a métodos violentos.

Las vulnerabilidades descritas por Feldman, Halderman y Felten (2007) no son privativas a los equipos Diebold. En el sitio web, en el cual está publicado su artículo junto con un video de diez minutos demostrando su ataque y una lista de preguntas frecuentes mencionan:

- «¿Por qué estudiaron éstas máquinas Diebold? ¿Por qué no otras tecnologías para votos?
- Estudiamos estas máquinas porque son las que conseguimos. Si hubiésemos tenido acceso a otro tipo de máquinas, probablemente las hubiéramos estudiado.
- ¿Son otras máquinas más seguras que las que estudiaron?

- No lo sabemos. Esperamos que así lo sean -las elecciones dependen ya de ellas- pero no hay suficiente evidencia para responder a esta pregunta
- Un rastro impreso verificado por cada votante es la protección más importante que puede hacer más seguras a las máquinas de voto electrónico».

El último punto mencionado es de especial relevancia: *Un rastro impreso verificado por cada votante*. La única garantía que un votante puede tener de que su voto fue registrado correctamente es que el sistema genere una boleta *impresa y de carácter irrevocable*, misma que sea verificada por el votante al instante, la cual se convertirá en el documento probatorio de la elección<sup>3</sup>. No hay manera -ver la cita de Thompson (1984) en la sección *Confiabilidad de los actores*- de que el estado interno de una computadora sea confiable, y muchísimo menos al tratarse del proceso más importante y más sensible de la vida política de un país.

Incluso obviando esto, incluso si el único argumento fuera el económico, la adopción de un sistema electrónico de votación sigue resultando más caro que llevar a cabo una votación tradicional: El Tribunal Supremo de Elecciones de Costa Rica anunció que no implementará urnas electrónicas por su elevado costo (Villalobos, 2009); al hacer este anuncio (y reforzando lo que se revisará en la sección *Agilidad en la obtención de resultados*), el presidente del TSE, Luis Antonio Sobrado, reconoció que hay «algunos riesgos que conlleva la puesta en marcha del voto electrónico como es el tener las urnas en línea, medida que a la fecha ningún país en el mundo ha querido asumir en este tipo de iniciativas».

Esto lleva entonces a una contradicción: El equipo de votación no es barato, en términos absolutos. Su adquisición por parte de un gobierno o ente de autoridad podría justificarse si se plantea prorratar a lo largo de varias elecciones -pero si éste tiene que estar sujeto a una estricta vigilancia continua, incluso en los años en que no será utilizado-. Debe recibir mantenimiento, y debe abastecerse con una cantidad no despreciable de insumos, para asegurar un rastro impreso verificado. Además, en caso de sufrir un desperfecto, todas las casillas deben tener un plan de respaldo: Casi indefectiblemente, esto significaría tener papelería tradicional para enfrentar desde un desperfecto del equipo hasta un

---

3 Y claro está, es fundamental que cada una de estas boletas sea generada por separado, recortada de la inmediata anterior y posterior, con garantía de que no haya un patrón observable en el corte, para garantizar el anonimato del elector

sabotaje, por ejemplo, en el suministro eléctrico. Por tanto, el supuesto ahorro puede volverse contraproducente, convirtiéndose en un gasto mucho mayor al que implican las votaciones tradicionales.

## 2. Agilidad en la obtención de resultados

Una de las principales obsesiones de la sociedad actual es la velocidad del acceso a la información. Los medios electrónicos de comunicación y el uso de Internet han acostumbrado a los ciudadanos a que la información debe estar disponible tan pronto ocurren los hechos, y debe llegar a toda la sociedad tan pronto está disponible.

Los sistemas electorales, en general, estipulan que para no manipular los resultados de una elección en proceso, no deben darse a conocer sus resultados parciales hasta que haya cerrado la última de las urnas. No hacerlo de esta manera significaría que el conocimiento público de la tendencia influiría en los resultados de muchas maneras indeseables. Sin embargo, una vez que cierra ésta última urna, en la mayor parte de las democracias modernas hay un periodo típicamente de un par de horas en que es necesario esperar a que las autoridades electorales recopilen la información generada por típicamente decenas de miles de casillas y den a conocer el resultado. Hay una gran presión por parte de los ciudadanos, y muy especialmente de los medios, para que las autoridades electorales publiquen los resultados *de inmediato*. Además del apetito por la información expedita, esto viene fundamentado en ejemplos de ocultamientos de información que eran realizados conforme los números comenzaban a fluir.

