CIPPEC
Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento

Políticas Públicas Análisis *N° 31*

Instituciones Políticas

Octubre 2006

Aportes para una aplicación eficaz del voto electrónico

Por María Inés Tula

El voto electrónico es una herramienta que se extiende cada vez más en nuestro país tanto para elecciones generales como para consultas populares vinculantes o no. Sin embargo, llama la atención que frente a este progresivo avance en la incorporación de nuevas tecnologías exista todavía un vacío normativo sobre qué y cómo regular su aplicación en los procesos electorales.

El objetivo de este trabajo es doble. Por un lado, describir qué es el voto electrónico para saber de qué se habla cuando se menciona una reforma política que lo incluya y, por el otro, avanzar en la elaboración de algunos principios generales que debieran ser evaluados a la hora de aprobar un sistema de votación con estas características.

I- Introducción[*]

Desde la primera experiencia efectuada en la Argentina en septiembre de 2003, el Programa de Instituciones Políticas de CIPPEC participó en la mayoría de las pruebas piloto que se llevaron adelante en el país y donde se pusieron a prueba los distintos mecanismos de votación electrónica para elecciones y variadas consultas populares. Desde elecciones a cargos públicos representativos, comicios estudiantiles universitarios, simulaciones de actos electorales hasta consultas populares efectuadas con diversos fines (como, por ejemplo, la instalación de casinos en un municipio de la provincia de Misiones o la autonomía de Quequén y Huanguelén en la provincia de Buenos Aires, entre otros).

Sobre la base de estas experiencias y de las observaciones relevadas por CIPPEC, se decidió conformar un "Consejo Asesor" con expertos nacionales e internacionales. El objetivo de esta convocatoria fue aprovechar el conocimiento de los integrantes de este Consejo y su vasta experiencia en el tema para recoger sus opiniones en un documento que sintetizara ciertos principios o requisitos mínimos que debieran guiar un proceso electoral con voto electrónico (Ver los integrantes al final de este documento).

Para ello, CIPPEC elaboró dos cuestionarios que se enviaron por correo electrónico entre julio y diciembre de 2005 con preguntas cerradas y abiertas agrupadas en tres secciones[1]. El

[*]Ursula Eyherabide participó de este trabajo en la etapa de envío y recepción de los cuestionarios, así como en la sistematización de las respuestas. Pablo Lozada Castro colaboró con la organización de la base de datos de las entrevistas.

[1]Estos cuestionarios presentan una limitación, y es que resulta difícil –cuando no imposible- definir normas cuando no se sabe cuál será el sistema de voto electrónico que finalmente se empleará en los comicios. Más allá de esta importante restricción, la idea de este trabajo consiste en elaborar algunos requisitos que consideramos ineludibles a la hora

cuestionario se dividió en tres partes por la necesidad de esquematizar las preguntas referidas a la incorporación del voto electrónico según las fases en las que puede dividirse el proceso electoral: 1) *antes* de la jornada electoral o etapa previa preparatoria, 2) *durante* la jornada electoral o el día de los comicios propiamente dicho, y 3) *después* o la etapa posterior a los comicios, que abarca los escrutinios parcial y total junto con la difusión de los resultados electorales y la nueva distribución institucional del poder.

Cada una de estas secciones se armó con interrogantes sobre qué elementos nuevos, hasta ahora no presentes en la elección tradicional con boletas partidarias de papel debieran instrumentarse para lograr un mayor control de los comicios y, a su vez, elecciones más transparentes.

En esta dirección, el presente documento busca a) promover la confianza en el sistema electrónico de votación a través de la divulgación y/o difusión de su uso, b) asegurar el cumplimiento de los procesos de fiscalización adecuados para brindar mayor control y seguridad en los comicios, y c) garantizar la universalidad, el secreto del sufragio y la integridad del voto[2].

Para una mejor comprensión del tema, este trabajo se divide en dos partes. La primera responde sintéticamente a la pregunta "¿qué es el voto electrónico?" y la segunda presenta los resultados del cuestionario organizados según los aspectos considerados prioritarios en una elección donde se aplique este sistema de votación. Por último, se incluye un glosario con los términos técnicos utilizados.

II- ¿Qué es el Voto electrónico?

En un sentido amplio, el término *voto electrónico* se utiliza para hacer referencia a las distintas tecnologías de la información empleadas en las diferentes fases del proceso electoral. Tales como el registro de los ciudadanos, la confección de mapas de los distritos electorales, la gerencia, administración y logística electoral, el ejercicio del voto, los escrutinios, la transmisión de los resultados y su certificación oficial.

