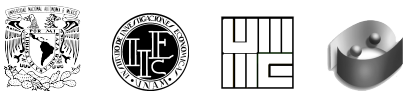
Construcción Colaborativa del Conocimiento

El presente trabajo forma parte del libro que recoge los trabajos del Seminario Construcción Colaborativa del Conocimiento (ISBN: 978-607-02-2373-0), coordinado por Gunnar Wolf y Alejandro Miranda.
Puede encontrar el libro completo para su descarga, así como los demás capítulos de forma individual, en
http://seminario.edusol.info/seco3



Apéndice C

Voto electrónico: ¿quién tiene realmente la decisión?

Gunnar Wolf[*]

Los promotores de las diferentes vertientes del conocimiento libre son los primeros en recalcar los tremendos fallos –de concepción y de puesta en práctica– que convierten en una causa perdida a las estaciones computarizadas de emisión y contabilización de votos (Heinz, 2006). Ninguna de las numerosas soluciones ofrecidas a la fecha han salido airosas ante el escrutinio (incluso casual) de expertos en seguridad (Felten, 2008a), incluso a veces con resultados verdaderamente nefastos (Balzarotti *et al.*, 2008a; 2008b). Generalmente grupos de activistas independientes dirigen los escrutinios buscando señalar las deficiencias del proceso, con la muy

[*]La postura que ante las votaciones electrónicas han tomado diversos grupos relacionados con la creación y escrutinio de software y de procesos sociales ilustra muy bien varios de los puntos delineados en otros capítulos de la presente obra.

El presente texto originalmente formaba parte del capítulo ??, "Software libre y construcción democrática de la sociedad", e ilustra una de las maneras en que las comunidades de creación de conocimiento (tanto de seguridad en cómputo como de software libre) han abordado un punto de gran importancia para la vida en sociedades democráticas actuales, insertándose en el entorno político imperante.

Hemos decidido, tanto por la extensión como por la relación de este tema con varios otros de los presentados en esta obra, hacer del presente apartado un apéndice independiente.

notable excepción del ejemplo del Tribunal Superior Electoral de Brasil, mismo que abordaremos más adelante.

Obviamente, estos resultados no agradan a las compañías que intentan vender máquinas supuestamente seguras, diseñadas *ex profeso* para el conteo de votos. Incluso se han dado a conocer amenazas contra equipos de investigadores (Felten, 2008b) que llevan a cabo esos análisis. La demanda es que en asuntos tan sensibles, relevantes y tan frágiles como la vida de una sociedad democrática, es sencillamente imposible asegurar los elementos básicos de confiabilidad y auditabilidad.

Cabe aclarar que la argumentación en este tema no pone en duda los *fundamentos matemáticos* de diversos sistemas aplicables a una votación electrónica, como las garantías descritas por Ruiz Duarte (2010), sino su *implementación.* La duda se mantiene, como veremos más adelante, aun suponiendo que el código está 100% disponible para su escrutinio. Lo que es más, algunos de los mecanismos descritos por Ruiz Duarte pueden utilizarse en contra del sistema democrático.[1]

Diversos argumentos se esgrimen a favor del voto electrónico, pero pueden resumirse en tres:

DISMINUCIÓN DE COSTOS. Un adecuado proceso democrático es caro. Se requiere imprimir la papelería electoral con mecanismos suficientes que aseguren su unicidad; proveerse mecanismos para garantizar que sólo los electores autorizados emitan su voto y ofrecer garantías de no manipulación para todos los componentes involucrados en el proceso. La automatización

[1] Tomo como ejemplo la prueba de la emisión de un voto basada en cero conocimiento: si bien el esquema sugerido permitiría a cada votante verificar 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 demostrar por quién voté, sin duda habrá quien me exija que le demuestre que voté en el sentido "correcto".

del proceso ayudaría a que estos candados tuvieran un menor costo.

Agilidad en la obtención de resultados. Nada genera mayor falta de confianza y suspicacia en los procesos que una demora en la publicación de los resultados. Se ha argumentado que, por medio del voto electrónico, los resultados pueden anunciarse 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 a la compra de conciencias, la extorsión o directamente a la violencia física); en un proceso controlado por computadoras, estos factores deberían perder peso.