Ejemplo de esto son las declaraciones que hizo, veinte años más tarde, Manuel Bartlett Díaz, quien fuera en 1988 Secretario de Gobernación y presidente de la Comisión Federal Electoral durante las muy cuestionadas elecciones presidenciales de ese año: «La decisión de no dar a conocer datos preliminares fue tomada por el presidente Miguel de la Madrid, dado que, cito: si se oficializaba en ese momento –con datos parciales– que Cárdenas Solórzano iba ganando, al final nadie aceptaría un resultado distinto» (Becerril, 2008).

En la experiencia mexicana, la situación ha cambiado radicalmente de la imperante hace tan sólo dos décadas, como claro resultado de las frecuentes acusaciones de fraude electoral que dicho sistema electoral ha sufrido. En vez de una demora cercana a una semana, el Instituto Federal Electoral y las autoridades correspondientes de cada uno de

las entidades federativas publican los resultados de las *encuestas de salida* y los *conteos rápidos* típicamente dentro de las dos primeras horas tras haber concluido la votación, siempre que haya suficiente margen estadístico para no causar confusión en la población.

Impulsar una solución con tantos riesgos como una urna electrónica para ganar como tope estas dos horas sencillamente no tiene sentido. Además, el tiempo invertido por los funcionarios electorales en cada casilla en el conteo de votos emitidos es sólo una fracción del dedicado a las tareas de verificación y protocolización que deben llevarse a cabo antes de declarar concluida una elección. Sumando esto a que —por consideraciones de seguridad<sup>4</sup>— las estaciones de voto no están pensadas para contar con conectividad a red (y que ni los países más industrializados cuentan con una cobertura de Internet del 100% de su territorio), por lo cual debe haber forzosamente un paso manual de comunicación de resultados al centro de control de la autoridad electoral, el argumento de reducción de tiempos queda descartado.

Federico Heinz (2006), cierra su texto *¿El voto electrónico mejora la democracia?* con la siguiente idea: «Una alternativa factible es realizar la votación mediante formularios que contengan a todos los partidos, dejar que los votantes marquen su elección con tinta, y usar un scanner óptico para hacer un escrutinio automático, verificable mediante un simple recuento manual. No hay nada en contra de un escrutinio electrónico, pero digitalizar el acto mismo de la emisión del voto es extremadamente peligroso para la democracia».

El uso de boletas de papel y tinta aptas para ser escaneadas por equipo de reconocimiento óptico puede ser la opción más adecuada en este sentido. Permite la verificación de cientos de boletas en apenas un par de minutos, y permite conservar todos los atributos positivos del sistema tradicional.

### 3. Confiabilidad de los actores

Algunos proponentes del voto electrónico mencionan que con el voto tradicional en papel todos estos fraudes siempre han existido<sup>5</sup>, y que

---

4 Si es de preocupar la falta de seguridad en una computadora que corre aislada de atacantes externos, no tiene sentido siquiera entrar en detalles respecto a la cantidad de riesgos que supondría tenerla conectada a Internet.

5 Por ejemplo, reseñando a la videoconferencia en que este tema fue presentado en el marco del Seminario en que se desarrolló el proyecto, Beatriz Ramírez refiere (<http://seminario.edu-sol.info/resena/beatriz-ramirez/2009/03-1>): «De acuerdo a mi experiencia, como ciudadana

éste no agrava los riesgos. Sin embargo, más que reducir las posibilidades de los agentes fraudulentos, al implementar el voto electrónico, se estaría aumentando la profundidad a la que podrían llegar, y lo que es más importante aún, imposibilitando cualquier acción de auditoría o rendición de cuentas.

