Elecciones (2004) 3, 81

Posibilidades y límites del voto electrónico

Juan Rial

EL PROPÓSITO DE ESTE TRABAJO es analizar los procesos electorales realizados con el auxilio de sistemas electrónicos mediante el estudio del proceso de introducción de la tecnología de la información (TI) en la realización de estas actividades, las que todavía, en la mayor parte de los casos, se realizan en forma manual, en especial en el acto de votar que continúa siendo el proceso de marcar una hoja de papel con la opción del ciudadano y depositarla en una urna.

Esto se debe a que, pese a la lentitud en el procesamiento de los resultados y a los costos que implica el empleo de estos métodos, las operaciones manuales siguen siendo un sistema «seguro» pues son conocidas tanto las técnicas como las medidas de seguridad que requieren. Su repetición ha permitido que la ciudadanía comprenda el proceso, y su simplicidad hace que los ciudadanos puedan confiar en «lo que ven». Sin embargo, desde hace ya dos décadas, una buena parte de las elecciones se realizan apelando, al menos parcialmente, a la tecnología de la información.

La proliferación de las encuestas a la salida de los locales de votación, llamadas también en la jerga periodística «encuestas a boca de urna», obligó a los organismos electorales a buscar formas rápidas de transmitir los resultados preliminares. También ya hace tiempo que, para facilitar las operaciones de votación, se envían a las mesas los padrones electorales en papeles

Uruguayo. Ex profesor de Ciencia Política de la Universidad de Montevideo, con estudios en Historia, Sociología y Ciencia Política, autor de libros y artículos en las áreas de elecciones, gobernabilidad, y defensa y seguridad nacional. En la actualidad es consultor de diversas organizaciones internacionales, entre ellas el PNUD e International IDEA. En el Perú se ha desempeñado como consultor a partir de 1990, su última tarea ha sido la asesoría al Congreso en la elaboración de la Ley de Partidos Políticos.

impresos en computadora. Sin embargo, una nueva etapa de cambios es la incorporación de la tecnología a otras áreas del proceso electoral.

1. DEFINICIÓN DE VOTO ELECTRÓNICO

Una *acepción amplia* del concepto de voto electrónico implica la referencia a todos los actos electorales factibles de ser llevados a cabo apelando a la tecnología de la información. Éstos incluyen el registro de los ciudadanos; la confección de mapas de los distritos electorales; la gerencia, administración y logística electoral; el ejercicio del voto en sí mismo; el proceso de escrutinio; la transmisión de resultados; y su certificación oficial. En una *acepción restringida* se refiere exclusivamente al acto de votar. En este documento empleamos la misma expresión en los dos sentidos y es el contexto el que permite saber a cuál se hace referencia en cada caso.

Al interior de la acepción restringida nos podemos referir al *voto digital* entendido como la posibilidad de sufragar utilizando Internet, o al *voto electrónico* que es el realizado por medio de máquinas y programas que no están conectados a la Red de Redes.

En el estado actual del desarrollo tecnológico no es posible aceptar el voto que utiliza Internet pues existen problemas de seguridad para garantizar la expresión efectiva del votante (la emisión del voto puede ser suplantada), tampoco se puede asegurar la privacidad (secreto) del voto; en general, es cuestionable la seguridad del sistema. Ni la adjudicación de un número de identificación personal (PIN —Personal Identification Number), ni la criptografía, ni la firma digital logran dar seguridad al voto por Internet. El punto sustancial, aun superados estos problemas, está en asegurar que quien vota sea, en efecto, el ciudadano y no otra persona. Por ello, hasta la fecha, se desaconseja su uso.

Por otra parte, el escepticismo de buena parte de la ciudadanía de algunos países acerca del secreto del voto y del rigor en su escrutinio crecería notoriamente si se impusiese una tecnología que no puede asegurar la limpieza de los procesos y de los resultados. En cambio, se recomienda el uso de mecanismos electrónicos siempre que se cumpla con ciertos requisitos para lograr que, en efecto, se garantice la expresión del ciudadano, y la privacidad y seguridad sean adecuadas.

El siguiente cuadro compara las principales operaciones de un sistema electoral manual y uno electrónico. Puede haber sistemas mixtos que realizan la identificación manual y recurren al voto y al escrutinio electrónico, u otros que sólo apelan al escrutinio electrónico.

CUADRO 1
Diferencias entre sistema electoral manual y electrónico

PROCESO		IDENTIFICACIÓN	VOTO	ESCRUTINIO
MESA	M	Control visual del documento y de la persona con el padrón de votantes.	La urna debe estar vacía al inicio. Si se usan boletas de marcar, éstas deben estar sin marcas al inicio. Pueden tener una pestaña con número o, eventualmente, ser firmadas por un integrante de la mesa para autenticarlas.	Conteo manual.
	E	Inserción del documento en la máquina de identificación. En el futuro puede preverse el uso de sistemas que comparen biométricamente al elector con un registro digital.	La mesa debe habilitar las pantallas adecuadas a la circunscipción del votante.	Conteo y preparación automática de actas finales por parte del sistema.
VOTANTE	M	El votante presenta su documento y puede pedir confrontarlo con el padrón de votantes.	El elector ve su voto, pues marca la boleta o la pone (con o sin sobre) en una urna.	El elector puede ver copia del acta de resultados al terminar el proceso.
	E	El votante debe presentar su documento.	El votante marca tocando la pantalla y, eventualmente, pulsando teclas.	
FISCAL, PERSONERO U OBSERVADOR	M	Control del fiscal que ve el padrón y al votante.	El fiscal sabe que una persona votó.	El fiscal presencia el conteo y recibe copia del acta de resultados.
	E	El fiscal puede ver si la máquina acepta la identificación.		El fiscal recibe copia del acta emitida por la máquina. Si también hay un respaldo en papel, puede pedir un recuento de votos para comprobar que coincida con el registro de la máquina.

M= Manual
E = Electrónico

2. ALGO DE HISTORIA SOBRE AUTOMATIZACIÓN ELECTORAL

Estados Unidos

En este país, las experiencias de automatización, desde la introducción de máquinas de votación a fines del siglo XIX en el estado de Nueva York (condado de Lockport), han sido diversas y han respetado, en cada caso, la autonomía en materia electoral que posee cada estado y hasta cada condado (3.155 en total), configurando la ausencia de un estándar nacional.

A este primer intento de automatización siguió la implantación del sistema de máquinas de palanca (*lever machines*) en los años treinta que también se comenzó a usar en Nueva York, manteniendo su vigencia hasta la fecha en casi todas las grandes metrópolis pues, hasta el año 2000, su uso incluía al 17,8% del electorado de cerca del 14,7% de los condados.

Luego, en los años sesenta, aparecieron las máquinas de perforar (*punch card machines*) inspiradas en las tarjetas perforadas Hollerit de la firma IBM. Estas máquinas requieren del uso de un papel y un perforador que se aplica sobre rectángulos prediseñados y los desprende (*chads*) para registrar la opción del elector y facilitar el escrutinio, que se efectúa mecánicamente. Vale anotar que en el año 2000 este sistema cubrió al 34,4% del electorado correspondiente al 19,2% de los condados.