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

C.1 Disminución de costos

La sociedad acostumbra a lidiar con los bemoles del voto *tradicional*, que utiliza al papel como su medio primario. El costo de éste constituye una crítica muy común a estos procesos, especialmente en los países con democracias no consolidadas y que, por tanto, requieren de mucho mayor inversión, tanto en la vigilancia como en la promoción de la participación de las elecciones. Podemos tomar como un caso extremo a México, el sistema electoral más caro de América Latina (Urrutia y Martínez, 2009; Ojeda Lajud, Rueda y Chávez, 2010): cada sufragio emitido en las elecciones federales intermedias de 2009 y en las estatales de 2010 costó más de 17 dólares, aunque hay estimaciones que refieren hasta 50 dólares, tomando en cuenta *gastos ocultos*.

Como mencionamos, sin duda podrían presentarse importantes ahorros en la generación, el manejo y la custodia del material electoral. Sin embargo, tras el estudio realizado por Feldman, Halderman y Felten (2007) a las estaciones de votación Diebold AccuVote-TS –las más difundidas en Estados Unidos y que captan votos de hasta uno de cada 10 electores de dicho país–, queda demostrado que enfrentadas a un atacante con conocimiento técnico especializado, estas máquinas presentan un nivel de confiabilidad verdaderamente bajo, y permiten –con un tiempo mínimo de acceso– la reprogramación de 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 no son privativas a los equipos Diebold. En el sitio web que publica su artículo, junto con un video de *10 minutos* demostrativo de su ataque, hay una lista de preguntas frecuentes:

> *¿Por qué estudiaron estas máquinas Diebold? ¿Por qué no otras tecnologías para votos?*
> Porque son las que conseguimos. Si hubiésemos tenido acceso a otro tipo de máquinas, tal vez las hubiéramos estudiado.
> *¿Son otras máquinas más seguras que las que estudiaron?*
> No lo sabemos. Esperamos que sí 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 las máquinas de voto electrónico.

Inclusive si el costo de adquisición o desarrollo de las urnas electrónicas fuera cero (que no lo es), si las urnas fueran suficientemente portátiles como para que su transporte a las mesas de elección no requiriera de logística especializada (que no lo son), y si fueran tan confiables como para no requerir personal especializa-

do que les diera soporte técnico en caso de fallo (que, nuevamente, no lo son), ante la evidencia de que su comportamiento puede modificarse en tan sólo 10 minutos, y sumados a este ejemplo muchos de los expuestos más adelante, concluimos que las urnas no pueden mantenerse sin custodia *ni por 10 minutos*. Una vez que un atacante logra la más trivial modificación en la operación de la urna, es prácticamente imposible detectar el alcance de su manipulación y revertirla a un estado confiable. En cambio, la papelería electoral sólo requiere vigilancia desde el momento en que se imprime hasta que la elección se declara válida y se ordena su destrucción. Un proceso de unas pocas semanas.

En caso de un proceso electoral controvertido, como el de 2006 en México, la situación resulta aún más complicada. Para asegurar una auditoría plena a una elección, es necesario conservar todo el material en un estado inalterado. Ante la obviedad de que es imposible auditar el estado interno de una computadora, se requeriría que las urnas permanecieran sin utilizarse hasta el cierre de la última apelación. A cuatro años del proceso de 2006, la papelería electoral sigue en custodia dado que existen aún soliictudes insatisfechas de información (Rubio, 2010). Si se hubiera recurrido a las urnas electrónicas, éstas no podrían haberse aprovechado para ninguna elección subsecuente, lo que significa que tendría que haberse adquirido o alquilado una segunda infraestructura completa o renunciar a la posibilidad de averiguar la verdad.