La votación electrónica tiene muchas modalidades y muchas aristas. En líneas generales, y contrario a lo que muchos esperarían, los expertos en seguridad informática y los activistas sociales involucrados en esta lucha no recomiendan exigir que las urnas electrónicas estén basadas en Software Libre para su funcionamiento, sino que sencillamente recomiendan en contra de su utilización. «El mecanismo de auditar completamente el funcionamiento de las urnas es impracticable. Esta es una tarea que sólo podría ser ejecutada por una elite de especialistas, de los que hay muy pocos en el mundo, y requiere la cooperación de las empresas que proveen las urnas así como de todos sus proveedores. Y aún si consiguiéramos todo eso, la eficacia de una auditoría sería más que dudosa: no sólo debemos garantizar que todo el software es correcto (lo que es imposible), sino que además debemos verificar que el software presente en las urnas el día de la elección es idéntico al auditado, tarea que nuevamente requiere de especialistas. ¿Y por qué hemos de confiar en los especialistas, si no queremos confiar en sacerdotes ni en empresas? Una de las muchas virtudes del “anticuado” sistema de escrutinio tradicional es que cualquier persona que sepa leer, escribir y hacer operaciones de aritmética elemental está en condiciones de controlarlo. Esta es una característica esencial y no debemos renunciar a ella» (Heinz, 2006).

Uno de los más interesantes argumentos que ilustran por qué las urnas electrónicas carecen inherentemente de confiabilidad es el presentado -sin aplicarlo en éste ramo específico- por Ken Thompson en 1983 (Thompson, 1984), en su discurso al recibir el Premio Turing de la ACM<sup>6</sup>, hace una sencilla demostración de por qué un sistema que llega al *usuario final* (y esto es mucho más cierto hoy en día que en 1983, en que los lenguajes y marcos de desarrollo utilizados suben increíblemente en la escala de la abstracción comparado con lo existente entonces) es prácticamente imposible de auditar por completo un programa, ni siquiera teniendo su código fuente, *ni siquiera teniendo el código fuente del compilador*. Traduciendo de las conclusiones de Thompson: «La moraleja es obvia. No puedes confiar en el código que

argentina, no he estado libre del robo —perdón quise decir “extravío”— de encomiendas postales, ni es secreto que en Argentina votan en elecciones presidenciales, cantidad de muertos».

6 Premio al que comúnmente se hace referencia como el *Nobel del cómputo*.

no creaste tú mismo. (Especialmente código proveniente de compañías que emplean a gente como yo). No hay un nivel suficiente de verificación o escrutinio de código fuente que te proteja de utilizar código no confiable. En el proceso de demostrar la posibilidad de este tipo de ataque, elegí al compilador de C. Podría haber elegido a cualquier programa que manipule a otros programas, como al ensamblador, cargador, o incluso microcódigo embebido en el hardware. Conforme el nivel de programación se vuelve más bajo, estos fallos se volverán más y más difíciles de detectar. Esta vulnerabilidad bien instalada en microcódigo será prácticamente imposible de detectar».

Este argumento ha sido clave para llegar a conclusiones como la adoptada en marzo del 2009 por la Corte Suprema de Alemania: «Un procedimiento electoral en el que el elector no puede verificar de manera confiable si su voto fue registrado sin falsificación e incluido en el cálculo del resultado de la elección, así como comprender cabalmente de qué manera los votos totales emitidos son asignados y contados, excluye del control público a componentes centrales de la elección, y por lo tanto no alcanza a satisfacer las exigencias constitucionales» (BVerfG, 2009 y Heinz, 2009).

El punto de la confiabilidad es el que más fervientemente se sigue debatiendo. El caso brasileño resulta muy esperanzador: A diferencia de la mayor parte de los gobiernos de países supuestamente desarrollados, en Brasil la tecnología utilizada para el voto electrónico está completamente basada en tecnología desarrollada localmente, empleando software libre. En noviembre del 2009, el Tribunal Superior Electoral brasileño convocó a la comunidad de seguridad a encontrar vulnerabilidades sobre las estaciones receptoras de votos, a cambio de una recompensa económica para los mejores análisis (TSEB 2009). Dentro de los términos estipulados, sólo uno de los participantes (Sergio Freitas da Silva) logró su propósito (Busaniche, 2009). Y si bien no logró vulnerar los resultados de éste sistema, si logró -mediante un monitoreo de las radiaciones electromagnéticas- averiguar por quién emitía su voto cada uno de los electores, rompiendo el principio de secrecía electoral, empleando únicamente equipo casero de bajo costo al buscar que esto fuera meramente una prueba de concepto; un atacante determinado podría utilizar equipo mucho más sofisticado para intervenir las votaciones a mucha mayor distancia.

