III CONGRESO ARGENTINO DE DERECHO ELECTORAL

OBJECIONES A LOS SISTEMAS DE VOTO ELECTRÓNICO

Enrique A. Chaparro

TEMA B) REGULACIÓN ELECTORAL Y MECANISMOS ELECTRÓNICOS DE VOTACIÓN. CUESTIONES CONSTITUCIONALES, REGLAMENTARIAS, CONTRACTUALES, ADMINISTRATIVAS Y JURISDICCIONALES.

SUBTEMA: OBJECIONES A LA ADOPCIÓN DE SISTEMAS DE VOTO ELECTRÓNICO.

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

– Kofi Annan

OBJECIONES A LOS SISTEMAS DE VOTO ELECTRÓNICO

Enrique A. Chaparro*

RESUMEN

Este documento explora las objeciones a los sistemas de voto electrónico; se analiza someramente el estado de la cuestión sobre el voto automatizado a nivel global, los factores de adopción y rechazo de estos sistemas, y los problemas planteados por la colisión entre las características opacas del voto electrónico y derechos ciudadanos fundamentales. Se ha sostenido que el voto electrónico reúne algunas ventajas en términos de velocidad y precisión de conteo, facilidad de emisión, prevención de fraude y disminución de costos, pero estas ventajas son cuando menos discutibles a la luz de la evidencia, y no compensan los invonvenientes que presenta en términos de confianza de los electores en el sistema electoral, usabilidad, seguridad de la información y protección del secreto. Por otra parte, la mediación informática, que solo puede ser comprendida por un número limitado de ciudadanos, deteriora la calidad democrática. Se concluye que no hay razones válidas para su adopción.

PRELIMINAR: DEFINICIONES

Adoptamos en este trabajo la definición de "voto electrónico" de (Alvarez y Hall 2010, 9–10): la acción del votante que convierte su selección en en una cadena de señales electrónicas define la condición de voto electrónico.[1] Esta, por lo demás, es consistente con la opinión generalizada tanto jurídica como técnica.[2] Los sistemas denominados comercialmente "boleta única electrónica", como los usados en las elecciones locales de 2015 en la Ciudad de Buenos Aires y en la provincia de Salta, pertenecen pues a esta clasificación: es un sistema de registro electrónico, puesto que las opciones escogidas por el votante se registran directamente en una memoria electrónica incluida en la BUE, e incluye un comprobante impreso verificable por el elector. Para el caso, carece de significación que el registro electrónico se realice en un dispositivo distinto de la misma especie para cada voto, o que se acumule en una única unidad de memoria incorporada al dispositivo en el cual se lleva a cabo la

* Fundación Vía Libre. Contacto: <*echaparro@vialibre.org.ar*>.

1 "En nuestra definición, un dispositivo de voto electrónico es aquel en que el votante ingresa sus preferencias electrónicamente – sea moviendo algunas palancas mecánicas que registran el voto en el dispositivo (...) digitando selecciones en un sistema de votación con pantalla táctil, o usando cualquier otro método de ingreso para indicar un voto en un dispositivo de voto electrónico. Cuando usa tecnologías de voto electrónico, el votante interactúa con un sistema informático que traduce lo que aquel ingresa en una corriente electrónica de información que luego es de algún modo registrada y preservada para su posterior tabulación. Puede que la máquina de voto electrónico simplemente registre lo que el votante ingresó en algún tipo de dispositivo o dispositivos de almacenamiento (incluyendo medios removibles y no removibles); o que traduzca lo que el votante ingresó a una papeleta que es impresa para que el votante la verifique y la deposite en una urna; o que almacene electrónicamente lo que el votante ingresa y suministre una papeleta impresa que el votante puede verificar. En tanto las preferencias del votante estén siendo registradas por él en alguna corriente inicial de información electrónica, consideraremos a esto voto electrónico."

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

emisión del voto, puesto que la lógica implícita es la misma. Tampoco hace diferencia que el proceso de totalización se lleve a cabo con cierto diferimiento o en simultaneidad con la emisión del voto, porque en ambos casos la operación involucrada implica leer del dispositivo de memoria (distribuido en dispositivos individuales en el caso de la BUE o sistemas similares, o consolidado en otros sistemas) mediante un programa y acumular los resultados parciales hasta obtener el escrutinio provisorio.

Los procesos automatizados a través del voto electrónico son entonces el de *emisión*, el de *registro* y el de *conteo* (o escrutinio primario). Definiremos como emisión al proceso por el cual el elector expresa su voluntad; registro, a aquel por el cual la voluntad expresada por el elector es fijada en un medio permanente y, al mismo tiempo, se torna imposible correlacionar la identidad del votante con su voto; y conteo al proceso por el cual se contabilizan los votos emitidos, asignándolos a las diversas candidaturas o propuestas. El objetivo, entonces, de un sistema electoral es que los votos sean emitidos como expresión fiel de la voluntad del votante (*cast as intended*), registrados tal como fueran emitidos (*recorded as cast*) y contados como fueran registrados (*tallied as recorded*). Como mecanismo adicional contra la coerción, algunos sistemas electorales establecen salvaguardas complementarias; las más usuales son que no se emita recibo que permita identificar qué votó el elector, y que el resultado no pueda ser conocido antes de un momento prefijado y posterior a la finalización del período establecido para que los electores puedan emitir sus votos.

I – EL VOTO ELECTRÓNICO

El acto de votar para elegir representantes o establecer opinión es central a las formas democráticas de gobierno. Toda soberanía emana del pueblo, como bien señala nuestra Constitución Nacional, y es mediante ese acto fundamental que los representes del pueblo, y por extensión todo el sistema de gobierno, obtienen su legitimidad. En las palabras de Thomas Paine (1795), un protagonista destacado de las dos grandes revoluciones del siglo XVIII que darán forma a los modernos estados democráticos, "el derecho al voto es el derecho primario con el cual se protegen todos lo demás". El eco de las palabras de Paine resuena en Alberdi (1920): el voto es "la primera y la más fundamental de las libertades". La Argentina tuvo un largo y complejo tránsito hacia el voto libre, universal, igual y secreto, y prueba de ello es que la legislación electoral nacional, basada en la ley 8871 por la que el nombre de Roque Sáenz Peña ha pasado a la historia, es extraordinariamente puntillosa, hasta en los detalles aparentemente menos relevantes, respecto de los procedimientos de garantía del sufragio.

En esencia, la cadena de legitimidad se construye a partir de la confianza del elector[3] en que su intención de voto va a ser computada fielmente. Es importante notar que nos referimos a la intención y no a la expresión de esa intención, el documento de cualquier tipo que la refleja; la diferencia radica en que es un requisito fundamental del sistema electoral garantizar el reflejo fidedigno de la intención en el vehículo que la documenta.[4] Los sistemas manuales de emisión y conteo primario que se utilizan en la mayoría de los países del mundo, bajo la forma de boleta única

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

4 Un claro ejemplo de esta diferencia son las ya famosas elecciones presidenciales estadounidenses del 9 de noviembre de 2000 en el condado de Palm Beach, Florida. Una boleta con diseño confuso (para el caso, del sistema Votomatic de tarjetas perforadas) llevó a que un número importante de votantes (se estima que unos 2800) que pretendían votar por el candidato demócrata Gore lo hicieran por el reformista Buchanan. George W. Bush ganó la elección en ese estado, y por consiguiente todos los votos del colegio electoral correspondiente que lo convirtieron en presidente de los EE. UU. por una diferencia de 537 sufragios.

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

La informatización del sufragio

La introducción de tecnologías informatizadas en el proceso de emisión del voto y en el conteo provisorio que sigue inmediatamente al comicio, sin embargo, trae consigo interrogantes nuevos sobre la preservación de las garantías. Es habitual que la tecnología se mueva más rápidamente que el sistema legal; no obstante ello, la evolución tecnológica debe ser siempre procurada como un medio para mejorar la vida humana y no como un fin en si misma. En este sentido, todo desarrollo tecnológico, y en particular cuando directa o indirectamente afecta principios fundamentales, debe ser cuidadosamente revisado centrando la atención en determinar su contribución hacia una sociedad mejor (Mitrou et al., 2002). Como bien señala Pellegrini (2014), "el buen desarrollo del proceso electoral se acredita por medio de cadenas de confianza, que se rompen con la introducción de dispositivos opacos, concebidos y aplicados por terceros". La certeza sobre la intención del votante se vuelve más difusa por la existencia de un mecanismo de expresión controlado por un programa informático que el votante desconoce (y es a veces desconocido también para las autoridades electorales), y que es imposible analizar sin un conjunto de conocimientos altamente especializados. Las tareas de control de las personas encargadas de verificar pasos esenciales del proceso electoral quedan reducidas a la mera visualización, o a actuar como dispositivos periféricos de alimentación de datos a un sistema informático que en esencia se desconoce; sostiene la Organización para la Seguridad y la Cooperación en Europa (2008, 2) que "suceden eventos electrónicos que no están sujetos al examen ordinario por el ojo desnudo del observador (...) (a)demás, el voto electrónico consiste en componentes tecnológicos que no son fácil ni rápidamente entendibles para el observador promedio".