Para el planteamiento anterior partimos de un costo de adquisición cero. La adopción de un sistema electrónico de votación resulta más costosa que una votación tradicional: el Tribunal Supremo de Elecciones (TSE) de Costa Rica anunció que no implementará urnas electrónicas por su elevado costo (Villalobos Ramírez, 2009), y 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.*

Llegamos 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 prorratear el costo a lo largo de varias elecciones, pero el equipo debe sujetarse a una estricta vigilancia continua, incluso cuando no se utilice, recibir mantenimiento y abastecerse con una cantidad no despreciable de insumos, para asegurar un rastro impreso verificado. Además, en caso de un desperfecto, todas las casillas deben tener un plan de respaldo; casi indefectiblemente, esto significaría contar con papelería tradicional para enfrentar desde un desperfecto del equipo hasta un sabotaje, por ejemplo, en el suministro eléctrico. Por tanto, el supuesto ahorro puede volverse en contra nuestra y convertirse en un gasto mayor que el de las votaciones tradicionales.

C.2 Agilidad en la obtención de resultados

La velocidad del acceso a la información es una de las principales obsesiones de la sociedad actual. Los medios electrónicos de comunicación y el uso de internet nos han acostumbrado a disponer de información tan pronto como ocurren los hechos.

Los sistemas electorales en general estipulan que no deben darse a conocer resultados parciales antes de que haya cerrado la última de las urnas, para no manipular los resultados de una elección en proceso; ya que el conocimiento público de la tendencia influiría en los resultados de muchas maneras indeseables. Sin embargo, luego del cierre de la última urna, en la mayoría de las democracias modernas es necesario esperar un par de horas a que las autoridades electorales recopilen la información generada por decenas de miles de casillas y den a conocer el resultado.

Hay una gran presión por parte de los ciudadanos, y muy en especial de los medios, para que las autoridades electorales publiquen

los resultados *de inmediato*. Además del apetito por la información expedita, esto se fundamentó en ejemplos de ocultamientos de información que podían ocurrir conforme los números comenzaban a fluir, como el que reveló Manuel Bartlett Díaz, 20 años después de las muy cuestionadas elecciones presidenciales de 1988, en que fuera secretario de Gobernación y presidente de la Comisión Federal Electoral (Becerril, 2008), acerca de que Miguel de la Madrid tomó la decisión de no dar a conocer datos preliminares dado que: "si se oficializaba en ese momento –con datos parciales– que Cárdenas Solórzano iba ganando, al final nadie aceptaría un resultado distinto".

En la experiencia mexicana, la situación ha cambiado radicalmente en comparación con la imperante hace tan sólo dos decenios, como claro resultado de las frecuentes acusaciones de fraude electoral que el 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*, por lo general, 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 que nos presente tantos riesgos como una urna electrónica para ganar como tope esas dos horas sencillamente no tiene sentido. Además, el tiempo invertido por los funcionarios electorales en el conteo de votos emitidos en cada casilla es sólo una fracción del tiempo dedicado a las tareas de verificación y protocolización requeridos antes de declarar concluida una elección. A ello se suma que –por consideraciones de seguridad–[2] las estaciones de voto no están diseñadas para contar con conectividad a red (y que ni los países más industrializados disponen de una

[2]Si nos preocupa 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.

cobertura de internet de 100% en su territorio). Por tanto, debe haber forzosamente un paso manual de comunicación de resultados al centro de control de la autoridad electoral, así que 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 conservar todos los atributos positivos del sistema tradicional.

C.3 CONFIABILIDAD DE LOS ACTORES

Algunos promotores del voto electrónico mencionan que con el voto tradicional en papel siempre hubo fraudes de diversas naturalezas (por ejemplo, robo de paquetes electorales, urnas con más papeletas que electores, papeletas premarcadas, voto en cadena, votos repetidos con documentos falsos y de personas fallecidas); que todos estos fraudes –y seguramente muchos más– siempre han existido, y que cambiar a una modalidad electrónica no agrava los riesgos. Sin embargo, más que reducir las posibilidades de los agentes fraudulentos, de migrar a un sistema de voto electrónico aumentaríamos la profundidad a la que podrían llegar y, sobre todo, imposibilitaríamos cualquier acción de auditoría o rendición de cuentas. Sí, requiere mayor sofisticación por parte del atacante que

un fraude electoral tradicional, pero le da posibilidad de incidir de forma mucho más decisiva.

La votación electrónica tiene muchas modalidades y 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 se basen en software libre para su funcionamiento. Citando a Heinz (2006), sencillamente no recomiendan su uso:

> El mecanismo de auditar completamente el funcionamiento de las urnas es impracticable. Ésta es una tarea que sólo podría ser ejecutada por una élite 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. Ésta es una característica esencial y no debemos renunciar a ella.