Y si bien, el sistema empleado por Brasil sale mucho mejor parado que los empleados en Europa y Estados Unidos, no debe tomarse la ausencia de evidencia por evidencia de ausencia: Lo único que demostraron

es que ninguno de los atacantes pudo demostrar una vulnerabilidad en el periodo estipulado, o no quiso hacerlo por el precio ofrecido, pero nada indica que no haya fallas no encontradas... o peor aún, *puertas traseras* intencionales.

## 4. Experiencias internacionales

Por último, se presenta un listado de experiencias en diversos países, ilustrando muy brevemente el tipo de problemas a que puede conducir la adopción del voto electrónico. Queda claro que esta no es una lista comprehensiva, sólo indicativa. Para una descripción mucho más exhaustiva, se sugiere consultar UMIC-ASC (2009).

- En 2004, el Secretario de Estado de California, Kevin Shelley, *des-certificó* y prohibió el uso de ciertos modelos de urnas electrónicas Diebold en cuatro condados, y ordenó a 10 condados adicionales dar pasos para mejorar la seguridad y confiabilidad de dichos equipos (Lucas, 2004), al descubrirse que el software con que habían sido enviadas dichas urnas no era el mismo sometido a la certificación.
- La elección municipal de 2005 en Montreal, Canadá, se realizó utilizando urnas electrónicas, con resultados desastrosos (del orden de 45000 votos fueron contabilizados doblemente, según Geist, 2006). La autoridad electoral realizó un análisis de las elecciones, y publicó un amplio reporte (DGEQ, 2006) analizando las causas y cursos de acción a seguir, entre los cuales se menciona la necesidad de tener acceso completo al código fuente, el empleo de pruebas de funcionalidad, establecimiento de un plan de respaldo en caso de problemas, la implementación de medidas estrictas para almacenamiento y resguardo de los equipos. Marcel Blanchet, funcionario electoral en jefe opina que las urnas y terminales de votación electrónicas son tecnologías vulnerables. Más allá, la manera en que fueron manejadas no ofrece suficiente garantía de transparencia y seguridad para asegurar la integridad del voto.
- Ed Felten ha escrito en repetidas ocasiones respecto a lo inadecuadas que son diversas urnas electrónicas. Uno de los primeros ejemplos que publicitó, en 2006, es la pobre seguridad física en dichos equipos: Las urnas pueden ser abiertas por una llave genérica de cajones de oficina y *minibares* de hotel (Felten, 2006).
- En Argentina, en 2007, se ensayó el voto electrónico en la localidad de Las Grutas, provincia de Río Negro. Hubo una muy gran cantidad

de discrepancias entre el padrón electoral y el padrón registrado digitalmente, con lo que muchos votantes no pudieron expresar su voluntad. Mientras en las mesas tradicionales se registró del orden del 70% de votación, en las mesas con urna electrónica sólo se llegó al 40%. Además de esto, por errores en el manejo de la urna por parte de las autoridades de una de las casillas, ésta eliminó los registros en vez de guardarlos en la memoria externa (Salinas, 2008). El ciudadano Sergio Daniel Plos presentó un amparo para que su localidad no volviera a participar en elecciones electrónicas, escrito al cual se adhirieron aproximadamente el 10% de los votantes de la localidad (Busaniche, 2007). En 2010, ante pasos que llevarían a la implantación de voto electrónico en la provincia de Salta, políticos de diversos partidos interpusieron un recurso refiriéndose al caso de Las Grutas (Busaniche, 2010).