A pesar de estas limitaciones problemáticas, que ponen en cuestión algunos de los atributos fundamentales del voto, a finales del siglo pasado y comienzos del actual hubo una marcada propensión a considerar las percibidas ventajas de los sistemas de voto electrónico que llevó a muchos gobiernos a experimentarlo y ponerlo en práctica. Los Estados Unidos fueron un país pionero en la implantación de sistemas de voto electrónico en los últimos dos decenios del siglo pasado, principalmente debido a tres razones: las particularidades de su sistema electoral, que hacen muy complicada la cuenta manual, el desarrollo de su industria informática y una prolongada tradición en el uso de dispositivos primero mecánicos y luego electromecánicos que se remonta a finales del siglo XIX.[6] El primer sistema de voto electrónico con selección por pantalla fue patentado en 1974 (McKay et al. 1974).En Europa, la adopción temprana tuvo lugar en los Países Bajos y

5 La primera legislación electoral del mundo que preveía voto secreto con cédulas de papel en que aparecían los nombres de todos los candidatos fue sancionada en Tasmania el 4 de febrero de 1856. Al poco tiempo siguieron Australia del Sur (12 de febrero) y Victoria (13 de marzo). La primera elección con el nuevo método se llevó a cabo en el este último territorio el 27 de agosto del mismo año. Cfr. (Newman 2003).

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

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

Mientras tanto, países que lo habían adoptado o realizado pruebas piloto fueron abandonándolo: los Países Bajos, donde la cantidad de votantes que utilizaban voto electrónico era superior al 90 %, retornaron al voto en papel con cuenta manual en 2008, después de que se detectase fraude en las elecciones comunales de una pequeña localidad, la asociación civil *Wij vertrouwen stemcomputers niet* demostrase graves fallas de seguridad en el sistema empleado (Gonggrijp y Hengeveld 2007) y el tribunal superior de Amsterdam anulara en octubre de 2007 la certificación de las máquinas Nedap; el tribunal constitucional federal alemán declaró la inconstitucionalidad del sistema de voto electrónico usado en ese país en 2009;[8] el tribunal constitucional de Austria, donde se había llevado a cabo una elección experimental pero vinculante para la Federación de Estudiantes la declaró nula y fijó normas muy estrictas para futuros intentos;[9] en enero de 2010 el Ministerio de Justicia de Finlandia comunicó que el gobierno de ese país desistía de sus proyectos luego de que el Supremo Tribunal Administrativo (*Korkein hallinto-oikeus*)[10] declarara nulas y ordenara rehacer por medios convencionales las elecciones en que se había experimentado en tres municipalidades en 2008;[11] y la corte constitucional de Bulgaria declaró inconstitucionales ciertas provisiones del código electoral que autorizaban el uso del voto electrónico.

En Francia el uso de *machines à voter* fue autorizado por la ley 69-419 del 10 de mayo de 1969 modificatoria del Código Electoral. Las máquinas electromecánicas nunca se extendieron demasiado, y pronto cayeron en desuso, pero en 2002 una nueva ola de modernización llevó a instalar en forma experimental sistemas de voto electrónico en tres comunas, incrementándose progresivamente el número hasta 2007. La instalación de sistemas de voto electrónico se encuentra en moratoria de facto, porque desde finales de 2007 el ministerio del Interior no ha dado nuevas autorizaciones a las comunas para incorporar este tipo de equipamiento, el uso ha disminuido desde su máximo de 82 comunas y 1,5 millones de electores en 2007 (5 % del padrón electoral nacional) a 64 comunas y 1 millón de electores en 2012, y se han presentado varios proyectos de ley para su erradicación definitiva.[12,13] Irlanda planeó introducir un sistema de voto electrónico para las elecciones de 2004 para lo que adquirió equipamiento entre 2002 y 2003, pero nunca llegó a

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

8 Por su interés para este ensayo, el fallo del tribunal constitucional alemán se comenta más adelante. Un relato de antecedentes y comentario de esta sentencia y la del Constitucional austríaco que se comenta a continuación, puede hallarse en Fernández Riveira (2013).

9 Verfassungsgerichthof. 2011. V 85-96-11/15. Sentencia del 13 de diciembre de 2011.

10 Korkein hallinto-oikeus. 2009. KHO:2009.39. Sentencia del 9 de abril de 2009.

11 Oeikusministerio. 2010. *Sähköisen äänestyksen kehittämistä ei jatketa nykyiseltä pohjalta.* Comunicado de prensa, enero 14.

12 Por ejemplo, proyectos de ley del senador Philippe Kaltenbach, registrado en el Senado el 22 de julio 2014, 763 (2014-2015) , y del diputado François Rochebloine, registrado en la Asamblea Nacional el 21 de enero 2015, 2510 (14^{éme}) .

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

efectivizarlo por resistencia de los electores e importantes sectores académicos, abandonando el proyecto en 2009 y finalmente destruyendo las máquinas en 2012;[14] en Lituania las intenciones de la autoridad electoral para introducir voto electrónico han sido sistemáticamente rechazadas por el parlamento; Noruega realizó un estudio de factibilidad en 2006, una prueba piloto en 10 municipalidades en 2010 y otra en 2013, para finalmente anunciar oficialmente el abandono de todas las pruebas en junio de 2014; el Reino Unido realizó varios pilotos entre 2000 y 2007, pero tomando en cuenta los resultados negativos en otros países y las críticas de la Comisión Electoral no se han hecho nuevos intentos desde entonces;[15] en noviembre de 2011 el gobierno de Kazajstán decidió abandonar el sistema Sailau que había iniciado en 2004, en razón de que la preferencia de los votantes por el papel, la desconfianza de los partidos y el costo;[16] y en Paraguay, que venía adoptando gradualmente el sistema brasileño desde 2001 y que para 2006 había alcanzado prácticamente la cobertura completa del padrón electoral, el Tribunal Superior de Justicia Electoral dispuso el retorno al voto manual en papel en las elecciones generales de 2008.[17]

Factores de adopción de los sistemas de voto electrónico

Sencillez del conteo. Los sistemas de voto electrónico se han introducido para hacer más simple la cuenta de votos y el cómputo de los resultados. Esta consideración es importante, pero solo se aplica a un número pequeño de elecciones complejas, basadas en preferencias (como el voto alternativo o el voto único transferible), o las que implican un gran número de categorías y cuestiones sometidas a referéndum,[18] y en ellas la cuenta manual puede requerir mucho tiempo y estar sujeta a error. No es el caso general de las elecciones en la Argentina, donde aún en el caso extremo de que coincidieran elecciones nacionales, provinciales y municipales la convocatoria involucra a lo sumo ocho categorías, y no existen casos de voto preferencial o condicional.

Facilidad de emisión. La confusión puede efectivamente el ejercicio del derecho al voto, especialmente cuando se trata de los electores más vulnerables (personas de edad, iletradas o con discapacidades). Las elecciones parlamentarias de Afganistán de 2005 tuvieron un cinco por ciento de votos nulos, una proporción inusualmente alta en la práctica internacional y que puede atribuirse tanto al confuso sistema afgano cuanto a los altos niveles de analfabetismo (Reynolds 2006).[19] Las tecnologías de registro electrónico prometen reducir estos niveles haciendo imposibles los votos nulos y difíciles los votos en blanco no intencionales. El Caltech/MIT Voting Technology Project ha argumentado que el empleo de tecnología puede reducir los votos "perdidos" en una variedad de formas, y la capacidad de generar interfaces más adecuadas puede potencialmente resolver problemas para personas con discapacidades o hablantes de lenguas minoritarias.

14 El sistema electoral irlandés es extraordinariamente complejo, con voto único transferible para la elección de los miembros del Dáil Éireann y segunda vuelta instantánea para la elección de presidente, por lo que en principio la automatización resultaba una alternativa de interés. Para detalles del proceso de adopción y abandono del voto electrónico, véase McDermott (2010).

15 Para una recopilación de la situación en Europa en general a mediados de 2014, véase Stein y Wenda (2014).

16 Una descripción del sistema Sailau y la historia de su implementación se encuentra en Jones, (2010).

17 Tribunal Superior de Justicia Electoral. 2008. *Resolución tsje Nº 12/2008 "Por la que se dispone la utilización de Boletines de Voto en las Elecciones Generales del 20 de abril próximo"*, febrero 4. Es interesante destacar que esas elecciones generales marcaron la única ocasión en que los partidos de oposición lograron imponerse sobre la oficialista Acción Nacional Republicana (Partido Colorado).

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

19 Reynolds, Andrew. 2006. "The Curious Case of Afghanistan." *Journal of Democracy* **17** (2): 113-4.

Sin embargo, al minimizar la posibilidad de algunos errores los sistemas de voto electrónico pueden incrementar la de otros. Es posible que los votantes no familiarizados con las computadoras no emitan ya votos nulos, pero puede emitir votos que no reflejen adecuadamente sus preferencias; es posible también que la asistencia a los votantes iletrados o con discapacidades resulte confusa, errónea, insuficiente o inhabilitante, o que la interfaz genere nuevos problemas para personas con discapacidades que en un sistema manual podían emitir su voto sin inconvenientes.[20] La presunción de mayor usabilidad[21] no ha sido probada rigurosamente para la mayoría de los sistemas. Ni las autoridades electorales de la India ni las de Brasil, los países de uso más extenso del voto electrónico, han publicado estudios científicamente válidos de la interacción de los votantes con su tecnología, y es significativo notar aquí que los niveles de voto nulo en Brasil desde la generalización del sistema de voto electrónico son inusualmente altos; en las últimas elecciones generales, fueron 6,68 millones en la primera vuelta y 5,22 millones en la segunda (respectivamente, 5,8 y 4,63 por ciento de los votos emitidos).[22] Sin estudios serios, es difícil establecer tanto la utilidad del voto electrónico cuanto la correcta aproximación a la educación de los votantes. Recientemente, Zucco y Nicolau (2015) han publicado un estudio extensivo sobre el impacto del voto electrónico en Brasil que muestra la sustitución de viejos errores por nuevos.