Uno de los argumentos más interesantes que ilustran por qué las urnas electrónicas carecen inherentemente de confiabilidad es el que –sin aplicarlo en este ramo específico– presenta Ken Thompson (1984), en su discurso para recibir el Premio Turing de la ACM.[3] Thompson hace una sencilla demostración de por qué un sistema que llega al *usuario final* es prácticamente imposible de auditar por

[3] Premio al que comúnmente se hace referencia como el Nobel del Cómputo.

un programa, ni siquiera teniendo el código fuente del compilador; 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 los ya conocidos. Traduciendo las conclusiones de Thompson:

> La moraleja es obvia. No puedes confiar en el código que 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 de 2009 por la Corte Suprema de Alemania [Das Bundesverfassungsgericht, 2009].

> 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 (Heinz, 2009).

Cabe aquí referir al último punto mencionado al inicio de este apéndice: *Un rastro impreso verificado por cada votante*. La única garantía para un votante de que su voto se registre correctamente es que el sistema genere una *boleta impresa y de carácter irrevocable*, que cada votante pueda verificar al instante y se convierta en

el documento probatorio de la elección.[4] No hay manera de que el estado interno de una computadora sea confiable, y mucho menos cuando hablamos del proceso más importante y sensible de la vida política de un país.

El punto de la confiabilidad es el que con más fervor aún se debate. El caso brasileño resulta muy esperanzador: a diferencia de la mayoría de los gobiernos de países supuestamente desarrollados, en Brasil la tecnología para el voto electrónico se basa por completo en tecnología de diseño local, con software libre. En noviembre de 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 (Tribunal Superior Eleitoral, Brasil, 2009). Dentro de los términos estipulados, sólo un participante, Sergio Freitas da Silva, logró su propósito, al buscar que fuera una prueba de concepto (Busaniche, 2009); no consiguió vulnerar los resultados del sistema, pero –mediante un monitoreo de las radiaciones electromagnéticas y un equipo casero de bajo costo– averiguó por quién emitía su voto cada uno de los electores, con lo que rompió el principio de secreto electoral; un atacante determinado podría utilizar equipo mucho más sofisticado para intervenir las votaciones a mucha mayor distancia.

Y si bien una evaluación al sistema brasileño resulta mucho mejor que los aplicados en Europa y Estados Unidos, no debemos tomar la ausencia de evidencia por evidencia de ausencia: el hecho de que ninguno de los atacantes pudiera demostrar una vulnerabilidad en el periodo estipulado (o que habiéndolo logrado, no quiso publicarla por el precio ofrecido, reservándola para algún momento más lucrativo), no asegura la ausencia de fallas no descubiertas, o peor aún, la presencia de puertas traseras intencionales.

[4] 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 en el corte, para garantizar el anonimato del elector.

C.4 Votos blancos y nulos: expresión legítima del ciudadano

No podemos dejar de llamar la atención que muchas de las implementaciones llevan en la práctica a limitar la capacidad de expresión del sentido del voto del ciudadano. A lo largo de la historia, y en diversos países, agrupaciones políticas o grupos de ciudadanos espontáneos han convocado –dependiendo del código electoral en cuestión– al voto en blanco o a la anulación del voto como expresión del descontento ante las opciones presentadas o como una expresión de desconfianza ante toda la clase política.

Ejemplos de esa convocatoria podemos verlos en México (Meyer, 2009), donde en las elecciones legislativas de 2009 la cantidad de votos nulos alcanzó niveles superiores a 5% en el ámbito nacional (equiparable a una quinta fuerza política) y en algunas entidades superó 10% (El Economista, 2009); en las elecciones legislativas al Parlamento Vasco alcanzó 8.84% tras la ilegalización de la izquierda *abertzale* (La Vanguardia, 2009); en Perú, la localidad de Santiago de Pupuja presentó 61% de votos nulos (frente a 8% del candidato con más votos) (Huahuacondori, 2010).