- Felten (2008a) exhibe también el ejemplo de una estación de votación para las elecciones primarias en Nueva Jersey, 2008, en que se puede ver un error aritmético al calcular la suma de votos.
- Las elecciones presidenciales de los Estados Unidos de América de noviembre de 2008, si bien no presentaron los graves problemas de legitimidad que sufrieron en 2000 y 2004, hubo irregularidades en varios Estados. El periódico Anchorage Daily News (Alaska), de acuerdo con Gordon (2008), reseña los siguientes casos: En Virginia y Pensilvania hubo varias descomposturas en las urnas electrónicas, lo que evitó que muchas personas ejercieran su derecho a voto. En algunos casos, les fueron presentadas boletas de tipo erróneo. Por otro lado, en Michigan, el día anterior a la elección se descubrió que varias de las urnas electrónicas presentaban desperfectos, por lo cual se instrumentó una votación tradicional — pero sin papelería electoral específica que presentara las garantías adecuadas de unicidad.
- Las elecciones primarias del Partido Laborista en Israel, 2008, tuvieron que ser pospuestas una vez que habían iniciado, dado que las urnas presentaban problemas de usabilidad... Algunas pantallas no registraban las respuestas de los votantes, otras registraban votos cuando no habían sido aún tocadas, o marcaban opciones equivocadas (Khoury, Singer-Heruti, Ilani 2008). Las fallas fueron generalizadas, tanto que el partido tuvo que cancelar la operación y repetirla al día siguiente al estilo *tradicional*, con sobres, papeletas y una urna de cartón.
- Después de que Holanda fuera uno de los países pioneros en implementación de urnas electrónicas, el grupo *Wij vertrouwen*

*stemcomputers niet* (*No confiamos en las computadoras votantes*) presentó en vivo, en el programa de televisión EénVandaag, cómo modificar la programación de las urnas electrónicas *Nedap*. Este hecho llevó a un amplio debate, que culminó con un reporte de la Comisión Asesora en Procesos Electorales, recomendando en 2008 revertir la recomendación que llevó a la implementación del voto electrónico, y rechazando la propuesta de reimplementar una nueva generación de urnas electrónicas paliando este problema, según WVSC (2009) y EPAC (2007). Hoy en día, los procesos electorales holandeses son nuevamente en papel, con conteo manual.

- Todo aparato electrónico emite radiación electromagnética dependiendo de sus procesos internos, mismos que pueden ser *olfateados* por equipos ubicados hasta a decenas de metros. Un ejemplo de esto, hecho completamente con equipo casero, es el ataque resultante de la convocatoria del Tribunal Superior Electoral de Brasil (TSEB, 2009), por medio del cual, con equipo completamente casero, el atacante logró averiguar el sentido de cada uno de los votos sin acceso al equipo (Busaniche, 2009 y Felitti 2009).
- En La India, prácticamente la totalidad de la población vota en urnas exclusivamente electrónicas (EVM), desarrolladas por el gobierno nacional en las últimas dos décadas. El funcionamiento interno de estos equipos se había mantenido en secreto para evitar que la comunidad dedicada a la seguridad en cómputo encontrara vulnerabilidades; en abril del 2010, un grupo liderado por Alex Halderman, Hari Prasad y Rop Gonggrijp consiguió una EVM y publicó dos ataques que pueden ser llevados a cabo en unos cuantos minutos, y permiten alterar los resultados. Dado que la EVM no produce rastro en papel y la única evidencia es su estado interno, esta modificación es indetectable, y resulta simple “obligar” a estas máquinas a entregar resultados fraudulentos.

## 5. Conclusiones

Casos ilustrativos de fracasos con urnas electrónicas hay de sobra -los aquí presentados y muchos más-. Claro está, hay también importantes casos de éxito. Si la discusión respecto a la conveniencia del voto electrónico sigue sobre la mesa, a casi 30 años de sus primeras aplicaciones internacionales, es reflejo de que en la amplia mayoría de los casos las urnas electrónicas sí han dado resultados aceptables a la sociedad.

Sin embargo, presentar un listado de países o regiones que han implementado esquemas de voto electrónico sin registrar incidentes está más allá del propósito del presente trabajo — No motivados por un ánimo de demeritar a dicha tecnología, sino por lo expuesto hacia el final de la sección 3: *No debemos tomar la ausencia de evidencia por evidencia de ausencia*. El que dichas votaciones hayan sido exitosas no significa necesariamente que no haya podido haber fraude de tipo alguno, sino que en caso de presentarse, éste podría no haber ser detectado.

Lo fundamental de los argumentos y casos aquí presentados no es el impacto que hayan tenido o que se hayan detectado a tiempo. Lo principal es que hacen patentes, en diversas dimensiones, los problemas de confiabilidad no sólo en los supuestos fundamentos de funcionamiento sino que en la misma naturaleza humana.