Un paso más en esta evolución son los sistemas que emplean boletas factibles de ser escaneadas con medios ópticos, más conocidas como *marksense ballots* o *bubble ballots*. En el año 2000 cubrieron el 40,2% de los condados y el 27,5% de los electores; pero evidenciando en algunos de ellos un elevado nivel de fallas en las máquinas lectoras.

En este contexto cabe anotar el infructoso intento de imponer máquinas de votar de grabación electrónica directa: Direct Recording Electronic Voting Machines (DREVM) en 1993 en la ciudad de Nueva York que no prosperó debido a que los sistemas no superaron las pruebas de seguridad requeridas. En la actualidad esta última modalidad ha resuelto en gran medida los errores que en el pasado impidieron su adopción y en el año 2000 fue empleada en el 8,9% de los condados por el 10,7% del electorado.

En la actualidad el escenario estadounidense es mixto y en él se aplican en menor o mayor grado los sistemas mencionados, incluyendo también

sistemas manuales que emplean boletas o cédulas de votación (*ballots*), que en el año 2000 llegaron a incluir a un 1,3% del censo electoral y al 12,5% de los condados, sobre todo en zonas rurales.

Finalmente, se debe señalar que, desde la elección intermedia del año 2002, se ha evidenciado una tendencia más fuerte hacia el empleo de máquinas de votación electrónica, motivada quizá por los severos problemas experimentados por las perforadoras utilizadas durante la última elección presidencial en el estado de Florida. Sin embargo, aún existen errores que subsanar, pues las prisas por cambiar de sistema han originado notorios inconvenientes en el manejo del soporte lógico de las máquinas (*software*), así como denuncias de intentos de vender máquinas de tecnología superada.[1]

Europa

En este continente se han registrado diversos e importantes intentos de utilización de TI entre los que destacaremos algunos.

En Noruega, la experimentación con máquinas de lectura óptica de papeletas de votación se inicia a partir de 1993 en la ciudad de Oslo. Durante este mismo período también se realizaron pruebas en Dinamarca.

En España, la Comunidad Autónoma del País Vasco es pionera en la materia y cuenta desde 1998 con una legislación electoral que permite instrumentar el voto electrónico. Otras comunidades de este país también han realizado pruebas, entre ellas Cataluña, Galicia y la Comunidad Valenciana.

En Francia, la legislación autoriza el uso de máquinas electrónicas desde 1969, destacan las pruebas piloto realizadas en Estrasburgo (1994), Issy-Les-Moulineaux (1995), Lyon (2000) y Mérignac (2002), donde se ha ensayado el uso de mecanismos electrónicos con el respaldo de la Unión Europea.

En Holanda, las experiencias datan de marzo de 1995, en la actualidad se encuentra en marcha el proceso de reforma de la legislación para poder implementar un sistema de votación mediante el uso de tarjetas magnéticas.

1. En 2003, en el condado de Dade, Miami, se compró máquinas iVotronic por valor de 24 millones de dólares (alrededor de US$ 3.600 cada una) para atender a 947.000 votantes. Las máquinas mostraron problemas para poder disponer de pantallas en tres lenguas: inglés, español y creole.

En Bélgica, ya desde 1985 la empresa Dzine experimentó con máquinas de votar. El sistema empleado primero identificaba al elector por medios tradicionales y, luego, le proporcionaba una tarjeta magnetizada que se deslizaba en la máquina y permitía marcar el voto mediante un puntero de luz (del tipo de puntero láser empleado para acompañar las presentaciones en Power Point). Luego, la misma tarjeta magnética se depositaba en una urna tradicional como respaldo del proceso electoral efectuado. En las últimas elecciones municipales, celebradas el pasado 8 de octubre de 2000, este sistema fue utilizado por el 44% de los electores.

También en Bélgica, desde el 2001, las tarjetas de identidad incluyen, además de la fotografía, una firma digital, y un *chip* con dos certificados digitales, uno para la autenticación del documento y otro para la firma. Su introducción en máquinas de votación permitiría dar un paso importante hacia la total automatización del proceso electoral. Este esquema puede difundirse al interior de la Unión Europea.

En Irlanda, un sistema parecido ha sido introducido en forma experimental a partir de mayo de 2002 en tres circunscripciones electorales.

Finalmente, en Rusia existe un diseño que espera ser probado en las elecciones previstas para el año 2004.

Asia

En Japón, la municipalidad de Kawaguchi, durante 1999, experimentó con un sistema de tarjetas magnéticas impresas a partir de la selección hecha por el ciudadano en una pantalla sensible al tacto (*touch screen*), pero el piloto cubrió sólo cerca de 55.000 electores. Del mismo modo, en junio de 2002, luego de la aprobación de una norma que dio carácter legal a la votación electrónica, más de 15.000 ciudadanos utilizaron pantallas sensibles para expresar su selección en 43 mesas de votación (*polling stations*) ubicadas en Niimi (cerca de quinientos kilómetros al suroeste de Tokio), nuevamente con carácter experimental.[2]

2. Fujitsu fabrica las máquinas que serán vendidas a las municipalidades a través de una subasta. El mercado potencial, si se incluyen elecciones nacionales, podría alcanzar un valor de doscientos mil millones de dólares.

En la India también se utilizan máquinas electrónicas de votar, aunque en forma restringida en ciertos estados. Al igual que las máquinas brasileñas, desarrolladas posteriormente, éstas se componen de dos unidades. Una unidad de control que maneja el encargado de la mesa y la unidad de votación (Balloting Unit). Las EVM[3] (Electronic Voting Machines) fueron fabricadas hacia fines de 1989 e inicios de 1990 e introducidas experimentalmente en 1998 para la elección de 16 asambleas estatales (Assembly Constituencies) en los estados de Madhya Pradesh (5), Rajasthan (5) y Delhi (6).

A modo de comparación, cabe resaltar que cada una de estas máquinas puede recoger el voto de 3.840 ciudadanos, mientras que cada mesa de votación manual sólo 1.500. Por otro lado, las EVM pueden incluir hasta 64 candidatos pues su estructura permite adosar hasta cuatro unidades de votación, cada una con dieciséis botones de selección.

América Latina

En varios países de América Latina se conducen elecciones con plenas garantías desde hace casi seis décadas y las modalidades de administración electoral pasan por encargar la logística comicial a organismos autónomos ad hoc, o en todo caso, al Ministerio del Interior con la supervisión del Poder Judicial, como es el caso de Argentina.

No obstante, no todo el panorama es similar. En otros países la pérdida de credibilidad de los organismos electorales ante la persistencia del fraude, llevó a buscar la creación de nuevas organizaciones electorales o a modernizar las preexistentes. El caso más notorio ha sido el de México con la creación del Instituto Federal Electoral (IFE) y el Tribunal Federal Electoral. El primero llevó adelante un nuevo registro y una distribución más ajustada de los distritos para que el elector no tuviese que desplazarse para votar, así como procedió a la instalación de sistemas de transmisión de resultados de manera automatizada, como piezas clave de los procesos de modernización.

3. Las EVM han sido inventadas y diseñadas por la Comisión Electoral (Election Commission) india en convenio con dos empresas, Bharat Electronics Ltd. y Bangalore & Electronic Corporation of India Ltd., después de una serie de reuniones, pruebas de prototipos y amplios estudios de campo. Las EVM son fabricadas ahora por estas mismas empresas. Al tiempo de su fabricación el costo era muy bajo, alrededor de 5.500 rupias (unos 105 dólares estadounidenses); pero ocultaba notorios subsidios pues estas empresas tenían vínculos con el sector Defensa.