El ejemplo más relevante viene de Argentina a mediados de siglo xx, durante el largo periodo de golpes militares y censura. Ante la prohibición de toda actividad política a Juan Domingo Perón, sus partidarios llamaron al voto en blanco. En las elecciones constituyentes de 1957 hubo cerca de 24% de votos en blanco (Melon Pirro, 2006). En las elecciones presidenciales de 1963 se repitió el escenario de censura, y los votos en blanco alcanzaron el segundo lugar con 19% frente a 25% de Arturo Illia (Guerrero, 2003), aunque varios actores de la época sostienen que incluso estas cifras están maquilladas.

Si bien es común escuchar críticas a los impulsores del voto en blanco en el sentido de que no aporta nada o que no influye en la distribución del botín electoral, es derecho de todos los ciudadanos

manifestar de esta manera su descontento. En el sistema electoral como el peruano, una alta proporción de votos nulos llevan a la anulación de la votación. En el sistema argentino, se diferencian *votos nulos* de *votos blancos*: los votos nulos, mal realizados, intencionalmente o no, no forman parte de los porcentajes electorales; y los votos blancos, explícitamente y sin espacio a ambigüedad para indicar la no preferencia por ninguno de los candidatos, es reportado dentro de los porcentajes resultantes de la elección. En el sistema mexicano, no se diferencia entre votos nulos y en blanco, lo cual reduce el efecto que éste puede tener. España tiene un sistema similar al mexicano, lo cual motivó la creación de la agrupación Ciudadanos en Blanco,[5] que se presenta a elecciones con el compromiso de dejar vacíos los escaños parlamentarios que obtengan, y reclamar que el voto en blanco sea (explícitamente) computable.

Independientemente de su validez y efecto legal, los votos blanco y nulo son una herramienta de expresión del individuo, y un atributo electoral que debe ser conservado. En las jurisdicciones donde el sistema electoral toma en cuenta los votos en blanco, una urna electrónica incluiría esta opción. Sin embargo, donde la ley asume que un voto nulo es un voto mal emitido, las autoridades a favor de la instalación de urnas electrónicas argumentan que éstas imposibilitan emitir votos erróneos. Esto limita la posibilidad del individuo de mostrar su descontento ante las opciones formales.

C.5 Experiencias internacionales

Por último, presentamos un listado de experiencias en diversos países, que ilustran en forma breve el tipo de problemas a que puede llevarnos el voto electrónico. Queda claro que no es una lista comprehensiva, sólo indicativa. Para una descripción mucho más exhaustiva, sugiero consultar UMIC, Agência para a Sociedade do Conhecimento (2009).

[5] http://ciudadanosenblanco.com

- 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 dichas urnas se habían enviado no era el mismo que el que se había sometido para certificación.

- La elección municipal de 2005 en Montreal, Canadá, se realizó mediante urnas electrónicas, con resultados desastrosos: alrededor de 45 000 votos fueron contabilizados dos veces (Geist, 2006). La autoridad electoral analizó las elecciones, y publicó un amplio reporte (Directeur général des élections du Québec, 2006) sobre las causas y cursos de acción a seguir, entre ellos: la necesidad de tener acceso completo al código fuente, la aplicación de pruebas de funcionalidad, un plan de contingencia en caso de problemas, y la puesta en marcha 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 de la manera en que fueron manejadas, no ofrecen suficiente garantía de transparencia y seguridad para asegurar la integridad del voto".

- Ed Felten ha escrito en repetidas ocasiones respecto a lo inadecuado de diversas urnas electrónicas. Uno de los primeros ejemplos que destacó (Felten, 2006), fue la pobre seguridad física en dichos equipos; las urnas pueden ser abiertas por una llave genérica de cajones de oficina y minibares de hotel.

- En Argentina, en 2007, se ensayó el voto electrónico en la localidad de Las Grutas, provincia de Río Negro. Hubo gran cantidad de discrepancias entre los padrones electoral y di-

gital, con lo que muchos votantes no pudieron expresar su voluntad. Mientras en las mesas tradicionales se registró 70% de votación, en las mesas con urna electrónica sólo se llegó a 40%; además, 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 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 exhibe también el ejemplo de una estación de votación para las elecciones *primarias* en Nueva Jersey, 2008 (Felten, 2008a), en que se puede ver un error *aritmético* al calcular la suma de votos. Siendo la función más básica de toda computadora la aritmética básica, no hay explicación posible a cómo puede una simple suma generar un resultado erróneo.