En cambio, en sentido estricto, la expresión *voto electrónico* remite únicamente al uso de ciertas tecnologías en el acto de votar o en el momento de "contar los votos" (Rial, 2005).

Es decir, se trata de un cambio en las formas tradicionales de votación que puede involucrar a todo el proceso electoral o sólo algunas fases relacionadas con el acto de votar con "máquinas" o "urnas electrónicas" el día de los comicios[3].

Algunas de las preguntas que generalmente se formulan cuando se habla de voto electrónico son: ¿en qué países se usa y por qué? y ¿qué ventajas y desventajas tiene su aplicación? Si bien el riesgo de generalizar es alto, porque no todos los prototipos de máquinas de votación funcionan de igual manera, a grandes rasgos puede señalarse que las ventajas del voto electrónico se asocian con los problemas o dificultades que se intentan solucionar con su aplicación.

En primer lugar, la necesidad de contar con resultados electorales rápidos, ya que la velocidad es una ventaja cuando el desconcierto generado por la demora de los resultados electorales se

de aprobar una legislación que incorpore nuevas tecnologías en el proceso electoral.

[2]Las afirmaciones aquí vertidas son exclusiva responsabilidad de la autora que firma este documento y no de los entrevistados que participaron del Consejo Asesor. A todos ellos se agradece su valiosa colaboración y la buena predisposición al aceptar participar de esta ronda de consultas.

[3]No es objetivo de este trabajo detallar las diferentes modalidades de voto electrónico. Para profundizar sobre ese tema, se recomienda la lectura del libro que editó CIPPEC y coordinó Tula (2005).

vincula con el fraude y la manipulación de los comicios. En este aspecto, el descreimiento y la desconfianza de las elecciones en algunos países de América Latina tendieron a promover reformas político electorales que profundizaran cambios, tanto en la organización como en la administración de los comicios.

Segundo, fomentar la participación política de los ciudadanos en los países que no tienen votación obligatoria. En Europa, una de las principales preocupaciones radica en combatir las altas tasas de abstención electoral. Es por ello que en estos países se efectúan numerosas pruebas piloto con el objetivo de facilitar el voto de sus electores a través de la tecnología como, por ejemplo, a través de internet y desde cualquier punto del país sin necesidad de trasladarse a una mesa de votación específica.

Tercero, el voto electrónico también es considerado una herramienta útil para la administración de los comicios, es decir, se lo relaciona con la posibilidad de hacer más eficaz la organización electoral. Por ejemplo, si se piensa en los casos de Brasil y la India, dos de los tres **únicos** países que introdujeron a nivel nacional máquinas electrónicas de votación, se observa que en ambas naciones los padrones electorales superan los cien millones de electores[4].

¿Cuáles son las críticas más comunes al voto electrónico? El aspecto más cuestionado es aquel que se refiere a las garantías de seguridad. Sólo con un control exhaustivo del diseño del hardware y software, y con mecanismos de auditoría previos y posteriores a las elecciones se estaría en condiciones de disminuir –aunque no de eliminar- una eventual manipulación electoral.

La fiscalización durante todo el proceso electoral efectuada por los partidos políticos y el atento monitoreo de las organizaciones civiles, por ejemplo, resulta clave en este punto. La complejidad que adquiere este procedimiento de control requiere de la especialización de sus observadores, que deben ser eficazmente capacitados para detectar fallas, errores o manipulaciones y efectuar los reclamos correspondientes ante el organismo electoral competente.

III- Análisis las entrevistas

En esta sección se presentan algunos aspectos clave que debieran tenerse presente a la hora de organizar un comicio con voto electrónico. Si bien algunas opiniones resultan muy variadas, creemos que esta heterogeneidad aporta una visión más general sobre cómo encarar la adopción de nuevas tecnologías desde el punto de vista normativo y desde la organización electoral[5].

-Organismos autorizados para desarrollar el software y el hardware.