En Venezuela, en los años noventa comenzaron a usarse escáneres para contar los votos con rapidez pero el sistema siguió teniendo por base el uso del papel (las boletas marcadas se introducen en una máquina que cuenta los votos). Durante las elecciones realizadas entre 1999 y el 2000 estos escáneres de reconocimiento óptico de caracteres (OCR) cubrieron el total de las mesas de sufragio y su introducción implicó adaptar el diseño de las boletas, de modo que su ancho fuese compatible con la boca de entrada de las máquinas. Dadas las disposiciones electorales del país eso determinó, en algunos casos, tener boletas electorales de más de un metro de largo por 24 centímetros de ancho. Asimismo, implicó una fuerte campaña de educación cívica para enseñar a la población la forma de marcar los óvalos dibujados en las boletas electorales para que el equipo de reconocimiento de caracteres los pudiese leer.

Otro es el proceso de modernización encarado por el Tribunal Supremo Electoral de Brasil, el primer país en aplicar a la totalidad de su electorado un sistema electrónico de votación. Aquí, las experiencias comenzaron con la eliminación del viejo carné electoral con fotografía y huella digital para pasar a la identificación del elector en una base de datos y la emisión de un simple cupón (*título de eleitor*) usado en forma masiva en 1989. Luego, en 1996, se experimentó con máquinas de votación en las elecciones municipales, consiguiéndose una fuerte integración de TI en el proceso electoral. En 1998 se ampliaron las pruebas y, en octubre de 2000, se llegó al total del electorado en las elecciones municipales; lo que significó el sufragio de cerca de 109 millones de ciudadanos. En esa oportunidad, se emplearon unas 354.000 urnas distribuidas en 315.000 secciones electorales por todo el país, se eligió 5.549 prefectos, intendentes o alcaldes, y 57.316 concejales de municipios. Por último, la prueba final se dio en el proceso de octubre de 2002 para renovar presidente, congresistas federales y autoridades estatales. En estos comicios se llegaron a instalar cerca de 406.000 urnas que recibieron el voto del 80% del electorado brasileño (95 millones de personas).

Finalmente, en Paraguay, en la elección general de abril de 2003, se esperaba utilizar el sistema de votación electrónica en una parte sustancial del electorado (la previsión inicial era para el 53%); pero las discusiones entre el tribunal electoral y los partidos terminaron por determinar un número menor. Se utilizaron máquinas brasileñas prestadas por el estado de Paraná.

3. ALCANCES ACTUALES DE LA AUTOMATIZACIÓN ELECTORAL

Los sistemas pueden estar totalmente integrados por componentes electrónicos y/o digitales, o parcialmente computarizados al mantener el carácter manual del resto de las operaciones. Los sistemas integrados de votación electrónica implican que el proceso de identificación del ciudadano, el acto del voto, el escrutinio y la transmisión y consolidación de datos se haga con máquinas electrónicas y medios digitalizados. Hasta el presente ningún país ha llegado a este nivel.

En los sistemas que usan parcialmente tecnologías electrónicas hay varias posibilidades y existen diversos ejemplos de su aplicación en distintos países. El caso más común es la transmisión de resultados a través de líneas telefónicas, de facsímil e, incluso, de teléfonos satelitales, para su procesamiento mediante computadoras. Todo el resto de la tarea es manual. La gran mayoría de los procesos electorales actuales cae dentro de esta categoría; pues son muy pocos los países que esperan a finalizar el recuento oficial manual para difundir los resultados electorales.

El uso de máquinas ad hoc para votar DREVM (de grabación electrónica directa que ya hemos mencionado) ya se ha impuesto en varias circunscripciones de EE. UU. y en Brasil.

Para la transmisión de resultados se utiliza Internet con diversos tipos de conexión, líneas dedicadas, telefonía tradicional, celular o satelital, además de los sistemas tradicionales de transporte directo de los datos. Su procesamiento requiere el uso de programas de conteo ad hoc capaces de hacer las operaciones necesarias para la adjudicación de cargos, según las normas legales existentes y de acuerdo a instrucciones impartidas por el programa correspondiente.

Para la identificación del votante se está buscando desarrollar nuevos sistemas, pues la emisión de documentos con códigos de barras o códigos magnéticos no mejora en mucho los niveles de identificación respecto a la mera constatación visual de una persona y su documento que, en muchos casos, cuenta con una fotografía. Para quien carece de un entrenamiento específico, como es el caso de los miembros de mesa, es muy difícil afirmar que la persona que presenta un documento es la misma que los datos allí registrados indican. Al pasar una banda magnética o un código de barras por un

escáner pueden aparecer en la pantalla los datos de la persona o, simplemente, indicar que la tarjeta corresponde a una persona registrada. Claro que el sistema permite indicar que esa tarjeta presentada sólo puede usarse una vez.

Un sistema «seguro» implicaría la comprobación in situ de datos biométricos; por ejemplo, la constatación de las huellas digitales escaneadas que serían confrontadas con las registradas al momento de ingresar al padrón; o el registro del iris de la persona que se presenta a votar. Pero estos sistemas son todavía muy caros y aún lentos para identificar a poblaciones numerosas, porque implican contrastar los datos de cada persona en el registro de una base de datos, y luego frente a todo el universo registrado para evitar que se vote más de una vez.

Para el proceso de escrutinio se puede apelar al uso de escáneres, máquinas que reconocen marcas. Normalmente consisten en círculos, óvalos, rectángulos o cuadrados rellenados con tinta o grafito que indican la opción u opciones del elector; hecho el reconocimiento, la máquina almacena los datos. En varios de los exámenes de control masivo realizados en universidades o institutos secundarios también se suele utilizar este mecanismo. La máquina «lee» las marcas y, al finalizar el acto electoral, consolida y transmite los resultados. Como hay un respaldo en papel, pues se guardan las boletas escaneadas, se puede comprobar si el conteo electrónico corresponde al total registrado en el papel.

El lector óptico, por su parte, es un instrumento que automatiza el escrutinio, mientras que el proceso de votación sigue realizándose en forma manual. Se diseña una boleta de votación que contiene óvalos (o rectángulos, cuadrados o círculos) que deben ser rellenados. Algunos de los aparatos requieren el uso de lápices de grafito suave (tipo F) lo que hace necesario disponer de un buen stock de marcadores, pero los equipos más recientes aceptan cualquier tipo de tinta para rellenar, excepto la roja. Es posible efectuar recuentos porque los votos originales pueden guardarse y volverse a contar, sea mediante escáner o en forma manual. La principal razón del uso de estos equipos es acelerar el proceso de escrutinio y disponer de resultados en tiempos cortos.

4. LOS PRINCIPIOS QUE DEBEN SER GARANTIZADOS

Todo organismo electoral debe cumplir con requisitos básicos para asegurar la integridad del proceso electoral. La *igualdad* supone una persona un voto.

