Revista Mexicana de Análisis Político y Administración Pública
Departamento de Gestión Pública y Departamento de Estudios Políticos y de Gobierno
Volumen 1, número 2, julio-diciembre 2012
Pp. 9-21

DEMOCRACIA, ELECCIONES Y NUEVAS TECNOLOGÍAS. EL VOTO ELECTRÓNICO

Democracy, elections and new technologies. The electronic vote

María Inés Tula

Resumen
En este trabajo se analiza la inclusión de nuevas tecnologías en los procesos electorales de los últimos años, específicamente, en la aplicación del voto electrónico y se describen una serie de premisas básicas a la hora de encarar un cambio en el sistema tradicional de votación con boletas de papel.

Palabras clave: Voto electrónico-nuevas tecnologías-proceso electoral-democracia- maquinas de votación.

Abstract
This work analyzes the inclusion of new technologies in the last electoral processes, specifically, in the implementation of electronic vote. Also we describe a number of basic assumptions when facing a change in the traditional system of voting paper ballot.

Key words: electronic vote- new tecnologies- electoral process- democracy- voting machines.

La inclusión de nuevas tecnologías en el campo electoral es un proceso que ya lleva varios años de aplicación y que se encuentra, además, en constante evolución. Sin embargo, un aspecto novedoso en esta materia es el "voto electrónico" entendido de manera simple como el acto de sufragar con distintos dispositivos electrónicos tales como, una computadora, escáneres ópticos, máquinas electrónicas de votación, etc.

Es importante señalar que, más allá de la gran difusión generada por sus partidarios, el *voto electrónico* ha comenzado a utilizarse con fuerza en los últimos quince años. Se trata, entonces, de un fenómeno relativamente reciente y en constante crecimiento. Por ejemplo, respecto del voto electrónico presencial, sólo un puñado de países cuentan con un sistema de votación totalmente automatizado (los más conocidos son la India, Brasil, Venezuela y Filipinas). También una veintena de naciones han experimentado diversos arreglos de este tipo en elecciones a nivel local (Argentina, México, España, Colombia, Alemania, por poner algunos ejemplos) e incluso algunas lo han hecho con intenciones de avanzar progresivamente (Perú, Inglaterra).

Fecha de recepción: 28 de abril de 2012
Fecha de aceptación: 22 de mayo de 2012

Introducción

En lo que respecta a las experiencias llevadas a cabo con voto electrónico remoto o por internet (no presencial), también éstas han sido escasas. Estonia es el país que lleva la delantera tanto en su aplicación como en la creación de un régimen jurídico que recepcione el cambio. Si bien su puesta en marcha se debatió entre 2001-2002, en 2005 fue la primera elección y en 2007 se usó para los comicios parlamentarios. Un año después se aprobó una ley que introdujo el *mobile voting (m voting)*, es decir, el voto a través de teléfonos móviles o celulares luego de considerar que se trata del dispositivo más utilizado sin distinción social, económica, de género, etaria, racial, etc. (Caporusso, 2010). Se probó en los comicios de 2011 y sólo el 9% del electorado lo hizo bajo este sistema (Rial, 2011).

De aquí que el aprendizaje actualizado sobre experiencias comparadas internacionales y nacionales resulte vital para fortalecer las capacidades de quienes tienen a su cargo la tarea de llevar adelante procesos eleccionarios con voto electrónico. No todos los sistemas de votación electrónica funcionan de igual manera y no todas las experiencias con éstos han sido organizadas con un marco jurídico acorde a las modificaciones introducidas. De allí que, también se considere al voto electrónico como un fenómeno complejo porque sus impactos en el electorado, en los partidos políticos, en el sistema político en general no pueden ser todavía generalizados -por lo menos hasta el momento- sino contemplados a partir de la aplicación concreta que se sucede en los múltiples y heterogéneos contextos sociales.

Sin caer en la *tecnofobia* pero tampoco en la *tecnofascinación* la inclusión de nuevas tecnologías en los procesos electorales han permitido 1) superar y resolver algunos problemas importantes en la administración y organización electoral de los comicios como es el caso de Brasil y la India, países con grandes extensiones geográficas y padrones electorales que superan los cien millones de electores en el primer caso, los seiscientos millones en el segundo; 2) mantener la confianza en el sistema democrático aumentado la rapidez en el recuento de sufragios y evitando toda sospecha de parcialidad, en particular en los países con baja credibilidad en sus instituciones democráticas en los ´90 y con un aceitado mecanismo fraudulento (Brasil, Venezuela), y 3) diseñar estrategias para incentivar una mayor participación política en países con voto facultativo facilitando la votación desde distintos lugares o puestos de votación (Tula, 2011). Incluso concebir al voto electrónico remoto o por internet como un complemento (o reemplazo) del voto postal o por correo.