Por otra parte, numerosos estudios de usabilidad proporcionan evidencia concluyente de nuevos problemas (Norden et al. 2006; Michel et al. 2007; Conrad et al. 2009), entre ellos cómo la voluntad del votante puede ser influenciada por la interfaz en que realiza la selección (Fairweather y Rogerson 2005; Card y Moretti 2007; Katz et al. 2011; Greene, Byrne, y Goggin 2013) y otros factores de entorno (Acemyan y Koopman 2015), y cómo determinadas formas de presentación afectan negativamente a los votantes de capacidades más limitadas (Selker et al. 2005; Selker 2007) y aún a aquellos sin aparentes limitaciones (Edelstein y Edelstein 2008), más aún cuando incrementos en la seguridad van en detrimento inevitable de la usabilidad (Belton et al. 2015) abd. La importancia de las pruebas de usabilidad de los sistemas es crucial (Herrnson et al. 2006), y en general se ha observado que, como en los casos testigo en la Argentina, no se realizan.

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

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

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

22 Fuente: TRIBUNAL SUPERIOR ELEITORAL. 2014. *Estatísticas eletorais – Estatísticas de resultados – Comparecimento e votação*. Disponible en línea en <http://www.tse.jus.br/eleicoes/ estatisticas/ estatisticas-eleitorais-2014-resultado>

considerablemente – basta un solo programador malintencionado para introducir código que afecte la veracidad del resultado de una elección. Como señala Mercuri (2002), "mientras que tecnologías previas requerían que el fraude electoral se perpetrase en un lugar de votación o en una máquina a la vez, la proliferación de sistemas de voto electrónico similarmente programados invita a oportunidades de manipulación a gran escala". El aumento de eficiencia de los ataques permite además la aparición de formas más sutiles de alterar resultados selectivamente, por ejemplo las que señalan Di Franco et al. (2004a, 2004b). La generación de registros impresos comprobables visualmente por el elector no es eficaz para contrarrestar este riesgo, por razones que discutimos más abajo.

Reducción de costos. Con frecuencia se aduce que el voto electrónico reduce cosos de administración electoral. Este argumento suena creíble por cuanto estamos acostumbrados a que el empleo de tecnologías de información aumenta la eficiencia de los procesos a los que se aplica y por lo tanto reduce costos en las actividades gubernamentales o del sector privado. Pero usualmente estas estimaciones se hacen en función de proyecciones de mediano y largo plazo, y no hay ningún estudio longitudinal que las confirme. En el caso del sistema adoptado para la ciudad de Buenos Aires, se ha aducido que se generará una significativa economía relacionada con el costo de impresión y distribución de boletas partidarias, pero cabe notar que esta reducción es consecuencia de la implantación del sistema de boleta única y no de la automatización. Existen pocos estudios comparativos rigurosos entre los costos por voto emitido de boleta única en papel y su equivalente electrónico; no obstante, en Bélgica los costos en la región valona se estiman respectivamente en €0,10 y €1,37 (*La Libre* 2015), mientras que la información oficial de costo por voto para el sistema Smartmatic, similar al empleado en Venezuela y en las localidades cordobesas de La Falda y Marcos Juárez en 2015, es de €4,4412 (Chambre des représentants 2015, 25). Existen en cambio datos sobre el costo por elector de diversos sistemas electorales; reduciéndolos a una divisa común y actualizándolos, hallamos que para algunas democracias estables los valores son: Australia US$ 4,97 (Gray 2005), España US$ 5,14, solo la gestión electoral sin incluir el registro de electores (López Pintor 2005b), Suecia US$ 7,60 (Gratschew 2005). Comparativamente, hemos estimado el costo para la primera vuelta de las elecciones locales de 2015 del sistema escogido para la Ciudad de Buenos Aires en 80,36 pesos por voto emitido, lo que a la fecha de ajuste de la orden de pago respectiva equivalía a US$ 9,05, solo para las etapas de emisión y escrutinio y sin contemplar otros costos logísticos, como las compensaciones a las autoridades de mesa y a los delegados de la autoridad electoral.[23]

Status. Un factor de adopción pocas veces considerado en la literatura es el del "prestigio tecnológico", una confusión de métodos y fines que supone que el uso de medios tecnológicos avanzados obra mágicamente para modernizar una democracia, o implica una aseveración sobre la modernidad de un gobierno o una autoridad electoral más que la solución a una necesidad específica. Como dice López Pintor (2005a, 44), el voto electrónico "se ha convertido en un símbolo de *status* para muchos países y organizaciones". En la cadena de decisión y sustento del voto electrónico, que Staszewski (2014) denomina "obstinación tecnocrática", Gauld y Goldfinch (2006) "fatuidad tecnológica" y Enguehard (2010) "quimera tecnológica", puede ocurrir un fenómeno de introducción de error sistemático conocido como sesgo cognitivo, por la sobreapreciación de la tecnología, que han investigado Moynihan y Lavertu (2012): la fe en la tecnología puede enceguecer a los funcionarios públicos respecto de las cualidades negativas de las innovaciones, llevándolos a preferir una tecnología novedosa y compleja que puede ser inferior a una solución más antigua, más

23 Nuestro cálculo se basa en el precio pactado ajustado por resolución 218/MJYSGC/15 (Boletín Oficial de la Ciudad de Buenos Aires 4614: 40, 10 de abril 2015), el número estimado de votantes proyectado a partir del número en las primarias abiertas y con la tasa de incremento de las elecciones nacionales de 2013 en el distrito, y la cotización del dólar estadounidense para la fecha de publicación de la resolución referida.

barata o más simple. Si la fe en la tecnología es un sesgo extendido y consistente entre los funcionarios públicos, será apropiado alentar una visión más pragmática, o aún pesimista, como contrapeso. Como mínimo, los decisores políticos generalmente proclives hacia la tecnología deberían intentar tomar esto explícitamente en cuenta cuando deciden respecto de la adopción de tecnología.

Riesgos de la adopción

La discusión precedente ha dejado en claro que muchas de las reivindicaciones sobre las ventajas de los sistemas de voto electrónico carecen de fundamento. Contra estas relativas ventajas, deben señalarse cuatro desventajas de mayor porte: en primer lugar, el daño a la confiabilidad y a la credibilidad del proceso electoral; en segundo, la transferencia del proceso del ámbito público al privado; en tercero, las cuestiones clave de seguridad de estos sistemas de información, y finalmente los obstáculos en los procesos de implantación y despliegue.

Daños a la credibilidad. Todo programa informático puede tener errores no intencionales no detectados ("bugs"). Todo programa informático puede ser cambiado en forma maliciosa en una forma indetectable a posteriori. Estas afirmaciones son verdaderas para cualquier software. Adicionalmente, toda computadora de propósitos generales (como las que normalmente constituyen la base de los sistemas de voto electrónico con pantalla táctil) es suceptible de explotación maliciosa (Bratus et al. 2011), y la verificación del software en tiempo de ejecución es un problema de tal complejidad que su implementación resulta prohibitiva. Hay medidas que pueden reducir las vulnerabilidades de un sistema de voto electrónico, incluyendo la seguridad informática, la seguridad física, las pruebas y los análisis de los sistemas y el código,[24] y buenos procedimientos electorales; pero ninguno de estos pasos, y ninguna combinación de ellos, puede cambiar la irreductible vulnerabilidad de los sistemas informáticos. Un texto ya clásico de Ken Thompson (1984) alerta sobre la cuestión.[25] Por ejemplo, es posible que las características de las máquinas usadas en la India hagan improbable que puedan ser reprogramadas por una persona con acceso limitado y casual a ellas (como un votante), pero son vulnerables ante quienes tengan menos restricciones de acceso, como los representantes de la autoridad electoral (Wolchok et al. 2010).

Esta vulnerabilidad implica que los resultados de una elección pueden ser manipulados, y también crea el peligro de que resultados legítimos de una elección no sean aceptados, porque es imposible refutar de manera concluyente las acusaciones de manipulación. En 2004, Venezuela tuvo un referéndum por la destitución presidencial. El entonces presidente Hugo Chávez se impuso cómodamente, con un 58 % de los votos, y los observadores internacionales en general acordaron en que no se había observado fraude. Pero, considerando que el 90 % de los votos habían sido emitidos a través de un nuevo sistema de voto electrónico, la oposición no estaba convencida, y con buenas razones: los observadores no pudieron certificar la confiabilidad de los sistemas de voto electrónico. El sistema venezolano emite un comprobante impreso verificable por el elector, pero la falta de procedimientos rigurosos de verificación y recuento hizo que la oposición no aceptara la veracidad de las verificaciones *ad hoc* llevadas a cabo después de la elección, e investigaciones estadísticas posteriores realizadas por académicos de Harvard y el MIT confirmaron la falta de confiabilidad del proceso (Hausmann y Rigobon 2004); en general, los estudios indican que no puede descartarse en el caso la posibilidad de fraude (Martín 2011; Pericchi y Torres 2011).