La *accesibilidad* implica que todos los ciudadanos deban tener la posibilidad de votar y, también, de ser candidatos de acuerdo con las normas constitucionales y legales existentes. Debe garantizarse que el voto sea *secreto*. El proceso debe ser *transparente*, abierto a la observación de todos los ciudadanos. El proceso electoral deber ser *neutral* pues no debe favorecer a ninguna fuerza partidaria o candidato sobre otros. La *simplicidad* es necesaria para que con una mínima instrucción del votante se pueda evitar los errores. También se requiere *flexibilidad* y *movilidad* pues el sistema debe ofrecer alternativas para quienes viajan y para quienes tienen problemas físicos de modo de no negarles el derecho a voto.

El proceso debe cumplir con el principio de *verificabilidad*, debe ser auditable en cada una de las etapas de su funcionamiento. Asimismo se requiere *rapidez en el recuento y transmisión de resultados*, ya que el sistema debe producir resultados confiables en el menor tiempo posible para no crear incertidumbre en el ámbito político. El sistema a adoptar debe también evitar la rápida obsolescencia, es decir asegurar *durabilidad y un costo razonable*; lo que significa que los sistemas de votación electrónica deben ser «mejorables» (*up grading*) para mantenerse en un costo razonable.

Dado que una elección no es un estudio basado en muestras probabilísticas, sino una consulta total a un universo definido, por principio no puede aceptarse la existencia de márgenes de error: *el resultado debe ser exacto*, reflejando la voluntad precisa de ese cuerpo ciudadano; debe registrar sin errores la voluntad de los ciudadanos votantes, sin ninguna alteración, asegurando así la *integridad* del proceso. Los sistemas electrónicos, al eliminar opciones dudosas que normalmente se presentan en sistemas manuales (doble voto, marcas fuera de los recuadros habilitados, boletas defectuosas o arruinadas, etc.) permite superar este problema. Pero, al mismo tiempo, los problemas de seguridad de los sistemas electrónicos pueden ser importantes.

5. EL SECRETO DEL VOTO Y LA CONFIABILIDAD DE LOS RESULTADOS

El principal problema de seguridad en los procesos de votación electrónica es la posibilidad de acceder al contenido del voto que puedan tener operadores, programadores o «súper usuarios» del sistema: que, mediante la manipulación de los programas del sistema antes, durante o luego del sufragio,

traten de conocer la identidad y preferencias de los electores o de cambiar su voluntad.

El principio constitucional del voto secreto y la necesidad de contar con procesos «limpios» hace que deba prevenirse que esto no ocurra, pues de lo contrario la confiabilidad del sistema desaparece. En los procesos manuales no existe este «súper usuario» y éste es el principal argumento contra la utilización de tecnologías modernas en los actos electorales.

La implementación de un proceso electoral demuestra, sin embargo, que siempre hay errores, sea en un proceso manual o en uno automatizado. Sin embargo, estos errores sólo pueden ser aceptados si no influyen en el resultado final de un proceso electoral. De lo contrario, si el margen de error detectado es mayor al de la diferencia entre ganador y perdedor de una elección, sólo queda un recurso: anular el proceso y repetirlo. Dado que esa posibilidad plantea grandes problemas y desasogiego en el conjunto de ciudadanos hay que extremar las medidas para evitar los errores.

Condiciones para un voto electrónico seguro

La principal «sospecha» que recae sobre un proceso electrónico es su grado de seguridad frente a uno realizado en forma manual. Por consiguiente, un sistema de voto electrónico debe estar atento a toda posibilidad de intervención indebida en el proceso, sea desde dentro o desde fuera del sistema.

En el acto de votar que, por sus características, no permite realizar correcciones, se aconseja utilizar mecanismos electrónicos de votación en una red cerrada sin conexión con Internet. Pero esa red cerrada, de todos modos debe cumplir con requisitos importantes de seguridad. Los que indicamos a continuación.

1. Integridad del sistema: tanto los equipos (*hardware*) como los programas (*software*) deben ser diseñados a prueba de fraudes. Idealmente no podría haber cambios una vez que se inicia el proceso electoral. Una vez certificados el equipo, el código fuente, los parámetros iniciales, la información referida a la configuración, y los programas básicos y rutinas deberían permanecer estáticos hasta el fin del proceso. Solamente podrían ingresarse datos y procesarlos de acuerdo a lo establecido previamente.

2. El *código fuente debe ser propiedad de la autoridad electoral responsable y no de la firma proveedora de los materiales*. Los equipos y programas del sistema, incluyendo el código fuente, deben estar disponibles para inspección en todo momento, así como toda la documentación de respaldo (manuales técnicos y de operación). No puede haber reclamos de secreto de parte de proveedores privados. Sin embargo, se sabe que la «oscuridad» es reclamada como necesidad para asegurar los sistemas. El acceso libre al código fuente, simplemente para verlo, para verificar su contenido y adecuación sin ninguna posibilidad de modificarlo, supone que sólo quienes tienen autorizaciones adecuadas (funcionarios electorales, delegados partidarios o de organizaciones de observación) puedan hacerlo. Quienes hacen la tarea deben pasar por controles de seguridad que aseguren su integridad personal.

La comprobación de la identidad del votante es un paso vital en el proceso electrónico de votación.

3. Sin embargo, hay que tener en cuenta los diversos niveles en los que opera el sistema, de modo que quienes estén autorizados para auditarlo puedan acceder a todos los niveles de la programación y no sólo a los programas que corren «superficialmente» (en los niveles superiores).

4. Quienes pueden acceder al sistema, sea para operar o para auditar, constituyen el eslabon débil de la cadena de seguridad. Al ser sus custodios se plantea la vieja máxima: *Qui custodies ipsos custodios* (¿Quién controla a los que controlan?).

5. El uso de la redundancia, o de programas que reiteran por otro camino el mismo proceso, parece en principio una buena idea para descubrir falencias, pero también las puede incrementar; por ejemplo, un virus puede introducirse al mismo tiempo en más de un programa de comprobación. Se recomienda el uso de algoritmos especiales que sean tolerantes a «n»

número de componentes con problemas, aunque se sabe que pueden llegar a fracasar al llegar a un «n + 1».

6. Los manuales y toda la documentación relativa al sistema deben estar redactados con claridad. No pueden ser inconsistentes ni contener frases ambiguas que planteen dudas, ni deben adolecer de falta de información sobre cada aspecto del proceso. El estándar de la industria informática respecto a la redacción de manuales que, precisamente, opta por la oscuridad para competir en el mercado, no puede ser aceptado. La documentación debe ser muy precisa sobre todo en lo referido al tema de seguridad, alertando de los problemas que eventualmente pueden presentarse.

7. El diseño, implementación y mantenimiento del sistema debe tender a llevar a cero las posibilidades de que haya un mal funcionamiento (*bugs*) en el sistema, así como de introducción de virus durante su operación. De ahí la necesidad indicada de no proceder a cambios luego de la auditoría que certifica que es adecuado para conducir la elección.

8. Los sistemas muy centralizados pueden conducir al peligro por la tentación de manipulación de parte de «súper usuarios» y facilitar así los intentos de subvertir el sistema a partir de una operación también centralizada y comprometer todo el proceso. Pero también, por otro lado, los sistemas que suponen un manejo fraccionado, desconcentrado, de las operaciones requieren mayor control en el diseño para evitar problemas de compatibilidad entre ellas y de una mayor cantidad de tiempo y personal para verificar su operación. La solución debe suponer el desarrollo de sistemas que funcionen coordinadamente pero desconcentrados. Para ello, se recomienda tener un sistema de registro y verificación de la identidad del votante, otro sistema para votar (integrado o no al de escrutinio), y uno de transmisión de resultados.

