¿CUÁNTO VALE CONFIAR?

Procesos de validación y acreditación de las infraestructuras de voto electrónico

INFORME A LOS PRESIDENTES (Informe IV, 15 Septiembre 2004)
Presidente del Gobierno de España, *D. José Luis Rodríguez Zapatero*
Presidente de la Junta de Castilla y León, *D. Juan Vicente Herrera*
Autor: OBSERVATORIO VOTO ELECTRÓNICO (OVE)
Dirección: www.votobit.org

Resumen*

EL RECIENTE referéndum revocatorio en Venezuela ha sido una excelente ocasión para comprobar los retos a los que debe enfrentarse cualquier tecnología de voto electrónico. Se desplegó allí una completa infraestructura de voto electrónico, de captura de voto, de transmisión de datos y de conteo general, pero tal esfuerzo propició paradójicamente resultados ambivalentes ya que, si bien diversas instituciones como el Centro Carter avalaron la consulta, buena parte del electorado, arropada por la opinión de algunos expertos, se ha permitido dudar de los manejos de las instituciones electorales venezolanas y de la confiabilidad tecnológica de Smartmatic, la empresa con sede en La Florida (EE UU) que asumió la provisión de sus soluciones de voto electrónico y cuya eficiencia no se discute aquí. Estamos seguros de que nadie deseaba generar el estado de percepción pública que se ha producido en Venezuela, con grave perjuicio, ***daño país****, para la credibilidad de sus instituciones electorales. Ni lo deseaba Hugo Chávez, ni la estructura electoral de Venezuela ni la empresa Smartmatic, pero entonces ¿cómo pueden solventarse situaciones como la de Venezuela o la de otras iniciativas de Estados Unidos como los casos Maryland y California?. El punto crítico radica en la certificación y acreditación de las infraestructuras, es decir, en el proceso por el que se intenta ofrecer garantías de la viabilidad tecnológica del sistema a las personas que reiteran legítimamente su escepticismo ante nuevos cambios. Es indispensable evitar la percepción eventualmente negativa de una parte de la opinión pública optimizando los protocolos de certificación y garantía de que dichas infraestructuras están protegidas contra intereses maliciosos y no van a ser usadas con dicho propósito. El objetivo de este informe consiste, precisamente, en analizar los procedimientos de acreditación y validación de las infraestructuras de voto electrónico sobre colegio electoral y las tecnologías de voto electrónico remoto (vía web) para el voto deslocalizado o con dificultades de acceso a un colegio electoral (emigrantes- o desplazados por razones de estudio, trabajo u otras).*

(*) Resumen revisado el 24/09/2004

Índice

1. Las infraestructuras de voto electrónico

Las infraestructuras de voto electrónico son costosas y generan las respectivas cuentas de negocio. Nada malo hay en ello. **Las infraestructuras de voto electrónico no obstante, son infraestructuras muy intensas en valor político y altamente críticas, que conviene descargar de tensiones innecesarias**. Es imprescindible conjugar negocio y transparencia para alcanzar con éxito el fin que se persigue. El debate, en ocasiones muy intenso, sobre las tecnologías de voto electrónico, que se ha seguido y se sigue en Estados Unidos ha aclarado muchas dudas sobre su despliegue y las rutinas de validación que deben seguirse. Son rutinas, por otra parte, muy ensayadas para otros muchos supuestos: auditoría interna + auditoría externa + periodo de alegaciones + transparencia.

El proceso en su conjunto exige que las decisiones se adopten con la suficiente antelación y previsión. Brasil necesitó seis años para validar su tecnología de voto electrónico hasta que obtuvo consenso por parte de los actores principales. ¿Puede acortarse?. Con la experiencia internacional acumulada, efectivamente, dicho proceso puede acortarse (dos años). Intentar acortarlo aún más, implica, eludir etapas claves de dicho proceso, provocar a la comunidad de expertos, excitar la atención de las distintas organizaciones sociales y abrir la caja de los truenos. Un debate prescindible e hijo natural de la soberbia y de la ignorancia, dos aliados extremadamente conflictivos que los españoles y europeos debemos ahorrarnos.