- Las elecciones presidenciales de Estados Unidos, en noviembre de 2008, si bien no experimentaron los graves problemas de legitimidad que sufrieron en 2000 y 2004, sí mostraron irregularidades en varios estados. El diario *Anchorage Daily News*, en Alaska, reseña (Gordon, 2008): 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 presentaron boletas erróneas. Por otro lado, en Michigan, el día anterior a la elección se descubrieron desperfectos en varias urnas electrónicas, por lo cual se realizó una votación tradicional, pero sin papelería electoral adecuada que ofreciera las garantías requeridas.

- Las elecciones primarias del Partido Laborista en Israel, 2008, tuvieron que posponerse una vez iniciadas debido a problemas de usabilidad en las urnas; 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 e 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 operar con 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, que aconsejó en 2008 revertir la recomendación que llevó a la realizar el voto electrónico, y rechazó la propuesta de desarrollar una nueva generación de urnas electrónicas que paliara el problema (WijVertrouwenStemComputersniet.nl, 2009; Election Process Advisory Commission, 2007). Hoy en día, los procesos electorales holandeses son nuevamente en papel, con conteo manual.

- Todo aparato electrónico emite radiación electromagnética en función de sus procesos internos, mismos que pueden ser olfateados por equipos ubicados hasta a decenas de metros. Un ejemplo de esto, es el resultado de la convocatoria del Tribunal Superior Electoral de Brasil (2009): un participante, con equipo completamente casero, logró averiguar el sentido de cada uno de los votos sin acceso a las urnas electrónicas (Busaniche, 2009; Felitti, 2009).

- En la India, casi la totalidad de la población vota en urnas exclusivamente electrónicas, desarrolladas en los últimos dos decenios por el gobierno nacional, la EVM. 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 de 2010, un grupo liderado por Alex Halderman, Hari Prasad y Rop Gonggrijp consiguió una EVM y publicó dos ataques que pueden efectuarse 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.

Casos hay muchos más. También se tienen importantes casos de éxito. Por volumen poblacional, cabe destacar al total de la población de India y Brasil, y cerca de la cuarta parte de la población de Estados Unidos; a pesar de los problemas antes ilustrados, el mero volumen de votaciones efectuadas mediante urnas electrónicas indica que se puede hacer un despliegue masivo. Sin embargo, lo fundamental de los casos anteriores no es el efecto que hayan tenido o detectado a tiempo; lo principal es que nos hacen patentes los problemas de confiabilidad, no sólo en los supuestos fundamentos de funcionamiento, sino en la naturaleza humana. Incluso para tareas aparentemente tan simples como la de sumar votos, no hemos podido –y muy probablemente nunca podamos– producir un proceso tan confiable y auditable como la revisión humana de papeletas físicas.

Acerca del autor

Gunnar Wolf — México

Ingeniero en software de formación autodidacta; entusiasta, usuario y desarrollador de software libre desde 1997, especializado en la administración de redes y en el desarrollo de sistemas Web.

Ha fomentado la cohesión y profesionalización de las comunidades locales de software libre. Es fundador del Congreso Nacional de Software Libre, y entre 2002 y 2004 se desempeñó como coordinador general del mismo. Además, desde 2003 colabora activamente como desarrollador del proyecto Debian. Es fundador del Encuentro en Línea de Educación, Cultura y Software Libres, mismo que coordinó entre 2005 y 2010.

Desde 2005 trabaja como académico del Instituto de Investigaciones Económicas de la unam.

Bibliografía

Balzarotti, Davide *et al.* (jul. de 2008a), «Are Your Votes Really Counted? Testing the Security of Real-world Electronic Voting Systems», *International Symposium on Software Testing and Analysis*, Seattle, WA, http://www.cs.ucsb.edu/~seclab/projects/voting/issta08_voting.pdf; p. 1.

Balzarotti, Davide *et al.* (2008b), *Evaluating the Security of Electronic Voting Systems*, http://www.cs.ucsb.edu/~seclab/projects/voting/index.html; p. 1.