9. Si se utilizan máquinas de votar del tipo DRE, éstas deberían permitir dejar evidencia física del voto para poder recontarlo y responder a eventuales reclamos y dudas. La mayoría de las máquinas DRE existentes en el mercado no dejan esa evidencia; sin embargo, algunas empresas ya ofrecen la posibilidad de producir tarjetas magnéticas que dejan constancia del voto y permiten una auditoría posterior. Es cierto que al introducir un voto impreso se encarece notoriamente el sistema y se deja de lado el ahorro que se producía al desaparecer el papel. Sin embargo, la

desconfianza que puede generar el sistema en un inicio, debería ser superada apelando a esta redundancia. Por ello sería recomendable que, por un tiempo, se utilice subsidiariamente esas tarjetas («el papel»).

10. Hay máquinas que pueden producir una cinta de papel con los resultados en lugar de los *chips* o tarjetas de memoria. Los carretes de papel impreso son relativamente «fáciles» de suplantar por lo que usar máquinas de ese tipo también implica mayor vulnerabilidad. Su uso se desaconseja. Los datos ingresados al sistema deben ser verificados adecuadamente de modo que sólo ingrese información correcta proveniente de fuentes que también deben ser a prueba de fraude.

11. Debe asegurarse el voto secreto de modo que no se pueda acceder a conocer la voluntad del elector tanto desde dentro como desde fuera del sistema. No puede haber asociación entre los sistemas de identificación del votante y el proceso de votar que permitan conocer el sentido del voto. Debe haber sistemas coordinados, paralelos pero no integrados, de identificación del elector y del voto. Hay quienes abogan por sistemas integrados que permitan el enmascaramiento de la identidad del elector y que no pueda revertirse los datos del voto para asociarlos con los del elector. Pero, para lograrlo, hay que hacer desaparecer las posibilidades de auditar el sistema posteriormente.

12. Los operadores internos del sistema deben asegurar que no se pueda ingresar a éste «por puertas traseras», mediante simples códigos alfanuméricos (*passwords*) que permitan el acceso al personal de mantenimiento del sistema, dando así oportunidad a la existencia de operaciones de fraude. La autenticación para el ingreso del operador debe ser del mismo tipo que la usada por organismos de seguridad e inteligencia. El personal que manipula los equipos debe estar sujeto al uso de mecanismos de identificación precisos de caracter biométrico y, posiblemente, utilizar más de un sistema (asociación de identificación del iris o huellas digitales, por un lado, para poder trabajar en los equipos y sus programas, y de pases específicos con códigos alfanuméricos para el ingreso a lugares restringidos, por el otro).

    Todo ingreso al sistema de quienes operen en él debe ser registrado sin posibilidades de borrar ese dato sin afectar su funcionamiento para establecer cualquier responsabilidad posterior. Se debe mantener un

inventario en tiempo real de la situación de los sistemas de administración y de distribución de los equipos periféricos, así como de los materiales fallados y su eventual reemplazo. Esto último no requiere tecnología especializada sino sistemas de gerencia adecuados. La seguridad incluye también la del local en el que se instalan los equipos y al que ingresan los funcionarios.

13. Se sabe que, finalmente, todo sistema es vulnerable y que existe siempre la posibilidad de subvertirlo por la vía de introducir virus que operan como «caballos de Troya» que no necesitan modificar el código fuente. También se sabe que pueden instalarse *bugs* que burlan los números criptográficos de comprobación. Los sistemas basados en computadoras personales son vulnerables a la aparición de falsos sistemas paralelos, es decir suplantadores, y la presencia de controladores «súper usuarios» puede llevar a la venalidad. Pero todo ello requiere de oportunidades y cierta laxitud de parte de los administradores. Se trata de realizar auditorías constantes y chequeos al sistema.

    Los funcionarios electorales mexicanos que, a fines de los años noventa, debían luchar contra la imagen que hacía equivaler una elección a un fraude, expresaban esta actitud que permitió un cambio sustancial en esa imagen con la expresión: «Hay que disponer de candados, contracandados y candados para los contracandados». Esa noción llevó a encarecer notoriamente el sistema debido al alto grado de redundancia de los controles e introdujo otros problemas, pero fue eficaz.

14. Además de los test iniciales y la certificación correspondiente, el sistema debe ser auditado una vez completado el proceso produciendo una evaluación integral de su operación.

15. El sistema debe permitir imprimir en papel las operaciones realizadas de modo de comprobar resultados, en diversas fases de la operación.

16. Al igual que las actuales leyes electorales, que suelen ser muy minuciosas respecto a los procesos manuales y, en muchos casos, requieren para su aprobación de mayorías especiales, todas las operaciones de los sistemas electrónicos de votación deben estar previstas en una legislación precisa y no dejada exclusivamente en manos de regulaciones emitidas por autoridades electorales o por personal de esos organismos. En muchos casos ni

siquiera son estas autoridades las que proponen las normas aplicables sino los funcionarios de las firmas a las que se encarga las operaciones mediante soluciones para todo el proceso (*end to end*) mediante contratos «llave en mano». Debe preverse lo esencial de modo que la toma de decisiones sustanciales del proceso no quede al arbitrio de quienes manejen el nivel técnico operativo, sean funcionarios estatales o de empresas privadas.

El aspecto más relevante de la seguridad es el personal que desarrolla, supervisa y administra el voto electrónico. Este personal debe poseer niveles de confianza certificados y debe ser remunerado en forma adecuada. Votar requiere criterios de alta seguridad que normalmente no son los aplicados en sistemas comerciales de operación. Demanda madurez y disciplina en el personal que maneja el sistema. El costo de operar sistemas de alta seguridad es casi el cuádruple de lo convencional y, aun así, pueden aparecer problemas.

6. SISTEMAS Y MÁQUINAS: EL CASO DE BRASIL

En Brasil los equipos utilizados en 1996 fueron proporcionados por Unysis do Brasil, y en 1998, 2000 y 2002 por la empresa Procomp, que puso al día las máquinas utilizadas anteriormente y dispuso de nuevas. Los programas fueron desarrollados para el Tribunal Superior Eleitoral, con asesoramiento de sus funcionarios, por las empresas Microbase, proveedora del *software* básico; y VirtuOS, del sistema compatible con MS Dos y Windows; y el *software* de aplicación por la empresa Procomp.

Las comunicaciones de la red de transmisión que consolida los resultados contenidos en los disquetes en los servidores de los organismos electorales utilizan para proteger los datos un programa denominado «biblioteca de criptografía», proporcionado por el Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC), organismo gubernamental dependiente de la Presidencia. La adopción del sistema fue impulsada por el Tribunal Superior Eleitoral, contando inicialmente con el apoyo de los ministerios del Ejército y de Aeronáutica (hoy dependencias del Ministerio de Defensa) y del INPE (Instituto Nacional de Investigaciones Espaciales).