Así como es importante reconocer estas ventajas en la incorporación del voto electrónico en los procesos electorales, vale señalar su aspecto más cuestionado: la seguridad.

Numerosos expertos han señalado cuáles son los riesgos para la integridad y secreto del sufragio con un sistema de votación electrónico sin controles exhaustivos (Mercuri, 2001; Mercuri y Neumann, 2001; Rezende, 2004, Brunazo y Cortiz, 2006). Cobra relevancia la conocida frase atribuida a Stalin que afirma "no importa cuántos votos tienes, sino quién cuenta los votos" para reflexionar sobre la importancia de fortalecer los mecanismos de control y fiscalización en los procesos de votación. Por ello, los planteos efectuados respecto de incluir el examen, verificación y revisión de los distintos componentes del software y

hardware en las distintas etapas del proceso electoral no se debe a razones infundadas sino más bien al conocimiento de rigurosos estudios técnicos-científicos que demuestran empíricamente sus falencias.

Sumado a esto, fue determinante la difusión que tuvieron ciertas experiencias que alertaron mundialmente sobre sus debilidades, como es el caso de California en 2004 y Holanda en 2006. En el primero, después de las primarias del partido Demócrata, el fabricante de máquinas de votar Diebold fue desacreditado como proveedor tras descubrirse que los programas utilizados habían sido alterados en relación a los homologados. En el segundo, poco tiempo antes de la fecha establecida para los comicios, un grupo de ciudadanos activistas autodenominados *"We dont´t trust voting computers"* (No confiamos en las máquinas de votación) mostró en un programa de televisión la vulnerabilidad de las máquinas que admitían alteraciones en el chip de registro de los votos. La crítica situación que se estaba mostrando dejó al descubierto la facilidad con la que puede tener cualquier persona acceso a los equipos y la frágil estructura de seguridad sobre la que se organizó esta experiencia. En 2008, Holanda volvió al voto con papel (Caporusso, 2010).

Por último, el argumento jurídico que dio la Corte Federal Alemana en una sentencia del 3 de marzo de 2009 puso en el centro del debate otro aspecto hasta el momento poco estudiado o, más bien, relativizado. En efecto, la consideración de ciertos principios básicos constitucionales que toda consulta popular debe mantener. Concretamente, el fallo no se pronunció en contra de las máquinas electrónicas de votación, sino en cuestiones reglamentarias relacionadas con el poder de policía electoral y de ejecución. La Corte sostuvo que se veían afectadas las garantías del *principio de publicidad* de las elecciones, el que ordena que todos los pasos esenciales de la votación deban estar sujetos al control público, en la medida en que otros intereses constitucionales no justifiquen una excepción. El tribunal también dictaminó que los ciudadanos —sin conocimientos técnicos especiales— deben poder controlar los pasos fundamentales del acto electoral y de sus resultados. De lo contrario se debilita el carácter público de la elección, dado que el votante común no puede comprender, "sin conocimientos especiales previos" y "sin ayuda de especialistas", cómo es el proceso por el que se recibe y contabiliza su voto. Tampoco tiene garantías de que el voto emitido digitalmente sea capturado de igual modo por la máquina de votación (Pérez Corti, 2009).

La Corte Constitucional alemana afirmó que "en la República la elección es cosa de todo el pueblo y asunto comunitario de todos los ciudadanos" y que la función del proceso electoral es la "delegación del poder del Estado a la representación popular". Por ello, su legitimidad no puede ser sacrificada en función de la comodidad de funcionarios o la ansiedad de políticos por conocer los resultados (Koessl y Pérez Corti, 2009).

Como se habrá podido observar, el voto electrónico no se inserta en el vacío, sino en un complejo entramado social, político, legal y electoral. Es en este contexto donde los múltiples y sucesivos análisis multidisciplinarios que se realicen de las innumerables pruebas pilotos permitirán probar y mejorar los diferentes sistemas de votación en disímiles contextos.