Lo que se alegue sobre los resultados electorales basados en sistemas de voto electrónico puede

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

25 Aunque es posible evitar el dilema de confianza última que plantea Thompson, los mecanismos para hacerlo revisten una complejidad excepcional y requieren ser aplicados tanto en los procesos de compilación, como plantea Wheeler (Wheeler 2009), cuanto utilizando hardware especializado y procedimien tos detallados para garantizar el *bootstrapping* de software "correcto" (Gratzer y Naccache 2006; 2007).

corroer rápidamente la confianza en las elecciones, pues aquellos no pueden ser adecuadamente probados ni refutados. Una encuesta de *The New York Times* y CBS mostraba en 2006 que el 64 % de los votantes demócratas y el 40 % de los definidos independientes creía que en las elecciones presidenciales de 2004 en el estado se había cometido fraude.[26]

Se ha postulado que algunos de los problemas del voto electrónico pueden ser salvados empleando comprobantes verificables por el votante vvpat o ,[27] pues estos permitirían al votante confirmar sus preferencias en un medio permanente y recontable. Para ser efectivos, deberían cumplir con un conjunto de criterios: no comprometer el secreto del voto; ser legibles; estar insertos en un procedimiento que aliente a los votantes a confirmar su contenido; y ser parte de un proceso que prevea la realización de recuentos manuales extensivos sobre muestras al azar estadísticamente correctas después del escrutinio provisorio. Sin embargo, la utilidad de los comprobantes impresos como elemento de confirmación de la voluntad del elector es cuando menos discutible, puede ayudar a convalidar resultados fraudulentos, y los impresos traen sus propios problemas, incluyendo la adición de más elementos propensos a fallar y la falsa sensación de certeza que pueden crear si no es establecen procedimientos claros sobre cómo emplear los comprobantes para determinar o verificar el resultado de la elección. Es significativo que la Dra. Rebecca Mercuri, quien desarrolló originalmente la idea, sostenga: "desde 2003, debido a los problemas irresolubles de implementación y despliegue de [estos] sistemas [...] y las dificultades expermientadas en usar los comprobantes para los recuento, he recomendado (y sigo recomendnado) contra la adquisición de estos dispositivos. Los votos deben ser preparados en papel (no en computadoras) y contados del papel (preferentemente por humanos)" (Mercuri 2007).

La confianza de los votantes en el proceso electoral es fundamental en las democracias, porque las elecciones establecen un vínculo entre los ciudadanos y sus servidores públicos elegidos. Si los electores tienen dudas acerca de lo fidedigno del escrutinio, sentirán que los resultados no reflejan la voluntad expresada por la mayoría; esta duda socava el aspecto más fundamental de las democracias modernas: la elección de los representantes del pueblo soberano (Atkeson y Saunders 2007; Alvarez et al. 2008). La legitimidad de los individuos elegidos, y la de los cuerpos colegiados, se debilitan cuando surgen estos cuestionamientos; esto puede llevar a minar las fortalezas del proceso democrático y de las instituciones. La mayoría de las democracias modernas han tenido épocas de cuestionamiento del proceso electoral (Lehoucq 2002). En democracias consolidadas, puede suceder que sin pérdida de confianza en las elecciones la haya respecto de la tecnología usada. Loeber (2011) ha investigado estas dos variables en las elecciones parlamentarias neerlandesas de 2006 y 2010, continuando un trabajo iniciado en 2008, y halló que aunque la confianza de los votantes en las elecciones no había experimentado variación significativa, la confianza en la aplicación de sistemas sistemas informatizados había disminuido significativamente.

Es inevitable coincidir con McGaley y Gibson (2003): "aparte del obvio requerimiento de que los votos sean computados correctamente, es vital que los votos se vean como computados correctamente. Un sistema de votación es solamente tan bueno como el público cree que lo sea".

Enajenación del proceso electoral. El proceso convencional no solo es bien entendido y fácilmente verificable por electores y autoridades electorales; además, todos sus pasos están bajo control de autoridades electorales permanentes o *ad hoc* y observación de fiscales partidarios y observadores. Pero cuando se implementan sistemas informatizados, al menos una parte significativa de los pasos pasa a ser mediada por un procedimiento automático cuyo funcionamiento se desconoce y que, por lo tanto, no puede ser controlado, y se introducen nuevos

26 CBS News / New York Times Poll: Campaign 2006 Ohio, 17 de octubre 2006. Pregunta 66, página 26. En 2004 George W. Bush ganó el estado de Ohio por un pequeño margen, y con ello su reelección como presidente.

27 La idea fue desarrollada por Mercuri (2002) y aparece abundantemente en la literatura; (Dill et al. 2003; Blanc 2007; Bishop y Wagner 2007).

actores en el proceso con roles generalmente poco definidos – o directamente indefinidos – en la normativa que adquieren un protagonismo central: los técnicos. La concurrencia de estos termina resultando indispensable para la ejecución de determinados pasos esenciales, especialmente cuando se presentan inconvenientes durante el desarrollo de las operaciones electorales. Las elecciones de 2015 en la provincia de Salta proporcionan un ejemplo de estas circunstancias: informes de observadores destacan el rol virtualmente autónomo de los técnicos de la empresa contratista (la misma de la ciudad de Buenos Aires) en el desarrollo de operaciones críticas sin adecuada supervisión.[28] Esta transferencia introduce un factor adicional de riesgo respecto de la transparencia de la elección.

Si bien los gobiernos, especialmente a partir de las décadas de 1980 y 1990, han tendido a confiar al sector privado la ejecución bajo contrato de algunas actividades relacionadas con las tecnologías de información,[29] los procesos electorales son especiales por su significación y sus consecuencias, y no pueden ser completamente tercerizados a proveedores del sector privado (Xenakis y Macintosh 2005). Como señala Lehoucq (2002), los estados latinoamericanos realizaron una gran contribución a la democracia constitucional con el surgimiento de autoridades electorales independientes de los poderes ejecutivo y legislativo, que incrementaron la confianza pública en las elecciones. Pero si estas entidades de control independientes pierden la capacidad efectiva de supervisar todos los detalles del proceso electoral, su rol de garantes de la transparencia ya no podrá ser cumplido cabalmente. ¿Cómo se comportará un contratista privado a cargo de un aspecto crítico de una elección cuyo resultado afecta sus intereses? Aún si se comportara con absoluta neutralidad, ¿cómo podrían aventarse las sospechas si la opción favorecida por el contratista resulta ganadora? La desafortunada declaración de Walden O'Dell, entonces presidente de la empresa productora de sistemas de voto electrónico Diebold,[30] previa a las presidenciales estadounidenses de 2004, todavía arroja sombras sobre la transparencia de aquella elección. Las fallas, accidentales o intencionales, de un sistema de voto electrónico tienen profundas consecuencias para la confiabilidad del sistema electoral y la confianza pública en él (Moynihan 2004).

Oostven (2010) analiza la pérdida de control público sobre el sistema electoral en el caso de los Países Bajos, y sus hallazgos son aleccionadores . La autora halla que después de dos décadas de uso de sistemas de voto electrónico, la autoridad electoral se encontraba limitada por tres falencias: la falta de capacidad técnica, la falta de apropiación del sistema, y la falta de control sobre el proceso electoral. Existe un serio riesgo de que ello suceda cuando la autoridad electoral carece de los recursos técnicos expertos que requiere un control efectivo de las elecciones.

Cabe señalar a manera de ejemplo que la adopción del sistema de voto electrónico de la ciudad de Buenos Aires en 2015 parece compartir una característica común con un número de iniciativas de informatización electoral tomadas en otros lugares: aparenta haber sido conducido por posibilidades tecnológicas y conveniencia burocrática, en lugar de por una determinación de utilidad social democráticamente debatida.[31] Cuando aquellos criterios prevalecen, como sucede en muchos casos de *outsoucing* de aspectos importantes de actividades del sector público, la eficiencia choca con la obligación de rendir cuentas y socava los valores democráticos (Verkuil 2007). Para acrecentar la transparencia de los procesos electorales hacia la ciudadanía, los partidos políticos y las propias autoridades electorales, es necesario que estas sean incorporen las capacidades técnicas

28 Véase, por ejemplo, el informe "Análisis y recomendaciones de la observación electoral Primarias Abiertas, Simultáneas y Obligatorias. Salta, 12 de abril de 2015 " preparado por la organización Poder Ciudadano.

29 No siempre de manera exitosa. En la Argentina se recuerdan los efectos negativos de estas operaciones de *outsourcing* en el Banco de la Nación (*vid.* Tribunal Oral en lo Criminal y Correccional Federal Nº 3, "Dadone, Aldo y otros s/defraudación contra la administración pública", causa 509/05) y en la administración impositiva.

30 En una carta a los recaudadores de fondos de campaña del Partido Republicano, O'Dell afirmaba estar "comprometido a ayudar a que Ohio diera sus votos electorales" a Bush (Carr Smyth 2003).

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

necesarias, mantengan el control, asuman plena responsabilidad y promuevan un rol activo de los ciudadanos en todos los procesos que llevan a la decisión sobre tecnologías electorales. La absoluta transparencia del sistema a utilizar es un indispensable primer paso.