El *hardware* del sistema lo componen una unidad de control, un pequeño computador que procesa los datos con un sistema de doble encriptación, y

Despliegue de urnas electrónicas durante elecciones nacionales brasileñas.

una unidad de votación. La unidad de control, denominada MT-UE (Microterminal da Urna Eletrônica), es una computadora que tiene un procesador Cyrix de 100 Mhx, una memoria de tipo *flash card* (tarjeta rápida) de 15 Mbytes, y una impresora térmica interna. Tiene, además, un pequeño visor para ver las operaciones.

La tarea del miembro de mesa es reducida. Comienza por introducir el número del llamado «titulo del eleitor», es decir el número de registro en el padrón. La unidad de control puede ser acondicionada para recibir una tarjeta con banda magnética o código de barras para la eventual identificación del elector si se emitiese con esa información. El microterminal tiene tres indicadores de luz: uno señala que la unidad está conectada a una fuente de energía (rojo), otro (amarillo) indica que la urna está siendo utilizada por el elector, y un tercero (verde) que está disponible para su uso.

El sistema puede alimentarse por la red de energía eléctrica común, pues la máquina puede funcionar tanto con 110 como con 220 voltios en forma automática. Si no hay energía la máquina posee una batería interna que, en el modelo 2000-2002, llega a doce horas de autonomía; aunque en el modelo de 1998 alcanzaba para sólo tres horas, y en los primigenios a una hora y media.

El MT-UE es un módulo físico conformado por una pantalla y una botonera con números y tres teclas: una para corregir, una para votar, y otra para la opción de voto en blanco. La botonera está dispuesta en la misma forma que en un aparato telefónico; dispone de puntos en Braille, así como de un botón en el número cinco para identificar esa tecla. En el año 2000 se agregó una unidad de sonido que reproduce lo indicado en la pantalla para informar al elector del contenido de ésta antes de su confirmación.

La unidad de voto tiene una placa *flash card*, memoria de lectura y escritura que almacena el *software* básico y aplicado que contiene los datos referidos a los partidos y candidatos para mostrar las pantallas al elector, así como el archivo de electores de la sección electoral correspondiente. Otra *flash card*, removible, tiene los archivos complementarios para que la unidad pueda funcionar. El disquete es el disco removible para la transferencia de los datos de la elección.

El proceso

El elector inicia el proceso digitando un número que corresponde al candidato de su preferencia. Dado que en Brasil existe el «sistema preferencial» (que permite escoger dentro de una lista partidaria a un candidato determinado) en las elecciones municipales se utilizan hasta cinco números. Los dos primeros identifican a la organización partidaria y los tres restantes al candidato a miembro de los concejos municipales (*vareadores*). Los números se reducen en otros casos al haber menor número de candidatos. Si el elector no quiere hacer uso del voto preferencial sólo digita los números del partido. Al hacerlo aparece una pantalla que indica qué candidato está eligiendo (una fotografía suya, su nombre, su partido y ubicación en la lista preferencial). Si está conforme, presiona la tecla VOTAR; si no es ésa su opción, puede corregir. Si lo desea puede ir directamente a la tecla de voto en blanco. Si utiliza números equivocados e igual selecciona la tecla de votar, su voto será nulo. La empresa busca corregir este problema tratando de impedir que se use esa opción.

Luego de votar en una categoría se vuelve a digitar para otra. Por ejemplo, en una elección municipal luego de optar por «vareador» aparecen las pantallas correspondientes a «prefeito» o intendente. Si hay otras elecciones pueden aparecer pantallas para votar a diputados estatales, gobernador del estado, diputado federal, senador y presidente, culminando el proceso. En todos

los casos se pide al elector que lleve anotados los números de los candidatos que prefiere y en el local de votación se exhiben en carteles las opciones existentes.

Cuando el elector ha acabado de votar, aparece la palabra FIN en la pantalla de la microunidad y se enciende el indicador de LIBRE en la unidad de control, por lo que no puede seguir usándose hasta que se habilita nuevamente por parte de quien maneja esa unidad de control. Al elector le es devuelto su documento de acreditación con la constancia de haber votado y finaliza así su actuación en la elección.

Al terminar el proceso electoral el encargado de mesa debe digitar una contraseña (*password*) para indicar que el proceso ha concluido en esa máquina de votación y que se debe imprimir el primer ejemplar del llamado «Boletim da Urna». Si la impresión no envía mensaje de error, el presidente presiona la tecla CONFIRMA en el teclado de la máquina de votar; y entonces se imprimirán los otros cuatro ejemplares del boletín y se grabarán los datos en un disquete interno de la unidad de control. De los cinco ejemplares impresos, el encargado de mesa deja uno en el local electoral para información pública, entrega un segundo a los fiscales de los partidos, y los otros tres son enviados, junto con los documentos de votación, a los centros de acopio. Allí los disquetes se procesan en un totalizador que envía los datos a los registros centrales para comunicar los resultados.

El boletín de urna indica el total de votos por partido, por candidato, votos en blanco, votos nulos, identificación de sección, zona electoral y municipio, hora de inicio y de cierre del proceso de votación, y el código de seguridad que corresponde a esa urna.

Cada sección electoral debe emitir un documento inicial indicando que la máquina no tiene ningún registro antes de comenzar la elección, denominada en la jerga operativa de ese sistema «zerésima» (o «puesta en cero»).

Costos y problemas

El equipo es compacto y mucho menos pesado que muchas de las DRE que se utilizan en EE. UU. Requiere sí de un cableado mínimo entre la fuente de energía y la unidad de control, a menos que emplee su batería, y entre esa unidad de control y la unidad de voto que debe disponerse en forma tal que

el elector goce de privacidad. Cada máquina atiende alrededor de quinientos electores.

El costo inicial de cada equipo se estimó en US$ 945 cuando los proveyó Unisys (1996); en 1998 Procomp lo estimó en US$ 700, luego en 2000 en US$ 550, y, finalmente en 2002, en US$ 500. En total la inversión en «urnas electrónicas», con el valor actual, es cercana a los cien millones de dólares. Si se agregan los programas y la transmisión de resultados se estaría hablando de una inversión probable de unos 450 a 500 millones de dólares. Con un electorado registrado de alrededor de 105 millones, sólo el costo de los equipos es de un dólar por elector. Si se agrega el costo de los totalizadores, equipos de control y transmisión de datos y del *software* para su uso, se estaría en cerca de tres dólares por voto. Seguramente se trata de un costo bajo debido a subsidios o costos escondidos que no se facturaron. En forma aproximada, esos costos «escondidos» más el costo de funcionamiento normal del sistema electoral, que incluye el registro de votantes y el mantenimiento de la administración, hace subir esa cifra a unos cinco o seis dólares por voto.

El personal técnico del Tribunal Superior Eleitoral sostiene que el sistema brasileño siguen las normas ISO 15.508, de diciembre de 1999, e ISO 9594-8, que establecen criterios de evaluación de seguridad en el ámbito de la tecnología de la información. Sin embargo, uno de sus críticos, el ingeniero Amílcar Brunazo (1999) dice que la norma ISO 15.508 nunca se aplicó en una evaluación del sistema de urna elecrónica que se emplea en Brasil.

