Aspectos tecnológicos del voto electrónico.

Luis Panizo Alonso . Secretario del Observatorio del Voto Electrónico. Universidad de León. España. luis.panizo@unileon.es

Resumen.
En este trabajo se pretende mostrar el "estado del arte" del uso de la tecnología en los procesos electorales. En primer lugar, exponiendo la situación actual en los diversos países y posteriormente analizando el estado de la investigación en la materia. También se pretende realizar una comparación entre los esfuerzos y determinar el camino correcto a seguir para conseguir que el voto electrónico consiga cumplir todos los requisitos necesarios para que sea considerado como otro medio más en los comicios.

Abstract.
This paper is a review of the 'state of the art' of the use of technology in elections. First, current situation all over the world is described. Then, several researching efforts related to electronic vote are analyzed and compared in order to establish the path to get the electronic vote to fulfill all the requirements to be considered just as the other instruments for elections.

Palabras clave: Voto electrónico. Voto por internet. Urna electrónica. Democracia electrónica. Seguridad en red. Seguridad en la votación.
Key words: Electronic vote (e-vote). Internet vote (i-vote). DRE. Electronic democracy (e-democracy). Network security. Security of voting.

Génesis del voto electrónico.

Puede parecer que los intentos de utilizar las Tecnologías de la Información y de las Comunicaciones (TICs) en los diversos aspectos del voto electrónico (VE) son recientes, pero no es así. De hecho una de las primeras aplicaciones de las tecnologías electromecánicas de finales del siglo XIX fue su uso para el ejercicio del VE y del recuento de votos posterior. Así Thomas Alva Edison en 1.869 firmó una aplicación de patente (nº 90646) para un sistema de grabación de voto eléctrico el cual luego sería utilizado para su primera patente, ya que nadie quiso utilizarla. En 1.892 Jacob H. Myers diseña la AVM (*Automatic Voting Machine*) que se utilizó en varias ocasiones en el estado de New York [1]. Era una máquina basada en mecanismos de levas que se siguieron utilizando posteriormente en otras máquinas similares (Davis y Boma

[1] Creelan J., Norden L. *The requirements of New York University School of Law*. Noviembre 2.005 . www.wheresthepaper.org/brennanctr11_16fullface.htm

machines). Con la aparición de los primeros computadores a mediados de los años cuarenta se retomó la posibilidad de utilizarlos para el VE y varios prototipos vieron la luz a mediados de los 60. Más tarde se han venido utilizando de modo generalizado en todo el mundo para el recuento de votos y el cálculo de resultados finales. La idea de modernizar los procesos electorales utilizando tecnologías basadas en la electrónica proviene de pensadores como Fromm (1.955) [2], Fuller (1.963) [3] , Arterton (1.987) [4] y Rheingold (1.993) [5]. En la actualidad raro es el país que no haya intentado desarrollar pruebas de voto electrónico con diversos tipos de soluciones y tecnologías.

¿Es necesario el VE?: ventajas e inconvenientes.

Muchas son las preguntas sobre la necesidad real de utilizar la tecnología para resolver los procesos electorales. Sus defensores enfatizan las ventajas y minimizan los desventajas. Alguno de estos aspectos son indiscutibles pero otros se dan por seguros incluso sin estudios básicos sobre el tema. En la parte positiva destacan la precisión y la rapidez y en la negativa la falta de seguridad.

Entre los aspectos positivos caben destacar: precisión en la contabilidad de los votos, rapidez en el recuento, incremento de la accesibilidad para discapacitados o por personas con diversidades funcionales, ahorro de papel, flexibilidad, posibilidad de crear una infraestructura permanente para la opinión con voto, mejora de la eficiencia, etc. También se dan por ventajas aspectos más discutibles como pueden ser el ahorro ecológico ya que las urnas tienen un determinado consumo energético en su fabricación y uso.