Pero más allá de la evaluación que hagan los expertos respecto del modo en que se encaran los procesos de modernización tecnológica de las elecciones, de las estimaciones que

éstos realicen sobre la conveniencia de modernizar una o varias fases del proceso electoral y de las conclusiones a las que arriben sobre las ventajas y desventajas de los distintos sistemas de votación electrónica, lo cierto es que las decisiones últimas sobre estos temas están en manos de la dirigencia política. A ellos les cabe la responsabilidad de crear el contexto propicio para que el cambio sea aprovechado en toda su magnitud. Con esta intención, las líneas que siguen describen ciertas premisas básicas, necesarias a la hora de encarar una modificación en el sistema de votación.

Diez premisas básicas para su aplicación

Diseño y ejecución del software y hardware

La primera gran decisión que debe tomarse cuando se incorpora voto electrónico es la de determinar quien o quienes se ocuparán del desarrollo del software y hardware. Una opción es convocar a proveedores de soluciones informáticas especializados en temas electorales para contratar sus servicios. La otra, propiciar desde el Estado el desarrollo del software y hardware para ser aplicados a sus propias necesidades institucionales, o bien, apoyar la compra de los productos. También podría darse una combinación entre estas dos opciones, en general, la más utilizada.

Sea cual fuere la decisión adoptada la evaluación recaerá principalmente 1) sobre los costos que demandará la puesta en marcha del sistema de votación electrónica y, 2) si se optará por software libre (código abierto) o por software propietario.

Cuando se presupuesta el costo de un proceso electoral con voto electrónico, no sólo debe pensarse en el modo que se desarrollará el software y el hardware sino también en el posterior mantenimiento de las soluciones informáticas, en la capacitación y en las sucesivas prácticas que deben llevarse adelante (pruebas piloto) antes de una elección general. El sistema adoptado debe evitar la rápida obsolencia a fin de garantizar durabilidad y, además, permitir que sean "mejorables" (posibilidad de *up grade*) de modo que su costo sea más razonable (Rial, 2011).

La premisa básica para considerar a un software libre de uno que no lo es, consiste en que los usuarios están autorizados para estudiar el funcionamiento del programa o sistema, adaptarlo a sus necesidades y estar en condiciones de distribuirlo, incluso produciendo programas derivados, aunque no necesariamente la condición de libre implica gratuidad (existen condiciones para su utilización) (Romero Flores y Tellez Valdez, 2010: 37). Quienes adhieren a esta postura consideran que este procedimiento resulta mejor en la tarea de adaptación o modificación del software, arreglar fallas operativas de seguridad, y verificar su funcionamiento interno sin depender de un único proveedor. El ejemplo de Australia en los comicios de 2001 ha sido señalada como un paradigma de transparencia y un modelo a seguir (Boltz y Centeno Lappas, 2005: 306).

Control y supervisión durante el diseño y ejecución del software y hardware.

Otro de los importantes interrogantes que surge cuando se habla de voto electrónico es sobre quienes recaerá la tarea de diseñar y ejecutar el software y el hardware. Básicamente, porque el acceso ilegítimo con intenciones de manipulación no solo puede efectuarse desde afuera (*hacking* o piratería) sino también internamente, en este último caso, por personal técnico especializado con acceso privilegiado al sistema.

De allí, la necesidad de reforzar todos los mecanismos de control y supervisión con el objeto de brindar seguridad y garantizar el principio de integridad del sufragio. Cranor (1996) establece que para mantener la integridad del voto, un sistema de votación tiene que ser exacto. A diferencia de los sistemas tradicionales de votación con boletas de papel donde la normativa legal prevé la participación de observadores y fiscales partidarios para controlar el acto electoral, en los comicios con voto electrónico este procedimiento cambia radicalmente. Ni la presencia de miles de observadores, ni un ejército de fiscales partidarios es suficiente para detectar si una máquina de votación modifica los resultados. Como se preguntan Boltz y Centeno Lappas (2005: 295), ¿cómo se garantiza que el sistema funcione con exactitud cuando la observación visual no es la clave?

En este sentido, la permanencia o rotación del personal involucrado pareciera ser uno de los puntos centrales a la hora de organizar y administrar una elección con voto electrónico. Cuando la aplicación del voto electrónico es una política pública pensada a largo plazo, la actuación de estos profesionales debe corresponderse con un periodo completo de gobierno (entre cuatro y seis años, según la legislación), estableciendo un límite que no exceda más de dos procesos electorales consecutivos. De este modo, si bien se limita temporalmente al personal técnico informático-electoral en sucesivos procesos eleccionarios, existe cierta continuidad al permitírseles acompañar una misma gestión de gobierno. Se gana así en experiencia, un requisito importantísimo a la hora de evaluar la logística de cualquier proceso eleccionario. Para reforzar aún más el control de quienes están a cargo del diseño y ejecución del software electoral podría pensarse incluso en una medida preventiva para evitar la corrupción como ser la obligación de presentar declaraciones juradas publicas de sus ingresos y no permitir la existencia de cuentas bancarias amparadas por el secreto (siguiendo las normas que rigen en algunos países para los dirigentes electos por el voto popular).