Becerril, Andrea (jul. de 2008), «De la Madrid me ordenó no informar que Cárdenas iba ganando, asegura Bartlett», *La Jornada*, http://www.jornada.unam.mx/2008/07/03/index.php?section=politica&article=013n1pol; p. 7.

Busaniche, Beatriz (2007), «Recurso de amparo contra el voto electrónico en Río Negro», http://www.vialibre.org.ar/2007/12/07/recurdo-de-amparo-contra-el-voto-electronico-en-rio-negro/ (visitado 28-05-2010); p. 15.

— (2009), «Un investigador logra violar el secreto del voto en las urnas brasileñas», *Voto electrónico* 2009/12/29, http://www.vialibre.org.ar/2009/12/02/un-investigador-logra-violar-el-secreto-del-voto-en-las-urnas-brasilenas/; pp. 11, 16.

— (mayo de 2010), «Partidos políticos impugnan el uso de voto electrónico en Salta», 2010-05-28, http://www.vialibre.org.ar/2010/05/28/partidos-politicos-impugnan-el-uso-de-voto-electronico-en-salta/; p. 15.

Das Bundesverfassungsgericht (2009), «Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.», http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html; p. 10.

Directeur général des élections du Québec (oct. de 2006), *Rapport d'évaluation des nouveaux mécanismes de votation*, Directeur général des élections du Québec, http://defids.qc.ca/english/news-detail.php?id=2624; p. 14.

El Economista (jul. de 2009), «Voto nulo "quinta fuerza electoral" en México», *El Economista*, http://eleconomista.com.mx/politica/2009/07/06/voto-nulo-quinta-fuerza-electoral-mexico (visitado 08-12-2010); p. 12.

Election Process Advisory Commission (sep. de 2007), *Voting with confidence*, The Hague: Ministry of the Interior y Kingdom Relations, pág. 74, http://wijvertrouwenstemcomputersniet.nl/images/0/0c/Votingwithconfidence.pdf; p. 16.

Feldman, Ariel J., J. Alex Halderman y Ed Felten (ago. de 2007), «Security Analysis of the Diebold AccuVote-TS Voting Machine», *2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, USENIX USENIX, http://itpolicy.princeton.edu/voting/; p. 4.

Felitti, Guilherme (nov. de 2009), «Perito quebra sigilo e descobre voto de eleitores em urna eletrônica do Brasil», *IDG Now!* 2010-05-28, http://idgnow.uol.com.br/seguranca/2009/11/20/perito-quebra-sigilo-eleitoral-e-descobre-voto-de-eleitores-na-urna-eletronica/; p. 16.

Felten, Ed (sep. de 2006), «"Hotel Minibar" Keys Open Diebold Voting Machines», http://freedom-to-tinker.com/blog/felten/hotel-minibar-keys-open-diebold-voting-machines; p. 14.

— (2008a), «Evidence of New Jersey Election Discrepancies», http://freedom-to-tinker.com/blog/felten/evidence-new-jersey-election-discrepancies; pp. 1, 15.

— (2008b), «Interesting Email from Sequoia», http://freedom-to-tinker.com/blog/felten/interesting-email-sequoia; p. 2.

Geist, Michael (oct. de 2006), «Time To Cast A Vote Against E-Voting», *Toronto Star*, http://www.michaelgeist.ca/content/view/1491/159/; p. 14.

Gordon, Greg (nov. de 2008), «Glitches hamper voting in five states», *Anchorage Daily News*, http://www.adn.com/2008/11/04/578431/glitches-hamper-voting-in-five.html; p. 15.

Guerrero, Osvaldo Álvarez (oct. de 2003), *Arturo Umberto Illia: Cuadragésimo aniversario de su asunción a la Presidencia de la Nación*, http://ricardobalbin.tripod.com/illia40.htm (visitado 08-12-2010); p. 12.

Heinz, Federico (2006), «¿El voto electrónico mejora la democracia?», http://www.vialibre.org.ar/2006/10/07/el-voto-electrnico-mejora-la-democracia/; pp. 1, 8-9.

— (mar. de 2009), «Alemania: urnas electrónicas anticonstitucionales», 2009/03/06, http://www.vialibre.org.ar/2009/03/06/alemania-urnas-electronicas-anticonstitucionales/; p. 10.