Otro aspecto es que su utilización parece ser más barata que el uso de la urna tradicional pero hay pocos estudios serios, por poner un ejemplo, en las últimas elecciones presidenciales con urnas electrónicas celebradas en Venezuela en Diciembre de 2.006 el coste estimado fue de 200 millones de dólares . Por otro lado hay comparativas de costes en U.S.A [6] entre las urnas basadas sistemas con exploración óptica (*optical scan*

---

[2] Fromm E. *The sance Society*. 1.955 . New York Rinhart
[3] Fuller B.R. *No more secondhand God*. 1.963 . Southern Illinois University Press
[4] Arterton C. *Teledemocracy: cantechnology protect democracy?*. 1.987 .SAGE publications
[5] Reingold H. *The virtual Community*. 1.993 . Addison-Wesley
[6] Hite R.C. (director) *Electronic voting offers, opportunities and presents challenges*. Julio 2.004 . U.S. Govermment Accountability Office

systems) y urnas electrónicas con registro directo o DREs (*direct recording electronic systems)*, pero la variación del precio de compra llega al 900% en función de las características del equipo y su configuración, siendo destacable que en el caso de las DREs se factura el coste de la máquina y el del software de forma separada.

A considerar también está el supuesto aumento de la participación [7] [8]en el cuál este trabajo no va a entrar.

En cuanto a los inconvenientes también son variados y algunos no demostrados como ocurre en el párrafo anterior. Lo cierto es que en general la seguridad del proceso de votación está en entredicho y se concluye que la tecnología tiene demasiados riesgos. Ha sido un error grave de los desarrolladores e investigadores considerar que el nivel de seguridad de una votación electrónica es similar al requerido en una entidad financiera [9], ya que en esta, el secreto de la operación puede ser conocido por terceros autorizados y en cambio en el voto electrónico el anonimato es parte esencial del mismo, con lo que NADIE puede tener información sobre el voto salvo en el proceso final de recuento y exclusivamente para la contabilidad. Este tipo de inconvenientes nos obligan a utilizar diversas técnicas de verificación del voto como el VVAT (*voter-verified audit trial*, prueba de auditoria mediante verificación del votante) [10], lo que complica y ralentiza el uso de las máquinas utilizadas para el voto electrónico. A pesar de todo hay claras limitaciones en la seguridad de estos equipos si no se toman las medidas oportunas desde el inicio de su diseño [11] [12] .

Otro aspecto negativo es el posible fraude que se puede realizar con este tipo de dispositivos. En este caso si hay estudios rigurosos como los de Di Franco et al [13] que demuestran que con una pequeña manipulación en la copia maestra del software de votación es posible producir un fraude electoral a gran escala.

---

[7] Fernández I.D. *El voto electrónico*. 2.003 . Revista del Ilustre Colegio de Abogados de Madrid

[8] Cantijoch M. *El voto electrónico ¿un temor justificado?*. 2.005 . Revista TEXTOS de la Cibersociedad nº 7

[9] Cox C. , Rubin A. *Is the U.S. ready for electronic voting?*. 20/09/2004 . New York Times Upfront

[10] Mercuri R. *Rebecca Mercuri´s statement on electronic voting*. 2.001 . www.notablesoftware.com/RMstatement.html

[11] Kohno T. , Stubblefield A. , Rubin A.D. *Analysis of an Electronic Voting System*. Julio 2.003 . IEEE Symposium on security and privacy 2.004

[12] Armen C. , Morelli R. *E-voting and computer science*. 2.005 ACM ITiCSE´05

[13] Di Franco et al. *Small vote manipulations can swing elections*. Octubre 2.004 . Communications of the ACM

Sin haber resuelto completamente estos aspectos, la tendencia actual es el uso de Internet para la emisión del voto electrónico, lo que incrementa enormemente los riesgos en seguridad.

En este caso varios autores [14] [15] [16] [17] denuncian el elevado riesgo en seguridad por el mero uso de Internet (virus, troyanos, denegación de servicio distribuida, falta de control por las autoridades electorales de los equipos utilizados por los votantes, etc.) y por la baja transparencia del procedimiento incluyendo la posible pérdida del anonimato. Incluso el propio Vinton Cerf considerado uno de los "padres" de Internet por su aportación al protocolo TCP/IP considera que una de las debilidades de la Red es su baja seguridad. No es menos cierto que aparecen ventajas inherentes a la independencia del tiempo y del espacio en la emisión del voto, al probable incremento de la participación al evitar los desplazamientos, a la reducción del coste, a pesar de no existir trabajos rigurosos al respecto, al decremento de votos nulos, etc.

