INTRODUCCIÓN
¿Qué es el voto electrónico?

Beatriz Busaniche y Federico Heinz

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

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

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

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

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

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

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

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

Sistemas usados

a. Sistemas de recuento automático

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

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

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

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

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

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

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

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

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

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

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

b. Sistemas de registro electrónico directo (RED)

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

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

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

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

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

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

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

c. Sistemas de votación a través de Internet

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

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

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

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

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

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

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

Principales problemas detectados en los sistemas de voto electrónico

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

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

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

1. La transparencia

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

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

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

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

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

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

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

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

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

2. *El fin del clientelismo*

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

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

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

3. La rapidez en el conteo

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

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

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

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

4. La economía

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

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

5. La participación ciudadana

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

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

---

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

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

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

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

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

6. Otros problemas generales

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

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

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

---

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