Resulta entonces de suma importancia contar con un cuerpo de inspectores rotativos pero también con delegados técnicos provistos por los diversos partidos políticos y de otras organizaciones (académicas, de la sociedad civil, por ejemplo) que puedan auditar este proceso con el objeto de brindar mayores garantías electorales.

Por último, es recomendable en la organización del sistema de votación un esquema descentralizado/desconcentrado que desalienta la tentación de una manipulación a gran escala comprometiendo los resultados de todo el proceso electoral. Los sistemas que suponen un manejo fraccionado de las operaciones requieren, a su vez, de una mayor inversión en el control del diseño en tareas de coordinación y de compatibilidad.

Procedimientos para la adjudicación de software y del hardware que se usará en los comicios

Para garantizar la transparencia del proceso electoral, tanto la adjudicación del software como del hardware debiera realizarse a través de un proceso de licitaciones públicas de manera de asegurar la equidad y competencia entre las firmas que comercializan soluciones informático-electorales. Los pliegos licitatorios deben formularse de manera clara, exacta y completa y evitar innecesarias especificaciones restrictivas o requisitos excesivos que pudieran limitar el número de participantes.

Verificabilidad del correcto funcionamiento y resguardo del Código Fuente. Validación

En los casos en que se aplique voto electrónico con software propietario, éstos poseen lo que se denomina un "bloque de seguridad", es decir, la existencia de una parte que no puede ser conocida y divulgada. Si bien para algunos especialistas este hecho puede ofrecer un cierto nivel de seguridad informática al estar restringido el acceso a su código fuente ((Romero Flores y Tellez Valdez, 2010: 36); otros consideran que el código fuente debe ser propiedad de la autoridad electoral responsable, dado que tienen que estar disponibles para inspección en todo momento (incluyendo los manuales técnicos y de operación) (Rial, 2011). El hecho de no poder efectuar una auditoría total y completa del software que se empleará en los comicios deja espacio a dudas y sospechas que no debieran existir en una contienda electoral. Numerosos y reconocidos expertos coinciden al señalar que un auditor nunca podrá garantizar en un 100% la seguridad del software que ha verificado (Thompson, 1984, Neumann, 1993; Mercuri 1993). Para evitar esta situación, se recomienda la inclusión de otros reaseguros (como el uso de comprobante papel para una auditoría ex post) que garanticen así mayor confianza en el sistema.

Otra cuestión importante es saber quiénes estarán autorizados para acceder a la revisión del código fuente, ya sea total o parcial. La legislación será la encargada de definir a este "corpus de revisores" que puede constituirse con cualquier ciudadano con conocimientos técnicos, por diversas instituciones como universidades, organizaciones civiles o sólo reservar esta medida a aquellos actores que formarán parte del proceso electoral (partidos políticos, organismos de administración electoral y justicia electoral).

Lo que sí resulta importante destacar es que TODOS tienen que ser competentes e independientes. Un empadronamiento previo de estos revisores permitirá también cumplir con la máxima de "controlar a quienes controlan". Tal como lo sugiere Hernández (2011) debe considerarse la inclusión de un Código de Conducta para que respeten quienes tienen la tarea de control y el compromiso de no divulgación de los detalles del software sometido a consideración.

También la de especificar qué procedimiento se utilizará, es decir, si únicamente se autorizará un mecanismo de control del tipo "sólo lectura" o se incluirá otros procedimientos

más complejos de revisión. Respecto de los plazos en los que estos revisores pueden evaluar el software resultaría conveniente fijarlo en la normativa electoral y que sea coincidente con el inicio de la campaña electoral. En otras palabras, lo menos cercano a la fecha establecida para los comicios a fin de contemplar objeciones e impugnaciones.

¿Qué sucede si esto ocurre? Primero definir con cuanto tiempo se cuenta para la presentación de estas observaciones al código fuente y, segundo, cuál es la vía legal en caso de considerarse válida. Otra cuestión no menor a precisar es el tipo de difusión que se le dará las observaciones presentadas por los auditores, si amplia y masiva en medios de comunicación o cerrada sólo entre los actores intervinientes a través de actas u oficios.