2. Rutinas de validación

La humanidad se ha servido de la tecnología de palitos durante siglos. Cada voto es un palito, se cuentan y tienen que coincidir los resultados de todos los que arrastran la cuenta. Es un proceso tedioso, poco preciso, que contrasta con las posibilidades que la tecnología nos brinda. Su sustitución por tecnologías electrónicas es irreversible. El único problema que plantean las tecnologías electrónicas es que están obligadas a preservar los indicadores de fiabilidad que nos ha legado el procedimiento manual. Un procedimiento electoral es eso, un conjunto de instrucciones para organizar la desconfianza de modo y forma que concluido el proceso se transforme en asentimiento y fe en la veracidad de los resultados. Hablamos de organizar la desconfianza, otorgando a las partes el derecho a no confiar, para que el proceso concluya con validación compartida de los resultados. Si algo tan elemental no se consigue, el proceso ha fracasado y poco importa que sea manual o electrónico.

Los contendientes electorales actúan como partes activas del procedimiento electoral, existe de todos modos, la parte pasiva o cuerpo electoral, el que otorga validez al procedimiento elegido. Si el cuerpo electoral desconfía, las partes contendientes que deseen desacreditar el proceso, encontrarán el terreno abonado en la misma proporción para las razones ciertas que para las insidias o razonamientos maliciosos.

Las tecnologías de voto electrónico se enfrentan a un reto primordial que a todos conviene que se supere con sobresaliente, el de su acreditación. Descuidar dicho objetivo es animar las diatribas y dar pávulo a las dudas. Existen suficiente casuística para afirmar que muchas de las soluciones de voto electrónico que se ofertan en el mercado adolecen de muy graves deficiencias con peligro para la integridad de todo el proceso. Acontecimiento que por sí mismo es razón suficiente para adoptar las preceptivas precauciones.

3. ¿Quién debe certificar el procedimiento y las tecnologías a desplegar?

Puesto que se trata de eliminar todo rastro de dudas y dado que estamos ante tecnologías nuevas o novedosas que escapan al control de los interventores clásicos de los partidos, se propone a los siguientes actores en el proceso de acreditación

1. Expertos de la propia administración electoral
2. *Panel de Expertos* de una organización independiente

3. Expertos cualificados a propuesta de los partidos
4. Expertos particulares (individuos u organizaciones que lo solicitan y que se acreditan para hacerlo)

4. ¿Qué procedimiento de certificación debe seguirse?

A propuesta de una organización independiente, se debe generar un procedimiento de actuación que tendrá que ser confirmado por la autoridad electoral correspondiente. El procedimiento que se sugiere es el siguiente:

1. Una organización independiente genera un panel de objetivos que debe alcanzar las soluciones de voto electrónico en sus distintas modalidades y las métricas que deben seguirse para verificar dichos objetivos **(TRES MESES).**
2. La administración electoral parcela las distintas áreas de la infraestructura electoral, las identifica y las describe de manera técnica. La parcelación de las infraestructuras se realizará con criterios de idoneidad, consistencia y facilidad de despliegue **(TRES MESES).**
3. Las tecnologías y soluciones elegidas por la administración electoral deben ser refrendadas por expertos de la organización independiente que emitirán un informe técnico cualificado, muy razonado, que será público **(10 - 12 MESES).**
4. Emitido el informe se procederá a un periodo de alegaciones al que tendrán acceso los distintos interventores-auditores que quieran nombrar los partidos y expertos particulares, individuos y organizaciones civiles que lo soliciten y que se acrediten para ello. **(TRES MESES).**
5. Las alegaciones, de naturaleza técnica, que deberán ser públicas, tendrán que ser examinadas, las que se consideren relevantes, por el *Panel de Expertos* de la Organización Independiente y contestadas públicamente. Como no puede ser de otro modo el *Panel* se reserva el derecho de modificar su opinión si obtiene una mejor en el periodo de alegaciones. (**(TRES MESES).**

La organización independiente deberá constituir el *Panel de Expertos* en función de las soluciones de hardware y software que se aportan, con declaración pública de identidad y méritos.

Concluido el proceso de acreditación la administración electoral adjudica el contrato. Las tecnologías examinadas pueden ser rechazadas por el *Panel de Expertos* por deficientes o muy deficientes, siempre previo informe público bien razonado, o pueden ser aceptadas. En el caso de ser aceptadas lo pueden ser en su totalidad o con la realización de algunos cambios. En el segundo caso, igualmente, con informe público bien razonado.

5. ¿Qué se debe certificar o acreditar?