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

Los análisis serios de seguridad requieren trabajo exhaustivo y especializado: el análisis del código fuente del software de las máquinas de voto electrónico Diebold AccuVote TS (Kohno et al. 2004) requirió de casi dos semanas a tiempo completo de cuatro notables expertos en seguridad informática. También es necesario notar que una inspección, por detallada que sea, no necesariamente encontrará todos los errores en un conjunto de programas, en algunos casos porque la técnica de ataque no es aún generalmente conocida (Checkoway et al. 2009). En el caso mencionado previamente, Rubin y sus colegas realizaron un análisis exhaustivo, aunque algo limitado en el tiempo de ejecución. Pero posteriormente, sobre la misma plataforma, fueron hallados reiteradamente nuevos errores o correcciones defectuosas que no eliminaban las vulnerabilidades previamente detectadas(Feldman et al. 2006; Calandrino et al. 2007; Gardner et al. 2009). Hasta sistemas con superficies de ataque menores, como los de lectura óptica de boletas marcadas manualmente por el elector, han mostrado vulnerabilidades graves (Hursti 2005).[32] Ocultar de la vista pública los detalles es una muy mala práctica en términos de seguridad de la información, porque retrasa el ciclo de reparación de defectos y disminuye la confianza en el sistema o la reduce a un acto de fe incompatible con la certeza racional. Desde hace tiempo la comunidad técnica adhiere al llamado "principio de Kerckhoffs":[33] la seguridad de un sistema no debe depender de que sus detalles permanezcan en secreto (Kerckhoffs 1883).

La problemática de seguridad de un sistema de voto electrónico debe ser vista desde la perspectiva general de la seguridad de la información, esto es, el cumplimiento de los atributos canónicos de confidencialidad, integridad y disponibilidad.[34] No obstante ello, la cuestión que trasciende los límites puramente tecnológicos: como señalan Oostveen y van den Besselaar (2004a; 2004b), "las complejas cuestiones técnicas relativas a la seguridad (...) deben ser respondidas antes de que los sistemas vayan a ser usados en elecciones gubernamentales de cualquier nivel", pero también deben tomarse en cuenta el entorno social y las consideraciones sociopolíticas, la percepción de la seguridad por parte del público, porque ya no existe una"fe ciega en la objetividad

32 En mayo de 2010, durante pruebas previas a las elecciones presidenciales en Filipinas, se detectó que 76.000 de las 82.000 lectoras ópticas dispuestas tenían placas de memoria defectuosas que daban como resultado asignación incorrecta de votos (cfr. RADIO FRANCE INTERNATIONALE 2010).

33 KERCKHOFFS, AUGUSTE. 1883. "La cryptographie militaire". *Journal des sciences militaires* IX (enero): 5-38 y (febrero): 161-91.

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

científica y los 'expertos'".

Es necesario notar que desde el punto de vista de la seguridad informática, los sistemas de voto electrónico plantean problemas especiales, no solamente por las graves consecuencias institucionales de los resultados erróneos. En efecto, estos sistemas plantean la singular demanda de satisfacer simultáneamente tres condiciones que se contraponen: por un lado, que el elector pueda asegurarse de que su intención de voto ha sido correctamente computada; por otro, que no tenga forma de probar ante terceros cuál fue el contenido de su voto (porque ello da lugar a compra de votos o intimidación); y, finalmente, que se conserve perfecto anonimato para garantizar el secreto del sufragio (Anderson 2010, 759–63). La inexistencia hasta el presente de modelos formales de seguridad de sistemas de voto que cubran efectivamente el amplio espectro de modelos de amenazas (Weldemariam y Villafiorita 2012), ha llevado a plantear la noción de "sistemas independientes del software" (Rivest 2008): un sistema de voto es "independiente del software" si un cambio o error no detectados en el software no pueden causar un cambio o error no detectables en el resultado de la elección. De ello surge el marco teórico de "verificabilidad de extremo a extremo" (*end-to-end verifiability*) (Benaloh et al. 2015); pero si bien este marco es formalmente correcto, se ha probado que los sistemas que lo implementan tienen graves problemas de usabilidad que conducen a bajos porcentajes de éxito en la emisión y la verificación del voto (Acemyan et al. 2014; Moher et al. 2014).

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

Las cuestiones centrales de seguridad radican en la preservación de la integridad y el secreto del voto. Cuando se utilizan sistemas de registro directo electrónico sin ningún comprobante verificable por el elector, el logro de estas condiciones es imposible de demostrar. Para la primera cuestión, como señalábamos más arriba, se ha intentado generar un elemento que el elector pueda verificar por sí mismo. Sin embargo, la observación empírica y el resultado de pruebas controladas proporcionan amplia evidencia de que la mayoría de los electores generalmente no verifican los comprobantes impresos (ni siquiera cuando ese control es un paso indispensable para completar la transacción) y, cuando los controlan, de todos modos se deslizan altas tasas de error. Selker y Cohen (2005) introdujeron 108 diferencias entre la emisión y el registro en una elección simulada, para evaluar dos métodos diferentes de verificación. Con el método de comprobante impreso, los votantes reconocieron 3 errores, aunque no reportaron ninguno a la autoridad electoral; con el de comprobación por audio, reconocieron 25 y reportaron 13. En un experimento diferente, Everett (2007) halla que más del 60% de los votantes no detecta los errores introducidos (algunos de ellos muy burdos, como la supresión de una categoría completa). Campbell y Byrne (2009) repiten el experimento de Everett mejorando la capacitación de los votantes y la usabilidad de la interfaz de pantalla, pero aún así no logran mejorar los niveles de detección más allá del 50%. La baja detección de error se atribuye a la disonancia perceptiva entre la información presentada en pantalla respecto de la registrada en un medio impreso. El bajo nivel de reporte, inferior en todos los casos a lo detectado, corresponde a un fenómeno bien estudiado: la atribución de "credibilidad" a las computadoras (Muir y Moray 1996; Tseng y Fogg 1999); por lo tanto los errores no pueden ser sino del elector, que se siente avergonzado de reconocerlos. Pero, por otra parte, el texto legible no dice nada respecto de los datos almacenados en la memoria, que son los que se utilizarán para el conteo.

Y los comprobantes generados producen dificultades cuando debe realizarse un recuento manual, con tasas de error mucho mayores a las de las boletas completadas a mano por el votante (Goggin et al. 2008).

La preservación del secreto es un problema aún más serio. El uso de cualquier identificador único (como el número de serie de los dispositivos RFID del sistema usado en 2015 en Salta y la ciudad de Buenos Aires) deja abierta la posibilidad de asociarla con el votante individual. Un sistema conceptualmente similar a ese fue ensayado en Israel en 2009, y rápidamente descartado al determinarse que el secreto podía ser vulnerado fácilmente (Oren y Wool 2009).

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

Procedimientos. Aún si se lograran en el software de los sistemas de voto informatizado niveles de seguridad comparables con los de los mecanismos convencionales, el aseguramiento de todos los procesos involucrados en la elección es pieza clave de su fiabilidad. Uno de los problemas más difíciles de resolver es el de la complejidad de la cadena de suministro, porque una falla accidental o inducida en cualquiera de los pasos se propaga hasta el resultado final. Yee (2006) ha esquematizado la cadena de suministro de software, y aún sin considerar el hardware la complejidad es evidente. En general, hay una marcada insuficiencia en los procedimientos establecidos por la autoridad electoral que eleva los riesgos. Por ejemplo, no suelen establecerse correctamente mecanismos para asegurar efectivamente que la versión del software a ejecutar durante la elección se corresponde con una versión previamente verificada, un problema que por cierto presenta dificultades extremas. Tampoco suele haber mecanismos para asegurar que el hardware se corresponde exactamente con algún modelo de referencia exhaustivamente verificado, ni se prevén acciones de verificación independiente y control por oposición, y la logística de distribución suele ser débil y suceptible de ataques internos y externos.

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

III – ¿QUIÉN SUPERVISA LA ELECCIÓN?

La perspectiva tecnicista. Algunas lógicas de empleo del voto electrónico suponen como inevitable el desplazamiento de la capacidad de control sobre los procesos electorales. Así, la mediación informatizada de aspectos críticos de una elección no habría de verse de modo diferente al empleo de computadoras en otras actividades que también revisten importancia significativa para las personas (Barrat i Esteve 2009). En esta aproximación ingenieril (Shamos 2007), la cuestión no sería diferente de otras en que los usuarios carecen de información de detalle sobre el funcionamiento real del sistema, y no tienen sobre él capacidades de supervisión inmediata pero depositan confianza en procesos de control llevados a cabo por terceros; característicamente, se ha equiparado esta cuestión a los procesos informatizados bancarios.