Los especialistas sostienen que cualquiera sea la posición adoptada sobre las observaciones presentadas, estas deben contar con el respaldo de informes calificados basados en aspectos técnicos y no en valoraciones o cuestiones subjetivas (Rial, 2001). Una vez validado (vale decir, revisado en su totalidad, auditado y encriptado) el código del software no debe poder modificarse ni por el fabricante, ni sus revisores o custodios.

Etapa de inseminación de software

En la etapa conocida como "inseminación de software" se busca controlar que el software validado en la etapa anterior haya sido correctamente cargado en cada una de las máquinas de votación que se usarán el día de los comicios.

Tanto la validación como la inseminación del software representan etapas muy importantes respecto a la transparencia del comicio. Por eso, su legislación debe ser precisa y detallada, tanto o más que las normas que rigen los procesos manuales.

¿Cómo se realiza este procedimiento? Generalmente, los partidos políticos acompañados de un asesor técnico (fiscal informático) solicitan a la autoridad electoral la selección al azar de algunas máquinas electrónicas de votación con el objetivo de analizarlas.

Las máquinas electrónicas de votación, una vez cargadas, deben estar depositadas en un lugar físico controlado por la autoridad electoral y con medidas de seguridad extremas. Puede incluirse también la participación de observadores o veedores electorales previamente autorizados por la autoridad electoral competente.

La legislación deberá contemplar los plazos para efectuar esta segunda auditoría, cercana ya a la fecha prevista para el comicio general. También tendrá que determinar el modo en que se realizará a partir de una muestra aleatoria.

A diferencia de otros sistemas informáticos, como el de las auditorías bancarias, el control del voto electrónico presenta la particularidad (y la dificultad) de que su buen funcionamiento no puede verificarse después de cada votación (como sí ocurre en cada operación bancaria) porque ello implicaría violar el secreto del sufragio.

Capacitación y difusión

Uno de los puntos clave en los comicios con voto electrónico es la capacitación que deberá efectuarse en lenguaje neutro. Gran parte del éxito o fracaso de un comicio con máquinas electrónicas de votación podría adjudicarse a la correcta o incorrecta campaña de difusión y capacitación. Una amplia y extendida campaña no sólo permite que los actores que intervienen en el proceso electoral comiencen a familiarizarse con las nuevas tecnologías sino también reduce los inconvenientes a la hora de votar.

El órgano responsable de llevar adelante estas capacitaciones debe ser la autoridad electoral competente. En cuanto a su contenido, éstas no solo debieran basarse en el uso de las máquinas electrónicas de votación sino también en el nuevo lenguaje informático y en la difusión de ciertos resguardos sobre cómo garantizar la seguridad y preservar el secreto del voto. Básicamente diferenciando los cambios existentes entre el sistema de votación tradicional y el nuevo sistema electrónico.

Si el esquema de organización de las capacitaciones contempla lugares públicos tales como centros comerciales, lugares abiertos de recreación (plazas, parques) se sugiere que éstos sean difundidos como "sitios oficiales" en los que autoridad electoral sea la única responsable de los contenidos que se imparten en esa capacitación y el modo en que se instruye a los ciudadanos.

La difusión sobre el nuevo procedimiento de votación debe considerar tanto los medios masivos de comunicación como prácticas de "sensibilización" en lugares públicos con un cronograma detallado de sus actividades y con folletos explicativos que describan el "paso a paso" de su uso. Las propuestas interactivas (diseñadas por la autoridad electoral) para practicar desde un ordenador personal también resulta un buen mecanismo de divulgación.

No se recomienda la capacitación el mismo día de los comicios. Esta objeción se funda en dos razones: por un lado, el hecho de no interferir en la organización y desarrollo del acto electoral y, por el otro, porque debe evitarse toda situación sospechosa que hiciera pensar que estas capacitaciones influyan sobre la decisión de los votantes ese día. Particularmente cuando se realizan con candidatos reales y no con personajes ficticios. La normativa electoral debería contemplar una veda de entre 48 a 72hs.

¿Son necesarios los asistentes informáticos? Se entiende por "asistentes informáticos" a aquellos individuos cuyo papel es ayudar al elector en caso de dudas sobre el manejo de las máquinas electrónicas. Este personal de apoyo no necesariamente cuenta con los conocimientos técnicos necesarios para solucionar algún problema que se suscite, su tarea se limita a facilitar el acto de votar a los ciudadanos y permitir un mejor desempeño de las autoridades de mesa en la recepción de los votantes y su identificación. No son capacitadores, sino que guían al votante en caso de dudas. Su lenguaje también debe ser neutro y debe mantener una distancia prudencial a fin de evitar la pérdida del secreto del sufragio. Su selección también debe ser tarea del órgano electoral competente, previa inscripción en un registro.