Mientras la mayoría expresa que tanto el software como el hardware podrían ser desarrollados por los propios gobiernos u órganos dependientes del Estado, otros consideran que al requerir el hardware de una gran inversión y de una producción de gran escala, ésta no resultaría conveniente para los gobiernos. En cambio, la decisión sobre el desarrollo del software sería más flexible dado que podría ser producido totalmente por el Gobierno, o bien, éste podría adquirir

[4]El tercero es Venezuela, con once millones de electores. Los motivos por los cuales Venezuela incorporó el voto electrónico, se asocian más al primer aspecto mencionado que al último. El caso de los Estados Unidos es diferente. La organización de las elecciones no es responsabilidad del gobierno federal sino de cada Estado, y dentro de cada uno de ellos, estas tareas pueden ser llevadas adelante por los Condados. En consecuencia, cada Estado puede tener diferentes formas de votación en cada uno de sus Condados.

[5]Esta diversidad de opiniones se debe también a que algunos autores responden según la propia experiencia en su lugar de residencia y con diferentes modalidades de voto electrónico.

uno y adaptarlo a las precisiones de cada lugar.

Sea cual fuere la opción aceptada, los especialistas enfatizan la necesidad de mantener un estricto control de todo este proceso por parte de la autoridad electoral.

Ahora bien, para el caso puntual de que el software fuera desarrollado por una empresa privada, algunos de los entrevistados consideran que ésta debiera ceder los derechos de propiedad. No se ponen de acuerdo sobre qué y cuántos organismos estarían autorizados para compartir esta propiedad. Así, mientras unos consideran que *sólo* debiera ser el órgano encargado de la administración electoral, otros incluyen al Gobierno dentro de este grupo. Sin embargo, esta última postura es la que más objeciones ha presentado entre los expertos dado que sostienen que para brindar mayores garantías electorales de equidad y competencia, el Gobierno tendría que mantenerse prescindente, precisamente, porque es parte integrante del juego político.

Por otra parte, están quienes adhieren al *software libre* porque consideran que este procedimiento resulta mejor en la tarea de adaptación o modificación del software, arreglar fallas operativas o de seguridad, y verificar su funcionamiento interno sin depender de un único proveedor.

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

Los expertos coinciden en señalar que para garantizar la transparencia del proceso electoral, la adjudicación del software y del hardware debiera realizarse a través de un proceso de licitaciones públicas de manera de asegurar la equidad y competencia entre las empresas que se presentan. Los pliegos deben formularse de manera clara, exacta y completa y evitar innecesarias especificaciones restrictivas o requisitos excesivos que pudieran limitar el número de licitantes.

- Aspectos vinculados con el Código Fuente

En algunos lugares, los programas de las urnas electrónicas poseen lo que se denomina un "bloque de seguridad", es decir, la existencia de una parte que no puede ser conocida y divulgada. Para algunos expertos, este aspecto es sumamente criticable dado que apoyándose en la seguridad, los procesos de auditoría y fiscalización nunca pueden ser del todo completos. Si bien la estrategia de limitar su observación se efectúa con el objetivo de evitar ciertas manipulaciones, deja espacio a dudas y sospechas que no debieran existir en una contienda electoral.

Otra cuestión importante es saber quiénes debieran estar autorizados para acceder al código fuente, ya sea totalmente o sólo revisando una parte. Ante este interrogante, los entrevistados presentaron diversos fundamentos según el grado de apertura o restricción en la participación de los distintos actores que podrían intervenir en este procedimiento.

Un primer grupo sostuvo que cualquier ciudadano podría tener el derecho de analizarlo de modo de controlar la transparencia del proceso electoral (con la salvedad de que durante su desarrollo, esta modalidad fuera cerrada).

Una posición intermedia adhiere a la postura de que sólo algunos actores estarían habilitados a participar de esta instancia de auditoría. Las instituciones autorizadas podrían ser los partidos políticos, las universidades, la Justicia Electoral, el Ministerio del Interior y las organizaciones de la sociedad civil.

En última instancia, la posición más restrictiva considera que sólo la Justicia Electoral y los partidos políticos debieran tener acceso al código fuente.

Por otra parte, tampoco resulta homogénea la postura sobre el modo en que este procedimiento debiera regularse,

es decir, si únicamente autorizar un mecanismo de control "de sólo lectura" o incluir otros procedimientos más complejos.

-Presentación de observaciones al código fuente ante el organismo electoral competente.