Al respecto, hay un punto a discutir que no hemos visto en el debate brasileño: para que un sistema pueda ser considerado seguro, en una instancia de alto riesgo como es una elección en la que no existe la posibilidad de corregir errores pues el tiempo constriñe a una sola oportunidad, *se requeriría de una norma específica* que aún no existe.

Por otro lado, una evaluación de parte de los partidos supone que éstos tengan interés en hacerla, lo que implica acreditar técnicos para las necesarias fiscalizaciones. Las normas legales brasileñas lo preven pero, prácticamente, no se ha realizado. Como es el proveedor de la urna quien instala el programa básico, los controles deben hacerse al momento de su entrega para poder instalar los programas de aplicación, o sea aquellos que contienen los datos con las listas de partidos y candidatos para cada circunscripción; y una auditoría completa, no estadística, para llegar a un nivel de error

cero que permita asegurar a los participantes que todo está en orden. Esto requiere de un importante número de técnicos y de horas de trabajo que no están al alcance de ningún partido político en tiempos en los que la militancia se reduce a aquellos que pugnan por un cargo. Habría que recurrir a técnicos contratados, lo que tampoco es factible por los costos que implica. La alternativa sería una auditoría basada en principios probabilísticos.

A su vez es lógico tener en cuenta que ninguna empresa proveedora de productos para un sistema electoral electrónico quiere tener problemas que podrían sacarla del mercado. Esa auditoría independiente debería ser realizada por una comisión técnica que debería contar con miembros de los partidos políticos y, eventualmente, de organizacines de la sociedad civil que trabajen en el tema de la participación ciudadana. Puede contratarse una empresa ad hoc que no tenga ninguna relación con las empresas proveedoras de los servicios, ni directa ni indirectamente, que debe realizar su tarea en presencia de los técnicos de los partidos y de la sociedad civil que estén interesados.

Las máquinas deben ser auditadas antes del proceso electoral para determinar que están en cero, deben ser cargadas con el programa de aplicación en las horas indicadas para hacerlo y siguiendo todos los procedimientos establecidos. Es obvio que en el caso de Brasil, con casi medio millón de máquinas, haya habido errores en estos procesos o no se haya seguido los pasos previstos. Igual que en los sistemas manuales, no es fácil contar con gente con el entrenamiento adecuado para todas las tareas. A pesar de todas las críticas, la introducción de las máquinas ha resultado un avance importante para el proceso electoral brasileño.

7. RECOMENDACIONES

Un sistema de votación es más que una tecnología. Es sustancialmente resultado de un consenso que se ha expresado en leyes y otras normas legales adecuadas a la situación de la sociedad política donde se aplican, mediante los cuales se dirimen contiendas políticas. Ese consenso básico tiene por actores a organizaciones e instituciones y prácticas, regladas formal o informalmente, que son parte de la cultura política del país. Las disposiciones legales son resultado de los consensos y los actos electorales están regulados por leyes y principios constitucionales.

La implementación de las elecciones supone recurrir a tecnologías aceptadas legalmente, por ello, se debe partir de la naturaleza histórica, cultural y política de los procesos electorales para poder decidir cuál es la tecnología que puede emplearse. Una misma tecnología en dos sociedades diferentes, o en la misma sociedad en tiempos distintos, produce resultados diferentes. Un cambio en la tecnología que busca el empleo de soluciones modernas no siempre es una garantía de mejora del sistema. Por ello se necesita evaluar primero el impacto en la cultura política de la introducción de nuevas tecnologías y si éstas responden a una necesidad de la sociedad.

Equipos y programas

Ya hemos descartado el uso de Internet en los procesos de votación en el día de la elección, salvo en la transmisión de resultados o en otras activiades administrativas. Y aun así, si bien se puede utilizar Internet para la transmisión de resultados, debe hacerse en paralelo con otros sistemas para evitar los riesgos que entraña.

En cambio, puede considerarse la introducción de sistemas electrónicos de votación que deben ser acompañados de un esfuerzo educativo de gran escala, pues es sabido que en los sectores populares aún existen dificultades para operar en cajeros automáticos o mecanismos similares y que lo mismo ocurriría con los sistemas de votación electrónica. Se debe difundir de un modo tal el desarrollo de habilidades en el uso de la tecnología que, en sí misma, *no distraiga al votante del fin que es elegir y no aprender a enfrentar una máquina*.

El foso que divide a los sectores que, como usuarios, dominan la tecnología electrónica digital de aquellos que no lo hacen en gran medida corresponde a una división por niveles educativos y sociales de la ciudadanía, y debe ser tomado en cuenta al adoptar sistemas electrónicos de voto.

El punto más sensible para la adopción de un sistema electrónico es la seguridad, la que implica confiabilidad en el sistema. Existen notorios incentivos para quienes trabajan dentro del sistema para apelar al fraude luego de recibir sobornos; no obstante, deben distinguirse los intentos de fraude de los «accidentes» que suelen producirse en los procesos de computación. Para certificar la adopción de un sistema se debe tener en cuenta las normas de seguridad para el voto electrónico que hemos señalado.

Los sistemas están compuestos por equipos (*hardware*) y programas (*software*). El equipo debe ser sencillo, robusto, pues debe poder ser operado en muy diferentes ambientes, en muchos casos por parte de personas con poco entrenamiento en tecnología de la información; fácil de almacenar; y capaz de ser reciclado de modo que pueda mejorarse.

Los programas deben ser propiedad del organismo electoral y no de la empresa que los provee. No se trata de adquirir licencias sino de adquirir el código fuente; lo que supone una inversión importante del organismo electoral para crear una unidad ad hoc en ese campo. Una alternativa es un convenio con un organismo internacional multilateral que pueda garantizar los programas y, eventualmente, los equipos.

Más adelante, especialmente para países más pequeños, puede explorarse también la posibilidad de compartir el uso de equipos y programas por más de un país para reducir costos. Las asociaciones de organismos electorales pueden manejar, junto con organismos internacionales multilaterales, un depósito de máquinas y programas y un equipo técnico mínimo que pueda ponerse a disposición de cada país por medio de mecanismos de licencia. La propiedad de los equipos y programas pasa a ser colectiva de los países que participan en ese acuerdo. Este tipo de arreglo requiere convenios políticos supranacionales, tratados de modo que puedan ser legalmente viables.

Máquinas

Las máquinas deben ser de diseño sencillo y peso ligero, de modo que sean fáciles de transportar y almacenar, requiriendo un mantenimiento mínimo y simple. No deben tener partes movibles ni necesitar de un sistema complicado de cableado, que se debe reducir a lo necesario para obtener energía eléctrica, más barata que las baterías, y para conectar unidades de control y de voto. Se puede evitar el uso de cables, pero las posibles interferencias no garantizan la seguridad del proceso.

Dados los posibles problemas con la energía eléctrica, o su inexistencia, deben tener su propia fuente de energía. Sería deseable que operasen con pilas estándar (ya hay máquinas que las utilizan).

Las máquinas deben permitir incluir en la pantalla todas las papeletas o balotas que están en juego en un momento dado para que el elector pueda

tener todas las opciones que considere conveniente. Asimismo, deben permitir al elector votar desde cualquier lugar para la circunscripción en la que le corresponde ejercer el voto. Deben permitir cambios de diseño de último momento de acuerdo con lo dispuesto por las regulaciones correspondientes.