En cualquier caso, es necesario garantizar una serie de aspectos en el voto electrónico lo que hace que las posibles soluciones sean cuando menos complejas:

1. Autenticación: que sólo los que estén legitimados para votar, voten.
2. Unicidad del voto (democrático): que sólo se pueda votar una vez y no se pueda modificar el resultado de dicha votación.
3. Anonimato: que no se pueda relacionar el votante con el voto.
4. Imposibilidad de coacción: el votante no puede en ningún caso ser capaz de demostrar qué voto emitió, impidiendo la compra masiva de votos y la presión (coacción) sobre los votantes.
5. Precisión: el sistema tiene que poder registrar los votos correctamente y con seguridad.
6. Verificación (trazabilidad): cada votante podrá obtener un recibo del sistema de votación que le garantice que su voto será incluido en el escrutinio final. Existen diversos niveles de verificación como veremos posteriormente.

---

[14] Schryen G. *Security aspects of Internet Voting*. 2.004 . Proceedings of the 37 th Hawai International Conference on Systems Sciences

[15] Schryen G. *E-Democracy: Internet Voting* . 2.003 . Proceedings of the IADIS International Conference

[16] Jefferson D. , Rubin A.D. et al. *Analyzing Internet Voting Security*. Octubre 2.004 . Communications of the ACM

[17] Wu C.K. , Sankaranarayana R. *Internet voting: Concerns and solutions*. 2.002 . Proceedings of the first International Symposium on Cyberworlds (CW´02)

7. Imparcialidad: todos los votos deberán permanecer en secreto hasta que finalice el periodo de votación. De esta forma se evita que los resultados parciales afecten a la decisión de los votantes que no han votado.
8. Auditabilidad: que existan procedimientos para poder verificar que todos y cada uno de los votos se han tenido en cuenta en el escrutinio.
9. Confiabilidad: los sistemas utilizados deben trabajar de modo seguro siempre, sin que se produzcan pérdida de votos incluso en casos extremos.
10. Flexibilidad: los equipos involucrados en la voto electrónico deben de ser flexibles con los formatos utilizados (idiomas, posibles elecciones a distintos órganos, diversos tipos de papeletas de votación) , y ser compatibles con todo tipo de plataformas y tecnologías.
11. Accesibilidad: que permita ejercer el voto a personas con diversidad funcional o discapacitados.
12. Facilidad de uso (usabilidad) : los votantes tienen que ser capaces de votar con unos requisitos mínimos formación y entrenamiento.
13. Eficiencia en el coste: los sistemas tienen que ser asequibles y reutilizables fácilmente.
14. Certificables: los sistemas deben poder comprobarse por parte de las autoridades electorales, para que puedan confiar en que cumplen con los criterios establecidos.
15. Invulnerable, impidiendo la manipulación a todos los niveles.
16. Compatible con la tradición electoral y por tanto que se parezca lo más posible a una urna convencional en su aspecto y uso.
17. Abierto, de forma que las autoridades electorales y ,si es el caso, el ciudadano en general puedan obtener detalles de su funcionamiento (hardware y software).
18. Barato, de forma que sea competitivo con el voto tradicional.
Sin duda que el cumplimiento en mayor o menor grado está en función de los diversos puntos de vista de los elementos involucrados: administración, ciudadanos (electores), empresas y la Academia. De esta forma la administración en general opina que los procesos electorales son complejos, costosos y en algunos casos poco eficientes y problemáticos, por lo que intentan utilizar las TICs para su simplificación, mejora y abaratamiento. Los ciudadanos observan que los métodos utilizados son arcaicos y en algún caso poco fiables (papeletas perforadas en el estado de Florida en Noviembre del 2.000, voto por correo en la mayor parte de los países, etc) pero no están seguros que los nuevos métodos usando la tecnología cumplan los requisitos imprescindibles. Las

empresas ven una oportunidad de negocio ofreciendo máquinas que cumplen con su cometido y muy probablemente bien desarrolladas , pero con escaso control por parte del contratante e intentando mantener la solución como una "caja negra" y con la única posibilidad de su verificación desde el exterior [11]. La Academia ve todo esto como un reto científico y tecnológico e intenta desarrollar soluciones que minimicen los problemas y garanticen el cumplimiento de los requisitos necesarios.

Clasificación del voto electrónico.