Huahuacondori, José (nov. de 2010), «Ganó voto nulo y no hay alcalde en Santiago de Pupuja», *Los Andes*, http://www.losandes.com.pe/Politica/20101113/43280.html (visitado 08-12-2010); p. 12.

Khoury, Jack, Roni Singer-Heruti y Ofri Ilani (dic. de 2008), «Labor sets primary for tomorrow after computer failure», *Haaretz*, http://www.haaretz.com/print-edition/news/labor-sets-primary-for-tomorrow-after-computer-failure-1.258707; p. 16.

La Vanguardia (mar. de 2009), «El voto nulo, que pidió la izquierda abertzale, superó los 100.000 sufragios», *La Vanguardia*, http://www.lavanguardia.es/politica/noticias/20090302/53650819652/e

l-voto-nulo-que-pidio-la-izquierda-abertzale-supero-los-100.000-sufragios.html (visitado 08-12-2010); p. 12.

Lucas, Greg (mayo de 2004), «State bans electronic balloting in 4 counties», *San Francisco Chronicle* A1, http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/05/01/MNG036EAF91.DTL; p. 14.

Melon Pirro, Julio César (jun. de 2006), «Los números del 'Recuento'. El primer test electoral del peronismo en la proscripción», *historiapolitica.com*, http://historiapolitica.com/datos/biblioteca/Melon1.pdf (visitado 08-12-2010); p. 12.

Meyer, Lorenzo (jun. de 2009), «El voto sin partido o cómo usar la crisis», *Reforma*, http://www.lorenzomeyer.org/Agenda-ciudadana/11junio2009.pdf (visitado 08-12-2010); p. 12.

Ojeda Lajud, Olga, Rivelino Rueda y Víctor Chávez (mayo de 2010), «El voto mexicano cuesta 18 dólares; es el más caro de América Latina», *El Financiero*, http://impreso.elfinanciero.com.mx/pages/NotaPrint.aspx?IdNota=320373; p. 3.

Rubio, Francisco (nov. de 2010), «Trasladan papelería de elecciones de 2006», http://www.noticiasmvs.com/Trasladan-papeleria-de-elecciones-de-2006.html (visitado 08-12-2010); p. 5.

Ruiz Duarte, Eduardo (feb. de 2010), «Álgebra de votaciones para procesos electorales», 2010-05-28, http://b3ck.blogspot.com/2010/02/algebra-de-votaciones-para-procesos.html; p. 2.

Salinas, Yamil (jul. de 2008), «Experiencia fallida de voto electrónico en Argentina», 2010-05-28, http://www.yamilsalinas.net/2008/07/22/experiencia-fallida-de-voto-electronico-en-argentina/; p. 15.

Thompson, Ken (ago. de 1984), «Reflections on trusting trust», *Communications of the ACM* 27.8, págs. 761-763, 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; p. 9.

Tribunal Superior Eleitoral, Brasil (2009), «Teste de segurança do sistema eletrônico de votação», 2009/12/29, http://www.tse.gov.br/internet/eleicoes/teste_seguranca.htm; pp. 11, 16.

UMIC - Agência para a Sociedade do Conhecimento (abr. de 2009), *Electronic Voting Experiments in Political Elections around the World*, UMIC - Agência para a Sociedade do Conhecimento; Ministério da ciéncia, tecnologia e ensino superior, http://www.english.umic.pt/index.php?option=com_content&task=view&id=3113&Itemid=448; p. 13.

Urrutia, Alonso y Fabiola Martínez (jun. de 2009), «Cuesta el voto en México 18 veces más que el promedio en AL, dicen expertos», *La Jornada*, http://www.jornada.unam.mx/2009/06/19/index.php?section=politica&article=014n1pol; p. 3.

Villalobos Ramírez, Marcela (dic. de 2009), «Desechan voto electrónico», *Diario Extra*, http://www.diarioextra.com/2009/diciembre/10/nacionales14.php; p. 5.

WijVertrouwenStemComputersniet.nl (2009), «The Netherlands return to paper ballots and red pencils», http://wijvertrouwenstemcomputersniet.nl/English; p. 16.