Las máquinas electrónicas de votación

No todas las máquinas electrónicas de votación que se han usado en diversas experiencias en el mundo tienen iguales características. Tampoco el modo en que estas máquinas se han insertado en un contexto de elección general. A grandes rasgos diferenciándose por la forma en que se ha desarrollado y ejecutado el software y hardware, por el tipo de legislación que ha acompañado la experiencia y por el procedimiento adoptado para su introducción, ya sea como una política pública considerada a largo plazo de carácter nacional (como es el caso de Brasil) o, por el contrario, como la práctica de varias experiencias heterogéneas en el ámbito provincial y municipal (como es el caso de Argentina). De allí que resulte importante el análisis de los formatos de estas máquinas electrónicas de votación porque su diseño y configuración son determinantes para el cumplimiento de los principios de universalidad y de secreto del voto.

Una de las críticas más importantes en el uso del voto electrónico es cuando el padrón electoral digitalizado está incluido en la misma máquina que se usa para votar. El riesgo que se corre cuando ambos se emplean juntos es la posibilidad de vincular a los electores con el sufragio emitido. El solo hecho de conocerse esta posibilidad (tanto la de quebrar el anonimato como la tentación a hacerlo) resulta un riesgo muy alto para mantener la confianza en el sistema. Por lo tanto, se sugiere mantenerlos separados.

Existe cierto consenso general en que las máquinas electrónicas de votación deben poseer las siguientes características: no incluir componentes abiertos, poder ser auditables en todas las etapas del proceso electoral (antes, durante y después de la jornada electoral) y contar con soporte papel o comprobante físico del voto. Este comprobante en formato papel representa, además, un reaseguro del principio de integridad del voto. Permite en un cotejo posterior a la elección comparar los resultados electorales digitales (arrojados por el conteo de la máquina) con los resultados electorales impresos (confirmados por el elector). Se sugiere que la autoridad electoral sea la encargada de organizar una auditoría final (ex post) seleccionando -a partir de una muestra diseñada a tal efecto- máquinas para controlar y cotejar ambos sufragios (virtual e impreso). La legislación debe prever este procedimiento antes de proclamar a sus candidatos. Frente al interrogante de cuál de los dos sufragios debiera primar si llegaran a encontrarse diferencias entre ambos tipos de votos, se deben considerar como validos los votos impresos porque éstos no sólo son aquellos que el elector vio y confirmó sino también los que tienen menos posibilidades de haber sufrido una manipulación intencional (a través del software).

Por otro lado, las máquinas de votación tienen que ofrecer alternativas para quienes poseen capacidades diferentes de manera tal de no negarles el derecho al voto a través de sistema braille, alguna marcación táctil que les permita identificar las teclas (como en los teléfonos fijos y celulares con la tecla número 5), dispositivos tipo *call center* que guíen al votante durante todo el proceso, etc.

Requisitos para la transmisión de resultados

Cuando el envío de los resultados electorales no se produce por la vía tradicional (manual, terrestre) debe considerarse la inclusión de canales de comunicación seguros y el órgano receptor de los resultados electorales (centro de cómputos) debe verificar la integridad y autenticidad de los datos recibidos antes de procesarlos. Los resultados electorales deben estar encriptados y firmados digitalmente (Hernández, 2011).

Del mismo modo, la necesidad de contar con una línea especial para la transmisión de los resultados y la prohibición de los componentes de comunicación en las maquinas de votar. De la transmisión de resultados deberán participar los fiscales partidarios y la autoridad electoral competente. Para garantizar la transparencia del proceso otras instituciones podrían actuar como veedores.

Logística de organización. Máquinas de reserva. Plan de contingencia

En los lugares donde se han efectuado experiencias con distintas modalidades de voto electrónico se mantienen en reserva algunas máquinas por si llegaran a fallar las que se están usando en los comicios. Por lo general, si el problema técnico no logra resolverse, debe haber un protocolo de acción que indique cuál es el proceso a seguir para el cambio del equipo (sobre todo si se trata de máquinas que almacenan votos).

Es desaconsejable el acceso a técnicos, aun habiendo sido acreditados por la autoridad electoral, sin la presencia de fiscales técnicos partidarios. Esta restricción tiene por objeto garantizar la seguridad del comicio, al igual que en el sistema tradicional de votación, donde la autoridad de mesa y los fiscales partidarios son los responsables de "custodiar" a las urnas mientras dure el acto electoral.