En los sistemas bancarios (donde además aparece la analogía entre los dispositivos de emisión del voto y los cajeros automáticos), en los sistemas electorales, o en cualquier otro entorno informatizado, la auditoría previa y posterior constituirán, entonces, un factor decisivo para la fiabilidad. Pero este recurso queda fuera del alcance de los usuarios, que carecen de los saberes requeridos; y tampoco los necesitarían, pues su intervención es irrelevante en tanto su confianza no debería basarse en el conocimiento de los detalles técnicos sino en la convicción de que el conjunto de medidas procedimentales adoptadas incluye las salvaguardas necesarias. En este sentido, no

habría diferencia con otros productos industriales sometidos a procesos de certificación; aunque en la mayoría de los casos los resultados de estos procesos solo serán conocidos por la autoridad electoral y la empresa proveedora, lo que, como señalan los funcionarios responsables del condado de Alameda, California, "es la práctica habitual de negocios de la industria informática respecto de la preservación de la seguridad de los sistemas",[35]

Pero es fundamental señalar que las elecciones presentan notables diferencias con otras áreas de uso de la informática. Una de las diferencias centrales es expresada sintéticamente por Richard M. Stallman: "el software de las máquinas de votación es un caso especial porque el mayor peligro para la seguridad proviene de la gente que se supone sea responsable por ella" (citado en Anderson 2010, 707). La comparación con los sistemas bancarios es falaz (Loeber 2008): en primer lugar, en estos no hay necesidad de una obligación pública de rendir cuentas y basta con una auditoría independiente. En las elecciones, en cambio, cada votante debería ser capaz de verificar que el sistema funciona correctamente, porque si esto no fuera posible la confianza en las elecciones, y por ende la confianza en los representantes elegidos, declinaría. Por otra parte, en los sistemas de banca electrónica un banco puede permitirse cada tanto un problema menor en el sistema; los errores causados por estos problemas pueden ser enmendados sin mayores consecuencias, y con buena probabilidad serán detectados porque los titulares de cuentas pueden verificar sus extractos, y la mayoría lo hace. En las elecciones no hay posibilidad de enmienda, y cualquier error menor, aún si se lo detecta, puede tener un impacto significativo sobre la cuestión de quien ejercerá la representación popular por los próximos cuatro años. Una pequeña cantidad de estos errores y la confianza se disolverá en el aire, con consecuencias desastrosas.

La perspectiva de las garantías fundamentales. Hay, sin embargo, una significativa línea de pensamiento que advierte que las condiciones fundamentales del proceso electoral deben preservarse con independencia del empleo de recursos tecnológicos. En ese sentido, el Tribunal Constitucional Federal de Alemania (*BVerfG*) resolvió favorablemente en 2009 una impugnación sobre el uso de sistemas de voto electrónico,[36] declarando inconstitucional la Ordenanza Federal sobre Máquinas de Votación (*Bundeswahlgeräteverordnung*) de 3 de septiembre de 1975 en su versión modificada por la Ordenanza Modificatoria del 20 de abril de 1999 (*Verordnung zur Änderung der Bundeswahlgeräteverordnung und der Europawahlordnung*). El valor teórico de esta resolución se acrecienta si tenemos en cuenta las similitudes de marco constitucional. El fallo establece dos principios esenciales: las elecciones como acto público (principio de publicidad),[37] y el derecho del elector a comprender todos los pasos esenciales de la elección y el escrutinio sin conocimiento experto (principio de entendimiento).

Respecto del primer principio, el alto tribunal halla que

> "La publicidad de las elecciones es condición fundamental para la construcción de una voluntad política democrática. Asegura la regularidad y transparencia del proceso electoral y se configura, con ello, como

35 En "Respondents/defendants County of Alameda and Dave MacDonald's combined response to Plaintiff's second set of specially prepared interrogatories", *Americans for Safe Access v. County of Alameda*, Alameda Superior Court, 18 de enero 2007. Citado en Jones (2007) .

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

37 Siendo un acto fundacional de lo público, es inevitable que esto sea así. Si todos los actos de gobierno son públicos, con más razón son públicos los únicos actos de los que emana la legitimidad de ese gobierno. Esta característica ineludible de las elecciones no colisiona con el secreto del voto de cada elector, porque el secreto del sufragio individual no es un elemento constitutivo del derecho a votar, sino una garantía, ciertamente indispensable, de que la expresión de la ciudadanía no estará sujeta a ninguna forma de coerción. En el mismo sentido, § 128 del fallo comentado: "No hay 'conflicto de intereses' entre el principio de las elecciones secretas y el principio de carácter público". Se ha formulado abundante teoría política sobre los aspectos positivos del voto no secreto, desde Mill al presente (Mill 1861); véase por ejemplo Brennan y Pettit (1990).

> condición esencial para una confianza fundamentada de los ciudadanos en el correcto desarrollo de la elección." (§ 106)

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

Ahora bien, de ese carácter publico sigue necesariamente el segundo principio:[39]

> "En una república, las elecciones son cuestión de todo el pueblo y preocupación común de todos los ciudadanos. En consecuencia, el control del procedimiento electoral también debe ser cuestión y deber del ciudadano. Cada ciudadano ha de poder seguir y entender de forma fiable las etapas centrales de la elección sin conocimientos técnicos especiales" (§ 109) "El votante por sí mismo debe ser capaz de verificar –también sin un conocimiento informático detallado– si su voto es registrado fielmente como base para el conteo o, si los votos son inicialmente contados con ayuda tecnológica, cuando menos como base para un subsiguiente recuento. No es suficiente si debe confiar en la funcionalidad de un sistema sin posibilidad de inspección personal." (§ 119) "La naturaleza pública de las elecciones requiere, en el despliegue de máquinas de votar controladas por computadora, que los pasos esenciales del acto electoral y la certeza de los resultados puedan ser revisados confiablemente y sin conocimiento experto especial". (§ 146)

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

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

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

38 Artículo 38.1: "Los diputados del Bundestag alemán serán escogidos por sufragio universal, directo, libre, igual y secreto. Son los representantes del pueblo en su conjunto, no ligados a mandatos ni instrucciones y sujetos únicamente a su conciencia" . Artículo 20.2: "Todo poder del Estado emana del pueblo. Este poder es ejercido por el pueblo mediante elecciones y votaciones y por la intermediación de órganos especiales de los poderes legislativo, ejecutivo y judicial" .

39 Este principio también es recogido por el Tribunal Constitucional de Austria (Verfassungsgerichthof, 2011, cit.) y constituye uno de los dos elementos centrales del fallo.

123)

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

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

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

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

El tribunal constitucional alemán reafirma, profundiza y precisa un principio ya establecido en la Recomendación REC(2004)11 del Consejo de Europa (2005): la obligación de los estados de garantizar que los votantes "entienden el sistema de voto electrónico y tienen confianza en él" (anexo I, § 20) y la disponibilidad pública general de "información sobre el *funcionamiento* del sistema" (íd. §21, el destacado es nuestro). Si bien estos términos pueden tener interpretaciones diversas, el Memorándum Explicativo de la recomendación se encarga de precisarlos: "la plena comprensión del sistema de voto electrónico es la base" de la confianza (§ 55) y recuerda, como señalábamos más arriba, que "los métodos de votación tradicionales son simples y han sido bien probados y ensayados... (l)os votantes están familiarizados con los sistemas de sufragio que usan papeletas y urnas y entienden las reglas generales que gobiernan cómo deben votar y cómo su voto es recogido y contado sin alteraciones" (§ 56).

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

IV – A MODO DE CONCLUSIÓN

Este brevísimo recorrido plantea entonces tres niveles de objeción al voto electrónico. En primer lugar, el razonamiento del *Bundesverfassungsgericht* alemán, perfectamente aplicable en nuestro entorno consitucional: el imperativo de que el votante pueda asegurarse por sí mismo y sin necesidad de recurrir a ayuda experta que su voto expresa correctamente su voluntad, y que se registra y cuenta debidamente. Ahora bien, el correcto entendimiento de esta exigencia plantea un problema irresoluble en el actual estado de la ciencia informática. En segundo plano se hallan las objeciones técnicas en sí: no es posible construir un sistema seguro que proporcione esas garantías, y aún cuando fuera admisible un ligero menoscabo de ellas, el sistema resultante presentaría serios problemas de usabilidad. Finalmente, los procedimientos necesarios para asegurar un correcto

despliegue son extremadamente gravosos.

A las presuntas ventajas de mayor celeridad y exactitud en el conteo se oponen problemas de tal magnitud que hacen desaconsejable la implantación de cualquier sistema de voto electrónico. Si bien se reconocen problemas en el sistema electoral vigente, no existe razón para suponer que estos no puedan ser resueltos por medios más eficientes. Debería ser un llamado de atención que, 40 años después de los primeros ensayos , los sistemas de voto electrónico en el mundo no han ganado impulso sino que, por el contrario, muchas democracias desarrolladas han decidido no adoptarlo, y en algunos casos rechazarlo después de haberlo empleado de modo significativo.

BIBLIOGRAFÍA

Acemyan, Claudia Z., y Philip Koopman. 2015. "Does the Polling Station Environment Matter? The Relation Between Voting Machine Layouts Within Polling Stations And Anticipated System Usability". *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 59 (1): 1066–70.

Acemyan, Claudia Z., Philip Kortum, Michael D. Byrne, y Dan S. Wallach. 2014. "Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II". *The USENIX Journal of Election Technology and Systems* 2 (3): 26–56.

Alberdi, Juan Bautista. 1920. "De la libertad y el gobierno". En *Obras selectas*, 17:9. Buenos Aires: La Facultad.

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

Alvarez, R. Michael, Thad E. Hall, y Morgan H. Llewellyn. 2008. "Are Americans Confident Their Ballots Are Counted?" *The Journal of Politics* 70 (3): 754–66.

Anderson, Ross J. 2010. *Security Engineering*. 2ªed. New York: John Wiley & Sons. https://www.cl.cam.ac.uk/~rja14/book.html.

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

Atkeson, Lonna Rae, y Kyle L. Saunders. 2007. "The Effect of Election Administration on Voter Confidence: A Local Matter?" *PS: Political Science and Politics* 40 (4): 655–60.