Una vez finalizada la etapa de análisis y control del código fuente (que la norma o reglamentación debe detallar con precisión) los interrogantes que surgen se vinculan con cómo debieran receptarse las observaciones efectuadas por los actores autorizados, una vez vencido el plazo para estas presentaciones. Existen dos posiciones diferentes. Por un lado, quienes consideran que las objeciones debieran difundirse masivamente a través de los medios de comunicación y, por el otro, los que avalan una postura más restringida a través de canales formales y únicamente entre los actores interesados. En este último caso, la difusión se efectuaría por medio de actas, oficios o por Internet en algún sitio del organismo electoral competente.

Así, mientras que para algunos la difusión masiva es un signo de transparencia, para otros podría acarrear un gran problema. En este caso, las restricciones que se impondrían a la difusión de las objeciones presentadas al código fuente buscarían preservar una mayor seguridad y evitar la tentación de *hackers* de vulnerar los contenidos de los programas de software.

Los especialistas sostienen que cualquiera sea la posición adoptada sobre las observaciones presentadas, éstas deben contar con el respaldo de informes calificados basados en aspectos técnicos y no en valoraciones o cuestiones subjetivas.

¿Quiénes pueden presentar objeciones? Para algunos, sólo los partidos políticos dado que la finalidad de estas observaciones es la solución o corrección de los problemas que son, precisamente, el objeto del reclamo. La Justicia Electoral, debiera ser el órgano que arbitrara los procedimientos de inmediata verificación y respuesta a todas estas observaciones. Otros expertos, más permisivos, incluyen a las universidades y a las organizaciones de la sociedad civil y, en menor medida, aceptan la participación de los medios de comunicación.

-Personal afectado al diseño y ejecución del hardware y software.

Uno de los grandes interrogantes que surge cuando se habla de voto electrónico es sobre quiénes recaerá la tarea de diseñar y ejecutar el software y el hardware. Básicamente, porque el acceso ilegítimo con intenciones de manipulación no sólo puede efectuarse desde afuera (*hacking*) sino también desde adentro, por personal técnico con acceso privilegiado al sistema (*insiders*).

En este sentido, la permanencia o rotación del personal involucrado pareciera ser uno de los puntos centrales a la hora de organizar una elección con voto electrónico.

Mientras que para algunos la rotación es fundamental para brindar mayor seguridad al proceso electoral, para otros alcanza con exigir ciertos recaudos de seguridad y confidencialidad.

Los entrevistados destacan que, gran parte del cuidado y control que tiene que prestarse en esta instancia del proceso electoral, depende de si los que están a cargo del diseño del software y hardware son empresas privadas que pasaron o no por un proceso de licitación pública, o bien, se trata de algún organismo de la administración electoral.

Así, para los que consideran que debe haber rotación de personal, la actuación de estos profesionales debe corresponderse con un período completo de gobierno, incluso estableciendo un límite que no exceda más de dos procesos electorales consecutivos.

Desde este punto de vista, es de suma importancia tener un cuerpo de inspectores rotativos y de delegados técnicos provistos por los diversos partidos políticos y de otras organizaciones que puedan auditar este proceso con el objeto de brindar mayores garantías electorales. Los especialistas que adhieren a esta postura sostienen también que una medida preventiva para evitar la corrupción del personal que trabaja en el desarrollo del software debiera ser la obligación de presentar declaraciones juradas públicas 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).

Por el contrario, los que consideran que no es necesaria la rotación de personal técnico focalizan su atención en brindar continuidad y experiencia en el tratamiento del tema. Sostienen que si la estructura operativa y el software contemplan mecanismos de seguridad robustos y han sido debidamente auditados por la autoridad electoral competente, no debiera perderse "personal capacitado y con experiencia previa", un requisito importantísimo para la logística de cualquier proceso eleccionario.

Con el fin de evitar situaciones poco claras, resulta imprescindible definir políticas precisas que permitan resolver y distinguir las evidencias de fraude, de los que son errores y de los problemas técnicos.

- Etapa de validación del software.

A través del procedimiento de validación del software, que generalmente se efectúa en un acto público, se comprueba y verifica que el software no presente fallas y alteraciones. Este acto representa una garantía de transparencia electoral, ya que participan de esta instancia tanto las autoridades electorales como los responsables informáticos de cada partido político y otros miembros autorizados como las universidades y organizaciones de la sociedad civil que acompañan en el monitoreo del proceso eleccionario.

Para que la validación del software tenga lugar debe preverse en la legislación un plazo flexible para que la auditoría se efectúe con cierto tiempo de anticipación. Para algunos especialistas, el plazo para el análisis del software depende de la extensión que éste tenga, llegando en algunos casos a resultar imposible su completo diagnóstico aún previendo varios meses de trabajo. Para otros, depende también de si se autoriza el análisis completo o sólo parcial del software que se usará en los comicios.