Las infraestructuras de voto electrónico tienen que cumplir un buen número de requisitos, todos ellos dirigidos a organizar la confianza final de todas las partes en los resultados parciales y totales. Y es imperativo certificar:

1. La topología de la red de comunicaciones, su orden de despliegue, su consistencia ante averías, sobrecarga o sabotajes y personal adscrito.
2. La arquitectura de hardware, su orden de despliegue, su consistencia en operaciones ordinarias y extraordinarias y personal adscrito.
3. La ingeniería de software, su orden de despliegue, sus consistencia en operaciones ordinarias y extraordinarias y personal adscrito.
4. La fortaleza de la arquitectura de software y hardware para garantizar **a)** que el voto es secreto y que nadie puede unir valor del voto e identidad del votante; **b)** que solo vota el que efectivamente tiene derecho a ello; **c)** que el que tiene derecho a ello solo vota una vez.
5. La fortaleza de la arquitectura del sistema para responder a ataques convencionales y extraordinarios y a las posibles maquinaciones para la alteración de los resultados.
6. La funcionalidad y usabilidad del sistema en todas sus operaciones, que garanticen una inmediata comprensión de todos los interfaces en todos los escalones y que se cumplen los requisitos legales de igualdad e información para todos los contendientes.
7. Los Protocolos de seguridad de arranque, operación y parada de toda la

arquitectura en todos los escalones para organizar los derechos y obligaciones de las autoridades electorales, los interventores y del personal técnico adscrito.
8. El Manual de Incidencias.

6. Alegaciones, activismo y transparencia

Añadir el periodo de alegaciones, abierto a la sociedad o al público, y requerir para todo el proceso el aval de la transparencia es consustancial con los cambios sociales producidos en nuestras sociedades. Las empresas, ejecutivos y legisladores de los Estados Unidos con sus decisiones precipitadas de informatización de todos los procesos de consulta y votación, originaron una fuerte polémica y elevada resistencia entre expertos y poderosos núcleos de acción social y política. El origen de toda la polémica, y no hay razones para no suponer que no se reproduzca con igual intensidad en Europa, reside en la incomprensión por parte del ejecutivo y el legislador estadounidense, del nivel cierto de desarrollo alcanzado por la oferta y la demanda de acción política electrónica (e-mail y www).

El activismo político electrónico es deslumbrante si se compara con épocas pasadas. Estamos ante un activismo atinente con la sociedad del conocimiento que ha sido capaz de generar numerosos individuos con un elevado grado de destreza en el uso de las nuevas tecnologías, conociendo con detalle y precisión sus potencialidades y debilidades.

Los tremendos agujeros de seguridad detectados en algunas soluciones de voto electrónico y la resistencia de algunas empresas, más o menos apoyadas por las autoridades electorales, ha mostrar ante el público su arquitectura de software, aportando todo el código para su auditoría, al amparo de supuestos derechos de propiedad intelectual, no ha conseguido distraer a los expertos. La Ley electoral de los Estados Unidos obliga a certificar todas las soluciones de voto electrónico y a aportar el código fuente para su auditoría.

El problema surge cuando se duda de la existencia de certificadores cualificados, identidad y formación; cuando no existe información de referencia bien documentada; cuando la opacidad preside todo el proceso y cuando se logra demostrar, como ocurrió en Maryland que la empresa seleccionada, Diebold Election Systems, que la auditoría contratada por el propio gobernador del Estado a la Universidad John Hopkins, revela que los expertos tenían razón y que eran otros los que mentían. La auditoría fue dirigida por una de las máximas autoridades en cortafuegos, seguridad y tecnologías de voto electrónico.

Los procesos electorales actuales semielectrónicos, con captación manual del voto y conteo general informatizado, se pueden realizar con los bajos indicadores de seguridad existentes en los actuales centros de cómputo, dado que las partes contendientes disponen de su propio testimonio escrito (actas) del resultado general de las distintas mesas electorales. Cuando desaparece de manera definitiva el recuento manual por la confiabilidad que ofrecen los sistemas electrónicos, la carga de la prueba recae sobre la garantías que proporciona el propio sistema en su conjunto. Y es en este punto cuando los expertos y las organizaciones civiles exigen una revisión exhaustiva de la infraestructura de voto elegida.