Barrat i Esteve, Jordi. 2009. "Observación electoral y voto electrónico". *Revista catalana de dret públic* 39: 277–96.

Belton, M. Grant, Philip Kortum, y Claudia Z. Acemyan. 2015. "How Hard Can It Be to Place a Ballot Into a Ballot Box? Usability of Ballot Boxes in Tamper Resistant Voting Systems". *Journal of Usability Studies* 10 (4): 129–39.

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

Bishop, Matt, y David Wagner. 2007. "Risks of e-voting". *Communications of the ACM* 50 (11): 120.

Blanc, Jarrett. 2007. "Electronic voting". En *Challenging the Norms and Standards of Election Administration*, 11–19. Washington, DC: International Foundation for Electoral Systems (IFES).

Bratus, Sergey, Michael Locasto, Meredith L. Patterson, Len Sassaman, y Anna Shubina. 2011. "Exploit Programming: From Buffer Overflows to 'Weird Machines' and Theory of Computation". *;login:* 36 (6): 13–21.

Brennan, Geoffrey, y Philip Pettit. 1990. "Unveiling the Vote". *British Journal of Political Science* 20 (3): 311–33.

Calandrino, Joseph A., Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, y William P. Zeller. 2007. *Source code review of the Diebold voting system*. Sacramento: California Secretary of State.

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

Card, David, y Enrico Moretti. 2007. "Does Voting Technology Affect Election Outcomes? Touch-screen Voting and the 2004 Presidential Election". *The Review of Economics and Statistics* 89 (4): 660–73.

Carr Smyth, Julie. 2003. "Voting Machine Controversy". *The Plain Dealer*, agosto 28.

Chambre des représentants de Belgique. 2015. "Compte Rendu Intégral - Commission de l'Interieur, des Affaires générales et de la Fonction publique". CRIV 54 COM 252. Bruselas: Chambre des répresentants de Belgique.

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

http://www.vialibre.org.ar/wp-content/uploads/2015/06/VE.CdBuenosAires.Parte1_.pdf.
Checkoway, Stephen, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, y Hovav Shacham. 2009. "Can DREs provide long-lasting security? The case of return-oriented programming and the AVC Advantage". En *Proceedings of EVT 2009*. Montreal: USENIX Association.
Conrad, Frederick G., Benjamin B. Bederson, Brian Lewis, Emilia Peytcheva, Michael W. Traugott, Michael J. Hanmer, Paul S. Herrnson, y Richard G. Niemi. 2009. "Electronic Voting Eliminates Hanging Chads but Introduces New Usability Challenges". *International Journal of Human-Computer Studies* 67 (1): 111–24.
Conseil de l'Europe, y Comité des ministres. 2005. *Les normes juridiques opérationnelles et techniques relatives au vote électronique*. Strasbourg: Ed. du Conseil de l'Europe.
Di Franco, Anthony, Andrew Petro, Emmett Shear, y Vladimir Vladimirov. 2004a. "Tiny Systematic Vote Manipulations Can Swing Elections". Technical Report yaleu/dcs/tr-1285. New Haven, CT: Yale University, Department of Computer Science.
———. 2004b. "Small Vote Manipulations Can Swing Elections". *Communications of the ACM* 47 (10): 43–45.
Dill, David L., Bruce Schneier, y Barbara Simons. 2003. "Voting and Technology: Who Gets to Count Your Vote?" *Communications of the ACM* 46 (8): 29–31.
Edelstein, William A., y Arthur D. Edelstein. 2008. "Touchscreen Voting Machines Cause Long Lines and Disenfranchise Voters". *arXiv preprint arXiv:0810.5577*.
Enguehard, Chantal. 2010. "Introduction à l'analyse de chimères technologiques, le cas du vote électronique". *Cahiers Droit, Sciences & Technologies, Editions du CNRS* 3: 261–78.
———. 2012. "Vote électronique: Élections cantonales 2011". Rapport exploratoire. Bruselas, Paris: Observatoire du vote.
Everett, Sarah P. 2007. "The usability of electronic voting machines and how votes can be changed without detection". Ph. D. thesis, Rice University.
Fairweather, Ben, y Simon Rogerson. 2005. "Interfaces for electronic voting: focus group evidence". *Electronic Government, an International Journal* 2 (4): 369–383.
Feldman, Ariel J., J. Alex Halderman, y Edward W. Felten. 2006. "Security analysis of the Diebold AccuVote-TS voting machine". En *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*. Boston: USENIX Association.
Fernández Riveira, Rosa María. 2013. "Argumentos de dos Tribunales Constitucionales en materia de voto electrónico". *Revista general de derecho público comparado* 13.
Franklin, Joshua, y Jessica C. Myers. 2012. "Interpreting Babel: Classifying Electronic Voting Systems". En *Proceedings of the 5th International Conference on Electronic Voting 2012*, editado por Manuel J. Kripp, Melanie Volkamer, y Rüdiger Grimm, 244–256. Lecture Notes in Informatics 205. Bonn: Gesselschaft für Informatik.
Gardner, Ryan W., Matt Bishop, y Tadayoshi Kohno. 2009. "Building Security In: Are Patched Machines Really Fixed?" *IEEE Security and Privacy* 7 (5): 82–85.
Gauld, Robin, y Shaun Goldfinch. 2006. *Dangerous Enthusiasms: E-government, Computer Failure and Information Systems Development*. Dunedin: University of Otago Press.
Goggin, Stephen N., Michael D. Byrne, Juan E. Gilbert, Gregory Rogers, y Jerome McClendon. 2008. "Comparing the Auditability of Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems." En *EVT 08*, 1–7. USENIX Association.
Gonggrijp, Rop, y Willem-Jan Hengeveld. 2007. "Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective". En *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*, 1–1. Boston: USENIX Association.
Gratschew, Maria. 2005. "Sweden". En *Getting to the Core: A Global Survey on the Cost of Registration and Elections*, editado por Rafael López Pintor y Jeff Fischer, 93–105. New York y Washington, DC: Programa de las Naciones Unidas para el Desarrollo e IFES.
Gratzer, Vanessa, y David Naccache. 2006. "Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry's Crypt". En *Proceedings EUROCRYPT 2006*, editado por Serge Vaudenay, 48–58. Lecture Notes in Computer Science 4004. Berlin, Heidelberg: Springer
———. 2007. "Alien vs. Quine". *IEEE Security and Privacy* 5 (2): 26–31.
Gray, Bill. 2005. "Australia". En *Getting to the Core: A Global Survey on the Cost of Registration and Elections*, editado por Rafael López Pintor y Jeff Fischer, 57–66. New York y Washington, DC: Programa de las Naciones Unidas para el Desarrollo e IFES.
Greene, Kristen K., Michael D. Byrne, y Stephen N. Goggin. 2013. "How To Build an Undervoting Machine: Lessons from an Alternative Ballot Design". *USENIX Journal of Election Technology and Systems* 1 (1): 38–52.
Hausmann, Ricardo, y Roberto Rigobon. 2004. "En busca del cisne negro: Análisis de la evidencia estadística sobre