Por estas razones, los especialistas consultados no acuerdan sobre los plazos que debe establecer la legislación electoral para evaluar el software. Mientras algunos consideran que la auditoría debiera comenzar antes del comienzo de la campaña electoral (entre seis meses y un año antes de la fecha estimada para los comicios), otros sostienen que con 60 ó 90 días antes de las elecciones es suficiente.

- Etapa de inseminación del software.

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

¿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 urnas electrónicas con el objetivo de analizarlas.

Las urnas, una vez cargadas, deben estar depositadas en un lugar físico controlado por la autoridad electoral y con medidas de seguridad extremas.

Algunos especialistas incluyen también en este procedimiento a las universidades y miembros de la sociedad civil como veedores electorales.

Con respecto a los plazos para efectuar esta segunda auditoría, los entrevistados no acuerdan un límite temporal único. Mientras algunos sostienen que debiera autorizarse el control hasta un día antes de los comicios, otros destacan la necesidad de tener una mayor organización poniendo como límite una semana antes de la fecha estipulada para las elecciones, y proponiendo que el día previo a la jornada de votación se realice una muestra aleatoria para confirmar nuevamente el resultado.

En base a la experiencia desarrollada en otros países, uno de los entrevistados afirma que no sirve auditar las urnas un día antes del comicio. Según su entender, éstas deben auditarse nuevamente *durante* la jornada electoral escogiendo urnas al azar de cualquiera de los centros de votación y llevándolas al centro de cómputos (Test de votación paralelo). Allí, los fiscales informáticos de cada partido político podrían comprobar que realmente el mismo software que fue lacrado en el procedimiento de validación se encuentra en esas urnas electrónicas seleccionadas.

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 con cada operación bancaria) porque ello implicaría violar el secreto del sufragio.

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.

-Capacitación y difusión sobre cómo votar con nuevas tecnologías.

Uno de los puntos clave en los comicios con voto electrónico es la capacitación que debe efectuarse a las autoridades electorales, personal afectado a la organización de los comicios, partidos políticos y ciudadanos en general. Gran parte del éxito o fracaso de un comicio con urnas electrónicas 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.

Todos los entrevistados coinciden en señalar que el órgano responsable de llevar a adelante las capacitaciones debiera ser la autoridad electoral competente. También podrían encargarse de la difusión y campaña de capacitación otras instituciones, tales como universidades u organizaciones civiles, siempre y cuando éstas se encuentren autorizadas por el organismo electoral pertinente.

En cuanto al contenido de estas capacitaciones, los expertos señalan que no sólo debiera basarse en el uso de las urnas electrónicas sino también en el nuevo lenguaje informático y 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.

¿Cuál es el tiempo necesario para llevar a cabo con éxito esta campaña de difusión y capacitación antes de los comicios? Cuando se trata de reglamentar una norma electoral es preciso fijar un límite temporal y plazos bien definidos de comienzo y fin de esta tarea. Los entrevistados consideran que si se trata de la primera vez que se realizan comicios con voto electrónico el tiempo para las capacitaciones debiera ser más amplio (entre 60 y 90 días) que si se usa

tecnología por segunda vez (30 y 45 días). En este último caso, dándose por supuesto que las urnas empleadas son siempre las mismas.

No hay acuerdo sobre cuándo debiera terminarse esta campaña de capacitación. Mientras que para algunos, tendría que efectuarse hasta siete días previos a la jornada electoral, para otros podría realizarse el mismo día de los comicios. Esta última opción presenta ciertas objeciones fundadas en dos razones: por un lado, no interferir en la organización del acto electoral con personal dedicado a la difusión y capacitación y, por el otro lado, porque debe evitarse que estas capacitaciones pudieran inducir sobre el votante sobre todo teniendo en cuenta que muchas capacitaciones se realizan con opciones reales y no ficticias. Pero aun tratándose de opciones no reales, la autoridad electoral tendría una tarea más: la de controlar que en cada centro de votación se estén usando correctamente softwares de simulación de comicios con personajes ficticios.

Frente a esta situación, algunos entrevistados señalaron que la normativa debería contemplar una veda electoral de entre 48 y 72 horas, con el objetivo de evitar que la instrucción pueda influenciar sobre los electores, reservando ese día para la reflexión electoral propiamente dicha.