Existen una gran diversidad de formas de votar y sistemas involucrados en los procesos de voto electrónico y su clasificación depende del punto de vista. Varios autores lo han realizado pero nosotros preferimos reducir esta clasificación al máximo posible para facilitar su comprensión y flexibilidad. La clasificación más sencilla es la que se produce al dividir los procesos de votación en presenciales y no presenciales.
Así cuando votamos con ayuda de una máquina dispuesta en un lugar específico (colegio electoral) y que para acceder a ella el votante, previamente, ha de ser identificado manualmente y autorizado a utilizar la máquina, que en este caso genéricamente se denomina DRE (*Direct Recording Electronic*) o sistema de registro electrónico directo, el proceso de votación es presencial. En este caso el proceso de identificación es independiente y no debe de existir la posibilidad de relacionarlo con el voto depositado y toda la información necesaria está "in situ". Por tanto se utiliza un equipo específico.
Por el contrario cuando el voto es ejercido no presencialmente, es decir, de forma remota, utilizando medios telemáticos (votación telemática) [18] o más concretamente Internet, el sistema lo hace todo (identificar y enviar el voto) y probablemente con independencia del dispositivo (ordenador personal o equipamiento equivalente). Por tanto, en este caso el equipo no es específico [19].
Clasificaciones más amplias permiten ver con más detalle los sistemas utilizados y su evolución. Sistemas tradicionales: papeletas, tarjetas perforadas, máquinas de palancas o

[11] Kohno T. , Stubblefield A. , Rubin A.D. *Analysis of an Electronic Voting System.* Julio 2.003 . IEEE Symposium on security and privacy 2.004
[18] Gómez A. , Carracedo J. *Del voto electrónico al voto telemático*. 2.004 . Boletín Red-Iris 66-67
[19] Qadah G.Z. , Taha R. *Electronics voting systems: requirements, design and implementation*. 2.007 . Computer standards & Interfaces , 29

levas. Sistemas de voto electrónico convencionales (genéricamente urnas electrónicas): urnas con OCR (reconocedores ópticos de caracteres), DREs (en general con pantalla táctil y guardado de datos en dispositivos basados en semiconductores), mixtos (híbridos). Voto remoto o telemático: en quiosco electoral ubicado en cualquier parte, en quiosco electoral ubicado en colegio electoral, sobre cualquier dispositivo con conexión a Internet y desde cualquier parte (voto remoto puro).

Las estadísticas de uso son muy variadas en función del país y el tipo de elecciones, pero dentro de las urnas electrónicas las más utilizadas en U.S.A. en el 2.004 fueron las ópticas seguidas de las DREs. En cambio el voto electrónico puro se ha utilizado en muy pocos países y menos de forma vinculante como ha sido el caso de Estonia en marzo de 2.007 [20].

Si nos centramos en los dispositivos electrónicos que podemos utilizar en el voto electrónico podemos finalmente clasificarlos en función de su uso controlado y no controlado [21]. En el primer caso podemos tener:

- Dispositivos de voto electrónico independientes o autónomos (*stand-alone)*
- Dispositivos de voto electrónico conectados a red (*networked)*

Y en el segundo:

- Dispositivos para voto electrónico remoto o telemático (PCs, móviles, PDAs)

Incluso podemos considerar el caso de dispositivos que puedan utilizarse en ambos ambientes, controlados y no controlados:

- Quioscos para voto electrónico conectados a red.

Estado del arte del voto electrónico en el mundo.

La mayor parte de los países en el mundo han considerado el uso del voto electrónico. De ellos una buena parte han realizado pruebas y algunos ya utilizan el voto electrónico de forma vinculante. En Europa como ahora veremos se han desarrollado diversos esquemas con pruebas en la mayor parte de los países. Fuera de Europa el uso del voto electrónico está ampliamente desarrollado en la mayoría de los estados de U.S.A. y en Brasil, seguido de cerca por Méjico. Está siendo considerado en buena parte de los países de América Central y del Sur. Además tenemos a una parte de los antiguos países

[20] Borland J. *Online voting clicks in Estonia*. Marzo 2007. www.wired.com/politics/security/news/2007/03/72846

[21] Krimmer R. *Overview*. 2.006 www.e-voting.cc

que formaron la Unión Soviética, India y Australia. Vamos a ver con más detalle el estado del arte en estos países.

Suiza, que recordemos está fuera de la Unión Europea, es un ejemplo a seguir por el desarrollo en la implantación del voto electrónico. En este país, dividido administrativamente en cantones, se llevan a cabo consultas de forma continua y era muy utilizado el voto por correo. Posteriormente en algunos de los cantores se pusieron en marcha pruebas de voto electrónico utilizando diversos métodos y durante varios años. Estudios posteriores determinaron su uso vinculante, sobre todo después del alto incremento en la participación que se produjo en los referendos de 2.003 y 2.004 realizados en Anieres, Cologny y Carouge [22] [23]. Hoy la mayor parte de los ciudadanos suizos utilizan y confían en el voto electrónico.