Sobre este punto, las normas que contemplen la adopción del voto electrónico deben ser claras y precisas. En particular cuando se refieren a las circunstancias extremas en que el presidente de mesa autorice al personal técnico a reparar el equipo o reponer por otro. Cada participación debiera ser registrada en un acta a fin de evaluar posteriormente los motivos de la falla.

Los fiscales informáticos y los fiscales partidarios

El uso de máquinas electrónicas de votación requiere de personal con conocimientos en tecnología pero también con una vasta experiencia en materia electoral. Con el sistema tradicional de votación, la participación de los fiscales informáticos se limitaba a la última fase del proceso electoral, en la transmisión de resultados.

Con el cambio de los sistemas de votación, el "fiscal informático" tiene una participación mayor dado que su actuación debe incluirse en las tres fases del proceso electoral (antes, durante y después). Puede entonces asumir como auditor, perito o veedor de de los diferentes procesos electorales. Valiéndose de técnicas de las ciencias forenses, la recolección y

preservación de evidencia es una tarea más que el fiscal informático debe conocer (Hernández, 2011).

No debe olvidarse que una elección supone una contienda entre varios aspirantes. Y que la confianza en sus resultados y, por ende, la aceptación de ganar o perder impacta sobre sus instituciones. Los partidos políticos deben tener presencia en todas las fases del proceso electoral pero muy especialmente durante el día de votación.

A modo de conclusión

La aplicación del voto electrónico no sólo supone la incorporación de máquinas electrónicas el día de los comicios sino, más bien, se trata de un profundo y gran cambio con impactos diferenciados en el orden social, jurídico y político. Una misma máquina de votación puede producir efectos distintos según el modo en que ésta haya sido insertada en dos países diferentes, o incluso impactar de modo opuesto en un mismo país pero en períodos temporales distintos. Por lo tanto, no se trata de buscar la aplicación tecnológica bajo el argumento de "el mundo va en esa dirección" sino de efectuar estudios que indaguen sobre cuáles son los beneficios reales que aportaría el cambio.

Los ejemplos de la India, Brasil y Venezuela resultan ilustrativos. Estos países encararon el cambio en sus sistemas de votación de manera gradual pero, aún con sus críticas, el voto electrónico logró aumentar la confianza en sus instituciones democráticas a través del mejoramiento en la administración y organización electoral. Pero a diferencia de lo que ocurre en otros países que ensayaron experiencias con voto electrónico, estas naciones conocían cuáles eran sus falencias. Cuando el diagnóstico sobre el cual se asienta el pedido de cambio en el sistema de votación no es claro, la introducción del voto electrónico "se contamina". Se desdibujan sus potenciales beneficios y aumentan las sospechas sobre negociados con empresas proveedoras de servicios y crecen los temores infundados a una gran manipulación electoral.

Por ello resulta decisivo no sólo una evaluación de cómo impactaría un proceso gradual de transición sino también en ser prudentes en sus expectativas. No debe "venderse" su aplicación afirmando de modo tajante que terminará con ciertos problemas patológicos de nuestra cultura política, tales como el clientelismo o la compra y venta de votos. A lo sumo permitirá atenuar algunas maniobras fraudulentas vigentes en los países con estos conflictos pero también, se deberá estar muy atento a la aparición de nuevos problemas. Como bien afirmaba Passalacqua (2005) "no existen las soluciones tecnológicas a los problemas políticos", la persistencia de los viejos "males" sumado a algunas "nuevas" contrariedades solo acentuará el rechazo de la ciudadanía a esta nueva forma de votación.

El uso de la tecnología a través de computadores y redes sociales es cada vez mayor. No obstante frente a este crecimiento debe tenerse presente que la introducción de voto electrónico requiere de una fuerte inversión en capacitación, al menos, en los primeros años de su puesta en marcha. Y de innumerables pruebas que sirvan como "ensayo y error", primero

en territorios acotados para luego ir avanzando progresivamente. Las evaluaciones de estas experiencias permitirán ir ajustando la logística y acomodando la legislación.

Por último, pero no por ello un tema menor, la introducción del voto electrónico es una decisión eminentemente política que debe ir acompañada por el consenso político y social. Por ello, a la dirigencia política le cabe la responsabilidad de no caer en el "idolatría informática" o de recurrir al voto electrónico sólo como una forma de "maquillaje" para que, en el fondo, todo el proceso electoral siga exhibiendo los mismos defectos que se pretendían eliminar.