Por último, la difusión sobre el nuevo procedimiento de votación tiene que efectuarse a través de los medios masivos de comunicación, en prácticas de "sensibilización" en lugares públicos con un cronograma de actividades detallado de dónde se podrá practicar el modo de sufragar (como shoppings, escuelas, plazas, etcétera) y con folletos explicativos que describan el "paso a paso" de su uso.

-Padrón electoral y software de votación.

Una de las críticas más comunes cuando se utiliza el padrón electoral digitalizado es la que advierte sobre la inclusión en un mismo dispositivo del padrón electoral y el software de votación. Según los expertos, el riesgo que se corre cuando ambos se emplean juntos es la posibilidad de vincular al elector con su sufragio, vulnerándose de este modo, el secreto del voto. La pregunta que surge es, ¿qué recaudos debieran tenerse presente en caso de que el sistema presentara estas característica?

Los expertos señalan que una manera de garantizar el secreto del sufragio es el de efectuar auditorías completas que garanticen la no vinculación. Otro grupo, en cambio, mantiene una posición más pesimista y sostiene que ante la imposibilidad de comprobar la no vinculación entre sufragio y elector, lo mejor es usar mecanismos separados.

-Diseño de las urnas electrónicas.

Los especialistas coinciden en señalar que éstas deben tener las siguientes características: no poseer componentes abiertos, ser auditable en todas las etapas del proceso electoral y contar con soporte papel o comprobante físico del voto

Además, tiene que ofrecer alternativas para quienes poseen capacidades diferentes de manera tal de no negarles el derecho al voto.

En todos los casos, los sistemas de votación electrónicos deben emitir actas de apertura donde conste la hora de inicio y muestre que ningún partido político y/o candidato posee votos y las actas finales, donde tendrían que registrarse los resultados electorales.

-Requisitos para la transmisión de resultados.

Los expertos señalan que los resultados electorales deben estar encriptados, más aún si el proceso de transmisión hacia el centro de cómputos no se efectúa manualmente.

La encriptación es un requisito importantísimo para evitar que los datos puedan ser manipulados fácilmente. Del

mismo modo, la necesidad de contar con una línea especial para la transmisión de los resultados y no cualquier línea telefónica que posea el establecimiento donde se efectúa el comicio. Aún más, algunos consideran que debieran prohibirse los componentes de comunicación inalámbricos *(wireless)* en las máquinas 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.

-Pantallas de votación.

Respecto de los sistemas que poseen pantalla para visualizar a los partidos políticos y, según el caso, también a los candidatos, se abre el interrogante acerca de cómo éstos debieran estar ordenados. Una alta fragmentación del sistema partidario supondría un sinnúmero de pantallas que el votante debería pasar hasta llegar a encontrar la agrupación política que desea votar.

En la Argentina, las boletas de papel deben ordenarse correlativamente dentro del cuarto oscuro, según el número lista. Sin embargo, estas listas partidarias muchas veces son mezcladas (cuando no eliminadas) por algunos votantes con la intención de perjudicar a otra fuerza política. Y es aquí donde radica la ventaja del voto electrónico, ya que los electores malintencionados no podrían cambiar el orden ni destruir las boletas a su antojo.

Los especialistas sostienen que las "boletas digitales" deben mantener el mismo formato que las boletas partidarias de papel. Tienen que admitir el uso del símbolo partidario y, de ser posible, la fotografía de los candidatos para aquellos casos que el sistema electoral incorpora el voto preferencial.

Respecto del orden que tendrían que presentar las boletas digitales en las pantallas de la urna electrónica, los especialistas indican que debiera ser igual al sistema tradicional, es decir, por número de lista.

Otras opiniones adhieren a un sistema novedoso de ordenamiento por el cual las máquinas se configuran para que presenten un mecanismo aleatorio de aparición con cada elector. Se argumenta que, con este método de ordenamiento, se evitaría el desgaste de las pantallas táctiles si el electorado centrara mayoritariamente su apoyo en un partido político frente a otros menos votados. A su vez, también evitaría favorecer a las agrupaciones políticas ubicadas en las primeras pantallas frente a las que se ubican últimas. Sin embargo, una dificultad que acarrea este método es que los electores demoren mucho tiempo intentando ubicar a su agrupación política favorita y, en consecuencia, el voto electrónico pierda rapidez y sencillez.