Incluso para tareas aparentemente tan simples como la de sumar votos, nadie ha sido capaz de producir un sólo proceso tan confiable y auditable como la revisión humana de papeletas físicas.

Los diversos trabajos que se han realizado buscando dar mayor fuerza a alguno de los atributos de la democracia basados en voto electrónico invariablemente hacen que los demás atributos pierdan. Dar verificabilidad a los votos emitidos a través del empleo de algoritmos criptográficos va en demérito del voto secreto; habilitar el acceso a las estaciones de votación desde computadoras conectadas a red se contrapone a un adecuado nivel de verificación de la identidad de cada votante; el confiar en la programación de una máquina para realizar el conteo va en contra de la *auditabilidad* del proceso por cualquier ciudadano. El voto electrónico no se volverá confiable al desarrollarse algoritmos adecuados, sino que —sea como sea que esté planteado— siempre representará una regresión en la confiabilidad del proceso más importante en la vida de una sociedad democrática.

Es por esto que la conclusión principal a la que el presente trabajo arriba es que el voto a través de urnas electrónicas no sólo es inadecuado el día de hoy para las necesidades de las sociedades latinoamericanas (y de otras latitudes), sino que es un tema con fallos insalvables desde su mismo planteamiento.

Un sistema democrático requiere, en primer y muy destacado lugar, de confiabilidad. Los argumentos por medio de los cuales se invita al voto electrónico son falaces, y más que resolver una problemática, la exacerban.

## Bibliografía

- BALZAROTTI, Davide; BANKS, Greg; COVA, Marco, FELMETSGER, Viktoria; KEMMERER, Richard; ROBERTSON, William; VALEUR, Fredrik and VIGNA, Giovanni (2008a) Are Your Votes Really Counted?: Testing the Security of Real-world Electronic Voting Systems [en línea] En: International Symposium on Software Testing and Analysis; ISSTA'08. (20-24/07/2008). Seattle (WA. USA): ACM. ISBN: 978-1-59593-904. <[http://www.cs.ucsb.edu/~seclab/projects/voting/issta08\\_voting.pdf](http://www.cs.ucsb.edu/~seclab/projects/voting/issta08_voting.pdf)> [consulta: 11/07/2010]
- BALZAROTTI, D. et. al. (2008b) Evaluating the Security of Electronic Voting Systems [en línea]. Santa Barbara (California, USA): Department of Computer Science, University of California. <<http://www.cs.ucsb.edu/~seclab/projects/voting/index.html>> [consulta: 19/10/2010]
- BECERRIL, Andrea (2008) De La Madrid me ordenó no informar que Cárdenas iba ganando, asegura Bartlett [en línea] En: Periódico La Jornada (03/07/2008). México D.F. (México): DEMOS, Desarrollo de Medios, S.A. de C.V. <<http://www.jornada.unam.mx/2008/07/03/index.php?section=politica&article=013n1pol>> [consulta: 07/2010]
- BUSANICHE, Beatriz (2007) Recurso de amparo contra el voto electrónico en Río Negro [en línea]. 07/12/2007. Córdoba (Argentina): Fundación Vía Libre. <<http://www.vialibre.org.ar/2007/12/07/recurso-de-amparo-contra-el-voto-electronico-en-rio-negro/>> [consulta: 28/05/2010]