Bibliografía

Boltz, Ingo y Centeno Lappas, Federico. 2005. "Riesgos y debilidades del voto electrónico: en busca de transparencia, seguridad y confianza en el proceso electoral", en María Inés Tula (Ed.), *Voto Electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales*, Buenos Aires, Ariel, pp. 287-314.

Brunazo, Amilcar y Maria Aparecida Cortiz. 2006. *Fraudes e Defesas no Voto Eletrônico,* San Pablo, All Print Editora.

Caporusso, Letizia. 2010. *Il voto elettronico come processo sociale* Tesis de Doctorado. Universidad de Trento.

Cranor, Lorrie. 1996. *Electronic Voting, computerized polls may save money, protect privacy*, en http://www.acm.org [Consultado en febrero de 2005]

Hernández, Héctor. 2011. *Fiscalización Informática del Voto Electrónico. Guía para la actuación profesional*. Argentina. Tinta Libre Ediciones.

Koesll, Manfred. 2010. Traducción Fallo de la Corte Constitucional Alemana. Sentencia 2BvC 4/07-Inconstitucionalidad del e-vote, en http://www.te.gob.mx/documentacion/publicaciones/Justicia_electoral/juel_a6_n2_1.pdf [Consultado en abril 2012].

Mercuri, Rebecca. 1993. The Business of Elections, en http://www.notablesoftware.com [Consultado en marzo de 2005]

Mercuri, Rebecca. 2001. *Rebecca Mercuri´s Statement on Electronic Voting*, en http://www.notablesoftware.com [Consultado en marzo de 2005]

Mercuri, Rebecca y Neumann, Peter. 2001. *System Integrity Revisited,* en http://www.csl.sri.com/users/neumann/insiderisks.html#127 [Consultado en marzo de 2005]

Neumann, Peter. 1993. *Security Criteria for Electronic Voting*, en http://www.csl.sri.com [Consultado en marzo de 2005]

Passalacqua, Eduardo. 2005. "El voto electronica. Ni panacea ni amenaza. Panorámica del estado de la cuestión y apostillas a un debate con sesgos y lagunas", en María Inés

Tula, (Ed.), *Voto Electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales*, Buenos Aires, Ariel, pp. 63-99.

Pérez Corti, José María. 2010. *Los principios generales del derecho electoral y su gravitación en la inconstitucionalidad del régimen alemán de voto electrónico,* en http://www.te.gob.mx/documentacion/publicaciones/Justicia_electoral/juel_a6_n2_1.pdf [Consultado en abril 2012]

Rezende, Pedro. 2004. *Electronic Voting Systems: Is Brazil ahead of its time?* en http://www.cic.unb.br [Consultado en marzo de 2005]

Rial, Juan. 2011. *El voto electrónico en América Latina. Consideraciones sobre su implementación*. Argentina , mimeo.

Romero Flores, Rodolfo y Téllez Valdez, Julio. 2010. *Voto Electrónico, Derecho y otras implicaciones*. México. Universidad Nacional Autónoma de México.

Thompson, Ken. 1984. *Reflection on trusting trust*. en http://www.acm.org [Consultado en febrero de 2005]

Tula, María Inés, "Las experiencias con voto electrónico en los procesos electorales recientes. El caso de Argentina", en Nicolás Loza (Ed.), *Voto Electrónico y democracia directa. Los nuevos rostros de la política en América Latina*. México, Flacso México/ Tribunal Electoral del Poder Judicial de la Federación.

María Inés Tula

Argentina. Politóloga y Doctora en Derecho por la Universidad de Buenos Aires. Actualmente se desempeña como profesora en la Carrera de Ciencia Política de la Universidad de Buenos Aires e Investigadora del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET). Ha publicado numerosos artículos sobre elecciones, sistemas electorales y partidos políticos en revistas científicas nacionales e internacionales. Como Directora del Programa de Instituciones Políticas del Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC) entre 2004-2007 participó como observadora de varias experiencias argentinas con voto electrónico, coordinó el libro Voto electrónico (Ariel-CIPPEC, 2005) y ganó el Primer Premio Provincial 2006 a la Innovación en la Gestión Pública por el Proyecto de reglamentación de la aplicación del voto electrónico en la provincia de Buenos Aires, otorgado por la Subsecretaria de la Gestión Pública, Secretaria General de la Gobernación de la Provincia de Buenos Aires, Argentina. En los últimos años, también ha editado los siguientes libros: *Aportes para la reforma política bonaerense (2005), y, Mujeres y política en América Latina. Sistemas electorales y cuotas de género* (2008).