Las máquinas deben ser de fácil acceso para que puedan votar quienes tienen impedimentos físicos. Por ello tienen que tener pantallas que permitan ver claramente a quienes tienen visión defectuosa; tener un mecanismo de audio para facilitar el voto de personas con ceguera; ser trasportables para que voten personas que no pueden bajarse de un vehículo; y adaptables para quienes usen sillas de ruedas. Deben disponer de adminículos alternativos para quienes tengan dificultades en la utilización de sus manos. Ya se están probando soluciones para cada uno de estos problemas por parte de los diversos fabricantes.

Escrutinio

Los sistemas deben ir registrando el voto a medida que se va produciendo, sin que sea accesible a otras personas. A los efectos de control puede requerirse que la máquina emita una tarjeta magnética que contenga el dato del voto individual de cada persona sin que aparezca ligado a la identificación del votante a los efectos de recuento y verificación. Esta tarjeta podría otorgarse en duplicado para que el propio votante verifique si su voto fue adecuadamente registrado.

Al finalizar la hora de votación la tarea de los miembros de mesa debe ser mínima: retirar el *chip* de memoria (disquete, cilindro o tarjeta PCMCIA, etc.) con los resultados para ponerlo en el mecanismo de transmisión o, si el sistema dispone de un cartucho impresor de votos, retirarlo. Asimismo, se puede proceder a una verificación de los votos mediante la lectura de las tarjetas magnéticas individuales. Finalmente, deberán empacar las máquinas y materiales utilizados para su devolución.

SERÍA ACONSEJABLE QUE EXISTA un comité de evaluación de calidad de los sistemas electorales que establezca criterios previos para adoptar el sistema. Los partidos políticos y sus representantes, los organismos electorales y representantes de organizaciones cívicas promotoras de la limpieza de los procesos electorales tienen mucho que decir al respecto. Establecidos los criterios, debe

procederse a convocar las ofertas de acuerdo con las normas legales y, luego, a una evaluación de los sistemas ofrecidos por las empresas privadas.

Si se adopta la decisión de implantar un sistema electrónico de votación para conseguir el máximo grado de legitimidad, se recomienda que, antes de la adopción de la legislación que lo autoriza, se realice un debate amplio entre todos los sectores interesados de los partidos políticos y de la organización electoral. La participación de organizaciones internacionales multilaterales puede ser bienvenida. En cambio, en esta etapa no se aconseja la participación directa de las firmas proveedoras. Sí vale la pena organizar reuniones ad hoc, como seminarios, que sí pueden ser acompañados por una exposición donde los proveedores muestren sus productos.

Una vez adoptadas las normas legales correspondientes, que deben ser exhaustivas, se recomienda adoptar el sistema que ofrezca mayores seguridades al elector. Sería conveniente que fuera un sistema que utilice máquinas tipo DRE que cumplan con las garantías de seguridad establecidas en este artículo.

De acuerdo a lo estudiado, puede observarse que implantar una reforma que sólo incorpore escáner de lectura, al estilo venezolano, no es una solución recomendable. Las máquinas utilizadas en Brasil constituyen un avance notorio, pero se requiere que el código fuente sea accesible a la autoridad electoral que lo adopte. No puede comprarse un paquete cerrado.

Las máquinas no amplían la participación electoral ni la restringen. La tecnología debe usarse apropiadamente y requiere entrenamiento específico por parte de las autoridades electorales con el cambio de las pautas existentes hasta el momento. También requiere instrucción ciudadana, como ocurre en el caso del voto manual.

Para adoptar un sistema sería conveniente realizar una convocatoria a licitación que claramente establezca que no habrá soluciones «end to end» compradas «llave en mano» y que el control del proceso debe quedar en manos de la autoridad electoral.

Dado que muchas empresas desean expandir los mercados para sus máquinas y que deben enfrentar las constantes dudas acerca de los problemas de seguridad, las posibilidades de negociar un precio adecuado en un marco

de amplia competencia pueden ser muy favorables. Por consiguiente, no recomendaríamos desde ya adoptar un sistema determinado sino un proceso abierto.

REFERENCIAS BIBLIOGRÁFICAS

BRUNAZO, Amilcar. «A segurança do voto na urna eletrônica brasileira». En: *Simpósio sobre Segurança en Informática*. São Paulo: Instituto Tecnológico de Aeronáutica (ITA), Divisão de Ciência da Computação (CTA), 1999.

— «Avaliação da segurança do eleitor com a urna eletrônica». Informe presentado a la Comisión de Constitución del Senado Federal del Brasil. Brasilia: 2000.

(THE) CALTECH / MIT VOTING PROJECT. *A Preliminary Assesment of the Reliability of Existing Voting Equipment*. Boston: Massachusetts Institute of Technology (MIT), 2001.

CAMARÃO, Paulo César Bhering. *O voto informatizado: Legitimidade democrática*. São Paulo: Empresa de Artes, 1997. (El autor es Secretario de Informática del Tribunal Superior Eleitoral de Brasil.)

COMPUTER SECURITY RESOURCE CENTER / NATIONAL INFORMATION ASSURANCE PARTNERSHIP / INTERNATIONAL STANDARDS ORGANIZATION (ISO) / INTERNATIONAL ELECTRIC COMMISSION. *ISO-IEC 15.408. Common Criteria.* En: http://csrc.nist.gov/cc/ccv20/ccv2list.htm, 2000.

GATES, Bill. «Better government? Sure, in the Information Age». En: www.microsoft.com-billgates-colums-1996essay-ESSAY960710.htm, 1996. (Ensayo donde el autor argumenta en favor del voto por Internet como fuente adecuada de información acerca de los candidatos posibles, sin hacer ninguna mención a la seguridad e integridad del voto.)

JUS NAVIGANDI (página especializada en Derecho, Sección sobre informática jurídica): www.jus.com.br-pesquisa-urna.html

MERCURI, Rebecca T. *Electronic Vote Tabulation Checks & Balances*. (Tesis de Ph. D.) Filadelfia: Engineering School, University of Pennsylvania, 2000a.

— «Inside risk: voting automation (early and often?)». En: *Communication of the ACM*. Nueva York: ACM, vol. 43, Nº 11, p. 176, 2000b.

MERCURI, Rebecca T. & Peter G. NEUMANN. «System integrity revisited». En: *Inside Risk 127. Communication of the ACM*. Nueva York: ACM, vol. 44, Nº 1, enero de 2001.

PÁGINA DO VOTO ELETRÔNICO (animada por el ingeniero Amilcar Brunazo): www.votoseguro.org

PHILLIPS. Deborah M. «Are we ready for Internet voting?». En: *The Voting Integrity Project*. Arlington, Va., 1999.

— «Setting the standard for election integrity». En: *The Voting Integrity Project*. Arlington, Va., 2000.

SALTMAN, Robert G. *Issues on National Planning for the Computerized Elections*. Washington, D. C.: Brand Program on Automatic Systems, 1996.

— *Accuracy, Integrity, and Security in Computerized Vote-tailling*. Washington, D. C.: Department of Commerce, National Bureau of Standards, 1998.

TEIXEIRA, Marco Coelho. «Avaliação da necessidade de modificações na urna eletrônica brasileira». Informe presentado a la Comisión de Constitución del Senado Federal del Brasil. Brasilia: 2000.