-Logística de la organización. Urnas de contingencia.

En los lugares donde se han efectuado experiencias con distintas modalidades de voto electrónico se mantienen en reserva algunas urnas electrónicas por si llegaran a fallar las que se están usando en el comicio. Por lo general, si el problema no logra resolverse, se cambian los equipos y se continúa con el proceso eleccionario.

Algunos expertos sostienen que las autoridades de mesa no debieran permitir el acceso de ningún técnico, 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 refieran

a las circunstancias extremas en que el presidente de mesa autorice al personal técnico a reparar el equipo o reponer otro.

-Auditoría del sufragio después de la elección.

Un grupo importante de expertos sostiene que toda urna electrónica debe contar con impresoras que emitan el sufragio para que el votante pueda verificar el resultado de su elección y no se quede únicamente con la imagen que vio en la pantalla. El comprobante físico del voto tendría, a su vez, otro aspecto positivo y es que sirve como mecanismo de control en caso de que se presenten dudas sobre los resultados digitales que emitió la urna electrónica. Una posterior comparación entre "votos digitales" y "votos impresos" permitiría detectar posibles errores, fallas y/o manipulaciones intencionales.

Frente al interrogante de cuál de los dos sufragios debiera primar si llegaran a encontrarse diferencias entre ambos tipos de votos, en su mayoría, los expertos responden que deben considerarse como válidos los votos impresos porque son aquellos que el elector vio y confirmó.

Ningún voto impreso debe quedar en manos del elector. Estos deben depositarse en otra urna, dado que estos sufragios deben ser conservados por la autoridad electoral hasta que finalicen los procesos legales de impugnación y se den a conocer los resultados definitivos del escrutinio.

La legislación electoral debe contemplar las auditorías posteriores a la jornada electoral comprobando la integridad del software, independencia y verificación de los componentes de transmisión de los datos y el hardware.

Este procedimiento debe, además, contemplar una proporción estadísticamente significativa para el testeo y garantías aleatorias para seleccionar las urnas que serán auditadas.

El recuento manual de los votos impresos, es la única garantía de que los sufragios sean verificables a través de un mecanismo independiente de la informática.

-Misión y objetivos de 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 urnas 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.

Los expertos señalan que en las primeras experiencias que se realicen con voto electrónico, los asistentes informáticos son de gran ayuda. Sin embargo, no debe dejar de tenerse presente que éstos debieran mantener una distancia prudencial del elector para evitar la pérdida del secreto del sufragio y deben manejar un lenguaje neutral, para no interferir con las opciones del votante ni inducir sobre el sufragio.

Estos asistentes deberán ser seleccionados por el órgano electoral competente, a través de concurso público previa inscripción en un registro.

IV- Reflexión final

Las propuestas aquí vertidas son el producto de una serie de entrevistas efectuadas a especialistas con la intención de contribuir con la difusión general de esta nueva herramienta de votación.

Este documento enfatiza la necesidad de incluir en las futuras legislaciones, normas que favorezcan la transparencia de los comicios y el control/fiscalización por parte de los actores políticos involucrados en el proceso electoral. El cumplimiento de estas dos premisas (transparencia y

control) permitirá el desarrollo de un proceso electoral justo y equitativo en términos de competencia política junto a resultados electorales dotados de legitimidad, es decir, sin graves cuestionamientos por parte de los actores que intervienen en el proceso electoral ni por la ciudadanía en general.

Bibliografía:

Rial, Juan: "Consideraciones políticas sobre la aplicación del voto electrónico en la Argentina", en Tula, María Inés, *Voto Electrónico. Entre votos y máquinas, Las nuevas tecnologías en los procesos electorales*, Ariel-CIPPEC, Buenos Aires, 2005.

Tula, María Inés: *Voto Electrónico. Entre votos y máquinas, Las nuevas tecnologías en los procesos electorales,* Ariel-CIPPEC, Buenos Aires, 2005.

Miembros del Comité Asesor

-Angelini, Sergio. Gerente General de Magic Software Argentina S.A. (MSA).

-Arreyes, Jorge. Gerente de Allpa Argentina S.R.L.

-Betinelli, Ernesto. Profesor de Derecho Constitucional, Universidad de Pavia, Italia. Consultor en el proyecto e-poll para la implementación del voto electrónico en la Unión Europea.

-Brunazo Filho, Amilcar. Fundador y actual supervisor general de Fórum do Voto Eletrônico na Internet en Brasil.