- BUSANICHE, Beatriz (2009) Un investigador logra violar el secreto del voto en las urnas brasileñas [en línea] 02/12/2009. Córdoba (Argentina): Fundación Vía Libre. <<http://www.vialibre.org.ar/2009/12/02/un-investigador-logra-violar-el-secreto-del-voto-en-las-urnas-brasilenas/>> [consulta: 29/12/2009].
- BUSANICHE, Beatriz (2010) Partidos políticos impugnan el uso de voto electrónico en Salta. 28/05/2010. Córdoba (Argentina): Fundación Vía Libre. <<http://www.vialibre.org.ar/2010/05/28/partidos-politicos-impugnan-el-uso-de-voto-electronico-en-salta/>> [consulta: 28/05/2010]
- BVERFG (2009) Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können. [en línea]. Leitsätze zum Urteil des Zweiten Senats vom 3. (März, 2009), paragraph 1-163. Karlsruhe (Deutsche): Bundesverfassungsgericht. <[http://www.bverfg.de/entscheidungen/cs20090303\\_2bvc000307.html](http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html)> [consulta: 28/05/2010]
- DGEQ, DIRECTEUR GÉNÉRAL DES ÉLECTIONS DU QUÉBEC (2006). Rapport d'évaluation des nouveaux mécanismes de votation. Inf. Téc. [en línea] Québec (Canada): Directeur général des élections du Québec. <<http://defids.qc.ca/english/news-detail.php?id=2624>> [consulta: 05/07/2010]
- EPAC, ELECTION PROCESS ADVISORY COMMISSION (2007). Voting with confidence [en línea] The Hague (The Netherlands): Ministry of the Interior and Kingdom Relations. 27/09/2007. 74 p. <<http://www.unic.pt/images/stories/publicacoes1/Votingwithconfidence.pdf>> [consulta: 05/07/2010]
- FELDMAN, Ariel J.; HALDERMAN, J. Alex and FELTEN, Edward W. (2007) Security Analysis of the Diebold AccuVote-TS Voting Machine [en línea] En: Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07) (08/2007). Princeton (New Jersey, USA): Princeton University. <<http://itpolicy.princeton.edu/voting/>> 24 p. [consulta: 05/07/2010]
- FELITTI, Guilherme (2009) Perito quebra sigilo e descobre voto de eleitores em urna eletrônica do Brasil. [en línea]. En: Revista "IDG Now!". Segurança, Privacidade. (20/11/2009). Sao Paulo (Brasil): Now!Digital Business Ltda <<http://idgnow.uol.com.br/seguranca/2009/11/20/perito-quebra-sigilo-eleitoral-e-descobre-voto-de-eleitores-na-urna-eletronica/>> [consulta: 05/07/2010]
- FELTEN, Ed (2006) "Hotel Minibar" Keys Open Diebold Voting Machines [en línea] Princeton (New Jersey, USA): Freedom to Tinker <<http://freedom-to-tinker.com/blog/felten/hotel-minibar-keys-open-diebold-voting-machines>> [consulta: 04/07/2010]
- FELTEN, Ed (2008a) Evidence of New Jersey Election Discrepancies. [en línea] Princeton (New Jersey, USA): Freedom to Tinker <<http://freedom-to-tinker.com/blog/felten/evidence-new-jersey-election-discrepancies>> [consulta: 04/07/2010]
- FELTEN, Ed (2008b) Interesting Email from Sequoia. [en línea] Princeton (New Jersey, USA): Freedom to Tinker <<http://freedom-to-tinker.com/blog/felten/interesting-email-sequoia>> [consulta: 04/07/2010]