fraude electoral en Venezuela". http://www.proveo.org/hausmann.pdf.
Herrnson, Paul S., Richard G. Niemi, Michael J. Hanmer, Benjamin B. Bederson, Frederick G. Conrad, y Michael Traugott. 2006. "The Importance of Usability Testing of Voting Systems". En . Vancouver, BC: USENIX Association.
Hosp, Ben, y Poorvi L. Vora. 2008. "An information-theoretic model of voting systems". *Mathematical and Computer Modelling* 48 (9): 1628–1645.
Hursti, Harri. 2005. "Critical security issues with Diebold optical scan design". Renton, WA: Black Box Voting, Inc. http://www.blackboxvoting.org/BBVreport.pdf.
Jones, Douglas W. 2007. "Computer Security versus the Public's Right to Know". En . Montreal.
———. 2010. "Kazakhstan: The Sailau E-Voting System". En *Direct Democracy: Progress and Pitfalls of Election Technology*, editado por Michael Yard, 74–95. Election Technology. Washington, DC: International Foundation for Electoral Systems (IFES).
Jones, Douglas W., y B. Simons. 2012. *Broken ballots: will your vote count?* CSLI lecture notes, no. 204. Stanford, Calif: CSLI Publications.
Katz, Gabriel, R.Michael Alvarez, Ernesto Calvo, Marcelo Escolar, y Julia Pomares. 2011. "Assessing the Impact of Alternative Voting Technologies on Multi-Party Elections: Design Features, Heuristic Processing and Voter Choice". *Political Behavior* 33 (2): 247–70.
Kerckhoffs, Auguste. 1883. "La cryptographie militaire". *Journal des sciences militaires* IX (enero y febrero): 5-38 y 161-91.
Kohno, T., A. Stubblefield, A.D. Rubin, y D.S. Wallach. 2004. "Analysis of an electronic voting system". En *2004 IEEE Symposium on Security and Privacy*, 27–40. IEEE.
La Libre. 2015. "Le parlement wallon se prononce en faveur de la fin du vote électronique", junio 3.
Lehoucq, Fabrice. 2002. "Can Parties Police Themselves? Electoral Governance and Democratization". *International Political Science Review* 23 (1): 29–46.
———. 2003. "Electoral Fraud: Causes, Types, and Consequences". *Annual Review of Political Science* 18 (6): 233–56.
Loeber, Leontine. 2008. "E-Voting in the Netherlands: from General Acceptance to General Doubt in Two Years". En *Electronic Voting 2008*, 21–31. Lecture Notes in Informatics 131. Bonn: Gesselschaft für Informatik.
———. 2011. "Voter trust in the Netherlands between 2006 and 2010". En *CeDEM11 - Proceedings of the International Conference for E-Democracy and Open Government*, 323–34. Krems: Donau-Universität Krems.
López Pintor, Rafael. 2005a. "Comparative Costs and Cost Management Case Studies Report". En *Getting to the Core: A Global Survey on the Cost of Registration and Elections*, editado por Rafael López Pintor y Jeff Fischer, 11–54. New York y Washington, DC: Programa de las Naciones Unidas para el Desarrollo e IFES.
———. 2005b. "Spain". En *Getting to the Core: A Global Survey on the Cost of Registration and Elections*, editado por Rafael López Pintor y Jeff Fischer, 81–92. New York y Washington, DC: Programa de las Naciones Unidas para el Desarrollo e IFES.
Martín, Isbelia. 2011. "2004 Venezuelan Presidential Recall Referendum (2004 PRR): A Statistical Analysis from the Point of View of Electronic Voting Data Transmissions". *Statistical Science* 26 (4): 528–42.
McDermott, Ronan. 2010. "Ireland: A Decade of Electronic Voting". En *Direct Democracy: Progress and Pitfalls of Election Technology*, editado por Michael Yard, 96–107. Election Technology. Washington, DC: International Foundation for Electoral Systems (IFES).
McGaley, Margaret, y J. Paul Gibson. 2003. "Electronic Voting: A Safety Critical System". Technical Report NUIM-CS-TR-2003-02. Maynooth: National University of Ireland.
McKay, Richard H., Paul G. Ziebold, James D. Kirby, Douglas R. Hetzel, y James U. Snydacker. 1974. Electronic Voting Machine. U.S. Patents and Trademarks Office 3,793,505, solicitada 16 de noviembre de 1972, y otorgada 19 de febrero de 1974.
Mercuri, Rebecca. 2002. "A Better Ballot Box?" *IEEE Spectrum* 39 (10): 46–50.
———. 2007. "Rebecca Mercuri's Statement on Electronic Voting". Notable Software. http://notablesoftware.com/RMstatement.html.
Michel, Gabriel, Walter de Abreu Cybis, y Eric Brangier. 2007. "Critères d'utilisabilité électorale pour la cyberdémocratie: quelques principes pour l'acceptabilité du vote électronique". *Revue d'Interaction Homme-Machine Vol* 8 (1).
Mill, John Stuart. 1861. *Considerations on Representative Government*. Londres: Parker, Son and Bourn.
Mitrou, Lilian, Dimitris Gritzalis, y Sokratis Katsikas. 2002. "Revisiting legal and regulatory requirements for secure e-voting". En *Security in the Information Society: Visions and Perspectives*, editado por M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi, y Heba K. Aslan, 469–80. IFIP Advances in Information and Communication Technology 86. Dordrecht: Kluwer.
Moher, Ester, Jeremy Clark, y Aleksander Essex. 2014. "Diffusion of Voter Responsibility: Potential Failings In E2E

Voter Receipt Checking". *USENIX Journal of Election Technology and Systems* 3 (1): 1–17.
Moynihan, Donald P. 2004. "Building Secure Elections: E-Voting, Security, and Systems Theory". *Public Administration Review* 64 (5): 515–28.
Moynihan, Donald P., y Stéphane Lavertu. 2012. "Cognitive biases in governing: Technology preferences in election administration". *Public administration review* 72 (1): 68–77.
Muir, B., y N. Moray. 1996. "Trust in automation: Experimental studies of trust and human intervention in a process control simulation." *Ergonomics* 39 (3): 429–60.
Newman, Terry. 2003. "Tasmania and the Secret Ballot". *Australian Journal of Politics and History* 49 (1): 93–101.
Norden, Lawrence, Jeremy M. Creelan, David Kimball, y Whitney Quesenbery. 2006. "The machinery of democracy: Usability of voting systems". Voting Rights and Elections. New York: Brennan Center for Justice at NYU School of Law.
Oostveen, Anne-Marie. 2010. "Outsourcing Democracy: Losing Control of e-Voting in the Netherlands". *Policy & Internet* 2 (4): 196–215. doi:10.2202/1944-2866.1065.
Oostveen, Anne-Marie, y Peter van den Besselaar. 2004a. "Ask No Questions and Be Told No Lies: Security of Computer-Based Voting Systems, Users' Trust and Perceptions". En *EICAR 2004 Conference*, editado por U. E. Gattiker. Copenhague: EICAR E.V.
———. 2004b. "Security as belief. User's perceptions on the security of electronic voting systems". En *Electronic Voting in Europe: Technology, Law, Politics and Society*, editado por A. Prosser y Robert Krimmer, 73–82. Lecture Notes in Informatics P47. Bonn: Gesselschaft für Informatik.
Oren, Yossef, y Avishai Wool. 2009. "Attacks on RFID-Based Electronic Voting Systems." *IACR Cryptology ePrint Archive* 2009: 422.
OSCE/ODIHR. 2008. *Discussion Paper in Preparation of Guidelines for the Observation of Electronic Voting*. Varsovia: OSCE - Office for Democratic Institutions and Human Rights.
Paine, Thomas. 1795. "Dissertation on first principles of government". En *Life and Writings of Thomas Paine*, editado por D. E. Wheeler, 9:260. New York: Vincent Parke & Co.
Pellegrini, François. 2014. "Chaînes de confiance et périmètres de certification: le cas des systèmes de' vote électronique'". Research Report RR-8853. Project-Team Bacchus. Talence: INRIA.
Pericchi, Luis, y David Torres. 2011. "Quick Anomaly Detection by the Newcomb–Benford Law, with Applications to Electoral Processes Data from the USA, Puerto Rico and Venezuela". *Statistical Science* 26 (4): 502–16. doi:10.1214/09-STS296.
Radio France Internationale. 2010. "Presidential poll under threat from faulty voting machines", mayo 10.
Reynolds, Andrew. 2006. "The Curious Case of Afghanistan". *Journal of Democracy* 17 (2): 113–14.
Rivest, Ronald L. 2008. "On the Notion of 'Software Independence' in Voting Systems". *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 366 (1881): 3759–67.
Selker, Ted. 2007. "Technology of Access: Allowing People of Age to Vote for Themselves". *McGeorge L. Rev.* 38: 1113–37.
Selker, Ted, y Sharon B. Cohen. 2005. "An Active Approach to Voting Verification". Working Paper VTP Working Paper #28. Cambridge, MA y Pasadena, CA: Caltech/MIT Voting Technology Project.
Selker, Ted, Jonathan A. Goler, y Lorin F. Wilde. 2005. "Who does better with a big interface? Improving voting performance of reading for disabled voters". Working Paper VTP Working Paper #24. Pasadena CA y Cambridge MA: Caltech/MIT Voting Technology Project.
Shamos, Michael Ian. 2007. "Voting as an Enginnering Problem". *The Bridge* 37 (2). .
Staszewski, Michel. 2014. "Vote électronique : une obstination technocratique". *Politique* 85 (junio): 76–81.
Stein, Robert, y Gregor Wenda. 2014. "The Council of Europe and e-voting". En *Proceedings of EVOTE 2014*, editado por Robert Krimmer y Melanie Volkamer. Tallinn: TUT Press.
Thompson, Ken. 1984. "Reflections on trusting trust". *Communications of the ACM* 27 (8): 761–763.
Tseng, Shawn, y B. J. Fogg. 1999. "Credibility and computing technology". *Communications of the ACM* 42 (5): 39–44.
Verkuil, Paul R. 2007. *Outsourcing Sovereignty: Why Privatization of Government Functions Threatens Democracy and What We Can Do About It*. New York: Cambridge University Press.
Weldemariam, Komminist, y Adolfo Villafiorita. 2012. "Can Formal Methods Really Help: Analyzing the Security of Electronic Voting Systems 361-80. Hershey, PA: Information Science Reference." En *Threats, Countermeasures, and Advances in Applied Information Security*, editado por Manish Gupta, John Walp, y Raj Sharman, 361–80. Hershey, PA: Information Science Reference.
Wheeler, David A. 2009. "Fully countering Trusting Trust through diverse double-compiling". Ph. D. thesis, Fairfax, VA: George Mason University.
Wolchok, Scott, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya

Yagati, y Rop Gonggrijp. 2010. “Security analysis of India’s electronic voting machines”. En *Proceedings of the 17th ACM conference on Computer and communications security*, 1–14. ACM.

Xenakis, Alexandros, y Ann Macintosh. 2005. “E-electoral administration: organizational lessons learned from the deployment of e-voting in the UK”. En *Proceedings of dg.o2005: the 6th National Conference on Digital Government Research Atlanta, Georgia, May 15-18, 2005*, editado por Lois Delcambre y Genevieve Giuliano, 191–97. Marina del Rey, CA: Digital Government Research Center.

Yee, Ka-Ping. 2006. “The Election System Software Supply Chain”. *Usable Security*. febrero 23.

Zucco, Cesar, y Jairo Nicolau. 2015. “Trading Old Errors for New Errors? The Impact of Electronic Voting Technology on Party Label Votes in Brazil”. *SSRN Electronic Journal*, marzo.