-Cook, Robert. Director de la empresa Smartmatic. Electronic Voting Project.

-Eterovic, Jorge. Director de Proyectos. Fundación para el Desarrollo del Conocimiento (FUNDESCO).

-Falabella, Osvaldo. Ingeniero, profesor en la Universidad de La Plata., Argentina

-Fraga, Pablo. Presidente de la Asociación Actuar.

-Fassano, Vicente. Asesor informático de la Junta Electoral de la Provincia de Buenos Aires.

-Fernández, Jorge. Director Business Development Group (BDG Group).

-Figueira, Francisco. Telecomunicaciones del Sur (Tesur).

-Lizeaga Romero, Itziar. Directora de Procesos Electorales y Documentación del Departamento del Interior, País Vasco.

-Miranda Jaimes, Rene. Coordinador General, Unidad de Servicios de Informática del Instituto Federal Electoral (IFE) de México.

-Ossa, Manuel. Asesor del Tribunal Electoral de Panamá.

-Presno, Miguel Ángel. Profesor de Derecho Constitucional, Universidad de Oviedo, España.

-Prince, Alejandro. Director de Prince & Cooke. Empresa de información de mercado.

-Quinteros, Yulimar. Empresa Smartmatic.

-Rial, Juan. Analista político uruguayo, consultor para organizaciones internacionales.

-Rodríguez, Elida. Coordinadora de la Unidad de Reforma y Modernización del Estado de la Provincia de Mendoza.

-Tullio, Alejandro. Director Nacional Electoral. Ministerio del Interior de la Argentina.

-Ventureira, Hugo. Telecomunicaciones del Sur (Tesur).

-Von der Walde, Guillermo. Director de Negocios de International Business Development.

Glosario Técnico

-Software: Es la parte lógica que dota al equipo físico de capacidad para realizar cualquier tipo de trabajo, tiene su origen en ideas y procesos desarrollados por el elemento humano, plasmado en un soporte determinado del hardware. Desde un punto de vista legal, el bien jurídico tutelado es la propiedad intelectual.

-Hardware: Todos los elementos y el equipamiento que componen un sistema informático. Se consideran la "parte dura" a diferencia del software, que contiene las instrucciones que le indican a la computadora las tareas a realizar.

-Código fuente: Es el programa en su forma original, tal como fue escrito por el programador. El código fuente no puede ejecutarse directamente desde la computadora; debe convertirse en lenguaje de

máquina mediante compiladores, ensambladores o intérpretes. Contiene las instrucciones del programa escritas en lenguaje de programación; es decir, se trata de un archivo de texto legible que se puede copiar, modificar e imprimir sin dificultad.

-Encriptar: Conversión de los datos propios a un código privado e ininteligible. La encriptación transforma la información a un estado incomprensible, utilizando un algoritmo que responde a una clave de encriptación llamada "llave". Es necesario poseer esta llave para "cerrar" (encriptar) y para "abrir" (desencriptar) archivos o mensajes. La encriptación se utiliza, por ejemplo, para transmitir documentos por una red o para codificar textos de modo que no puedan ser modificados con un procesador.

Fuente: Tula (2005)

María Inés Tula. Directora del Programa Instituciones Políticas de CIPPEC. Magíster en Ciencia Política, IDAES-Universidad Nacional de San Martín. Participó de varios proyectos de investigación nacionales y extranjeros sobre elecciones, partidos políticos y sistemas electorales. Colaboró en varios libros y ejerce la docencia en distintos seminarios y materias de grado en la Universidad de Buenos Aires.

Si desea citar este documento: Tula, María Inés "Voto Electrónico: Algunos principios generales para su aplicación", *Documento de Políticas Públicas*, CIPPEC, Buenos Aires, octubre de 2006.

Acerca de CIPPEC

CIPPEC (Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento) es una organización independiente y sin fines de lucro que trabaja por un Estado justo, democrático y eficiente que mejore la vida de las personas. Para ello concentra sus esfuerzos en analizar y promover políticas públicas que fomenten la equidad y el crecimiento en Argentina. Nuestro desafío es traducir en acciones concretas las mejores ideas que surjan en las áreas de Educación, Salud, Justicia, Política Fiscal, Transparencia, Instituciones Políticas, Gestión Pública Local, Incidencia de la Sociedad Civil y Programa de Formación de Líderes Públicos.