Como fuera que numerosas autoridades electorales en los Estados Unidos, para proteger sus decisiones de adjudicación de soluciones de voto electrónico, se han negado a revisiones cualificadas, la movilización de expertos, organizaciones cívicas e incluso los grandes partidos, ha supuesto la irrupción de todo tipo de dudas y desconfianzas sobre la tecnología, sobre sus operadores y quienes les respaldan, convirtiendo un problema técnico en otro, muy distinto, de naturaleza política.

Cuando hablamos del pésimo cálculo del poder ejecutivo y legislativo sobre las dimensiones y tamaño del activismo político en la red, nos estamos refiriendo a la incapacidad que han demostrado para superar la barrera argumental de dichos grupos, con mayor crédito y autoridad en estos lances que las autoridades correspondientes.

La opinión pública está en exceso familiarizada con los graves problemas de seguridad asociados al gigante de Redmond,

Microsoft, como para aceptar de buen grado y a la primera, la fiabilidad de las soluciones de voto electrónico que promueven muy diversas empresas. No es difícil imaginar lo que pueden pensar y suponer los expertos.

7. Prioridad jurídica

Invocar la supremacía de los derechos de propiedad intelectual de empresas particulares, que ocultan su código tomando como rehén a toda la ESTRUCTURA ELECTORAL, sobre los derechos políticos de toda una comunidad, cuando se ha demostrado fehacientemente la existencia de irregularidades, es una opción discutible, controvertida en muy alto grado, que invita a deducir que se oculta al escrutinio público porque protege intereses maliciosos.

8. Voto electrónico remoto

Las tecnologías de voto remoto, vía web, tan atractivas e interesantes, que tanta inmediatez proporcionan y que tanto nos acercan a lo que la experta y analista Pippa Norris, de John F. Kennedy School of Government de Harvard University, llama ***política total***, se enfrentan a los problemas de seguridad que plantean los ordenadores personales que corren sobre el sistema operativo **Windows**.

No se trata de problemas específicos de las tecnologías de voto electrónico o de interacción, de su consistencia y seguridad, se trata de las graves vulnerabilidades del sistema operativo **Windows**, que afectan a la oferta y demanda de servicios y acciones políticas, relacionadas con la interacción eficiente y segura entre los participantes y que están lastrando el débil despliegue de la oferta política por parte de las distintas administraciones.

La ***política total,*** al intervenir acortando prodigiosamente el espacio y el tiempo –proporcionando un grado de sofisticación en la participación imposible de imaginar hace unos pocos años–, actúa sobre los incentivos estratégicos para los partidos, los políticos y los ciudadanos. Impacto que terminará cambiando las reglas electorales que a su vez generarán cambios en los comportamientos políticos para terminar afectando a la intensidad y complejidad de los derechos políticos tal como hoy los conocemos.

Internet tiene un intenso impacto sobre los estándares de acción y participación política, razón, por sí misma, de suficiente entidad como para considerar con seriedad la conveniencia de estimular los sistemas de participación y voto electrónico vía web o remoto con las debidas garantías y cautelas.

9. Infraestructuras estratégicas

Existen dos procedimientos para estimular las tecnologías de voto electrónico, el inmediato e instrumental, favoreciendo su despliegue para satisfacer una necesidad puntual y concreta, y el estratégico, que sienta las bases para una transformación de España. El estratégico lleva implícito decisiones operativas, logísticas y legales para favorecer el despliegue de los **Núcleos de Habeas Data** y una sólida red pública de identificación remota (yo soy quien digo ser) como se relata en los informes I y II.

España posee la estructura del DNI, un sistema de identificación biométrica, censal, numérico y caligráfico. Posee además un censo estable. Ninguna de las dos estructuras es considerada por los españoles como una invasión intolerable de la privacidad como ocurre en el Reino Unido o en EE UU. En nuestras opinión se trata de ventajas cualitativas que hacen más fácil el despliegue de los **Núcleos de Habeas Data**. Dos requisitos, en cualquier caso, deben respetarse: **1)** la transparencia (eso es un **Núcleo de Habeas Data**) y **2)** el resguardo de las instituciones públicas del descrédito y la desconfianza. La utilidad práctica de los **Núcleos de Habeas Data** se describe con detalle en los informes I y II antes citados y presentes en nuestra página web.

OBSERVATORIO VOTO ELECTRÓNICO – OVE
León, 15 de Septiembre de 2004
www.votobit.org