- GEIST, Michael (2006) Time To Cast A Vote Against E-Voting [en línea] (23/10/2006) Ottawa (Canada) <<http://www.michaelgeist.ca/content/view/1491/159/>> [consulta: 07/07/2010]
- GORDON, Greg (2008) Glitches hamper voting in five states [en línea]. En: Anchorage Daily News (04/11/2008). Anchorage (Alaska, USA): The Anchorage Daily News, a subsidiary of The McClatchy Company. <<http://www.adn.com/2008/11/04/578431/glitches-hamper-voting-in-five.html>> [consulta: 05/07/2010]
- HEINZ, Federico (2006) ¿El voto electrónico mejora la democracia? Voto electrónico: Los riesgos de una ilusión [en línea]. 07/10/2006. Córdoba (Argentina): Fundación Vía Libre. <<http://www.vialibre.org.ar/2006/10/07/el-voto-electrnico-mejora-la-democracia/>> ISBN: 978-987-22486-5-9 [consulta: 06/03/2009]
- HEINZ, Federico (2009) Alemania: urnas electrónicas anticonstitucionales [en línea]. 06/03/2009. Córdoba (Argentina): Fundación Vía Libre. <<http://www.vialibre.org.ar/2009/03/06/alemania-urnas-electronicas-anticonstitucionales/>> [consulta: 06/03/2009]
- KHOURY, Jack; SINGER-HERUTI, Roni and ILANI, Ofri (2008) Labor sets primary for tomorrow after computer failure [en línea]. En: Haaretz (03/12/2008). Tel Aviv (Israel): Haaretz Newspaper <<http://www.haaretz.com/print-edition/news/labor-sets-primary-for-tomorrow-after-computer-failure-1.258707>> [consulta: 06/03/2009]
- LUCAS, Greg (2004) State bans electronic balloting in 4 counties. [en línea] En: San Francisco Chronicle (01/05/2004) San Francisco (California, USA): Hearts Communications Inc. <<http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/05/01/MNG036EAF91.DTL>> [consulta: 06/3/2009]
- OJEDA LAJUD, Olga; RUEDA, Rivelino y CHÁVEZ, Víctor (2010) El voto mexicano cuesta 18 dólares; es el más caro de América Latina [en línea]. En: El Financiero (20/05/2010) México D.F. (México): El Financiero S.A. de C.V. / El Financiero Comercial S.A. de C.V. Consultado en: 20/05/2010 <http://impreso.elfinanciero.com.mx/pages/NotaPrint.aspx?IdNota=320373> [consulta: 20/05/2010]
- RUIZ DUARTE, Eduardo (2010). Álgebra de votaciones para procesos electorales [en línea]. 11/02/2010 <<http://b3ck.blogspot.com/2010/02/algebra-de-votaciones-para-procesos.html>> [consulta: 28/05/2010]
- SALINAS, Yamil (2008) Experiencia fallida de voto electrónico en Argentina [en línea]. 22/07/2008. <<http://www.yamilsalinas.net/2008/07/22/experiencia-fallida-de-voto-electronico-en-argentina/>> [consulta: 28/05/2010]
- THOMPSON, Ken (1984) Reflections on trusting trust. [en línea]. En: Communications of the ACM (08/1984) p. 761-763. ISSN: 0001-0782. New York (NY, USA): Association for Computing Machinery, ACM. <[http://portal.acm.org/citation.cfm?id=358210&jmp=cit&coll=portal&dl=ACM&CFID=//cacm.acm.org/magazines/1984/8&CFTOKEN=cacm.acm.org/magazines/1984/8\\$\\$CIT](http://portal.acm.org/citation.cfm?id=358210&jmp=cit&coll=portal&dl=ACM&CFID=//cacm.acm.org/magazines/1984/8&CFTOKEN=cacm.acm.org/magazines/1984/8$$CIT)> [consulta: 27/05/2010]
- TSEB, TRIBUNAL SUPERIOR ELEITORAL DO BRASIL (2009). Teste de segurança do sistema eletrônico de votação [en línea]. Brasília DF (Brasil): Tribunal Superior Eleitoral do Brasil <[http://www.tse.gov.br/internet/eleicoes/teste\\_seguranca.htm](http://www.tse.gov.br/internet/eleicoes/teste_seguranca.htm)> [consulta: 29/12/2009]
- UMIC-ASC (2009) (UMIC Agência para a Sociedade do Conhecimento) Electronic Voting Experiments in Political Elections around the World [en línea]. . Porto Salvo (Portugal): UMIC - Agência para a Sociedade do Conhecimento; Ministério da Ciência, Tecnologia e Ensino Superior. (Last updated: 19/07/2010) <[http://www.english.umic.pt/index.php?option=com\\_content&task=view&id=3113&Itemid=448](http://www.english.umic.pt/index.php?option=com_content&task=view&id=3113&Itemid=448)> [consulta: 20/07/2010]
- URRUTIA, Alonso y MARTÍNEZ, Fabiola (2009) Cuesta el voto en México 18 veces más que el promedio en AL, dicen expertos [en línea]. En: La Jornada (19/06/2009). México D.F. (México): DEMOS, Desarrollo de Medios, S.A. de C.V. <<http://www.jornada.unam.mx/2009/06/19/index.php?section=politica&article=014n1pol>> [consulta: 19/06/2009]
- VILLALOBOS RAMÍREZ, Marcela (2009) Desechan voto electrónico [en línea] En: Diario Extra (10/12/2009). San José (Costa Rica): Sociedad Periodística Extra Limitada <<http://www.dia-rioextra.com/2009/diciembre/10/nacionales14.php>> [consulta: 28/05/2008]
- WVSC (2009) The Netherlands return to paper ballots and red pencils. [en línea]. 11/10/2009. Netherlands: WVSC, Wij Vertrouwen Stem Computersniet <<http://wijvertrouwenstemcomputersniet.nl/English>> [consulta: 12/10/2009]