Bélgica fue el pionero del voto electrónico en Europa. Lo utilizaron en el cantón de Verlainer en 1.991 con tarjeta magnética y lápiz óptico. En Octubre del 2.000 ya el 42% de la población votó electrónicamente. En cualquier caso este país es muy especial debido a que el voto es obligatorio y su sistema electoral muy complejo, por lo que el uso del voto electrónico es valorado positivamente por la administración electoral.

Holanda ha llevado a cabo grandes pruebas en estas tecnologías incluyendo el voto por Internet y teléfono. La mayor de ellas se desarrolló en Junio de 2004 para las elecciones al parlamento europeo. Actualmente se puede votar electrónicamente pero la opinión de los ciudadanos está dividida, sobre todo después de una demostración en directo, por televisión ,de cómo se puede modificar una parte del software de la máquina y recibir emisiones radioeléctricas a distancia con información de quién está votando [24]. La empresa que fabrica la urna (Nepad) ha garantizado que corregirá los errores. Esta misma máquina con pequeñas variantes se está utilizando en pruebas en Alemania y Francia. En Irlanda se duda de su seguridad después de diversas pruebas.

Inglaterra ha desarrollado pruebas a gran escala, a nivel municipal, desde el 2.000. En Junio de 2.004 se hizo una prueba de voto electrónico en Londres. El proceso seguido es minucioso y se desarrolla con tiempo, obteniendo de esta forma un avance seguro hacia

---

[22] *The Geneve E-Voting Project*. www.geneve.ch/chancelleire/e-goverment

[23] Braun N. , Brändli D. *Swiss e-voting pilot proyects: evaluation, situation analysis and how to proceed* 2.006 E-Voting.cc

[24] Gonggrijp R. , Hengeveld W.J. *Nedap/Groenendaal ES3B voting computer*. Octubre 2.006

un escenario de voto electrónico bien diseñado y correctamente planificado, [25] [26] lo cuál no significa que por el camino aparezcan problemas como lo ocurrido en los comicios municipales celebrados en Mayo de 2.007 en los que se perdieron una parte de los votos. Un estudio posterior critica la falta de un sistema lo suficientemente riguroso de certificación que asegure que tanto el hardware como el software que se utiliza está libre de vulnerabilidades.

Escocia que un caso similar al anterior. Además dispone de uno de los sistemas electrónicos de participación ciudadana (e-petición) para el parlamento escocés más elaborado, analizado y cuidado de Europa.

Irlanda desde el año 2.000 ha llevado a cabo un proyecto elaborado cuidadosamente para introducir quioscos de voto electrónico en todos los colegios electorales para las lecciones locales de Junio de 2.004. Finalmente y gracias a que el proceso fue totalmente abierto, se emitió un informe [27] por parte de dos destacados científicos que pusieron en duda la fiabilidad del sistema y no se llevó a cabo el proyecto [28].

Alemania comenzó sus primeras pruebas de voto electrónico en 1.999 pero en ámbitos no políticos y ha elaborado una documentación precisa sobre los requisitos que deben de cumplir los equipos involucrados. Posteriormente , en septiembre de 2.005 se utilizó el voto electrónico presencial para las elecciones parlamentarias de forma vinculante en algunos colegios con éxito desigual. También se desarrolló un sistema de voto por Internet (i-vote) que no ha sido utilizado para elecciones legislativas.

Austria estableció en Julio de 2.003 un plan para el voto electrónico [29]. Se han desarrollado pruebas de voto por Internet, en paralelo con las elecciones presidenciales en Abril de 2.004 con buenos resultados. En la primavera de 2.004 el Ministerio del Interior constituyó un grupo de trabajo sobre voto electrónico.

Francia ya en el 2.003 utilizó Internet para elecciones para el Consejo Superior de Franceses en el Extranjero (CSFE) , pero sin conseguir incrementar la participación. También se ha utilizado voto electrónico en colegios electorales seleccionados, usando

---

[25] The Electoral Commission. *The shape of the elections to come*. 2.003 . www.electoralcommission.gov.uk

[26] The Electoral Commission. *The electoral pilots at June 2004 elections*. 2.004 . www.electoralcommission.gov.uk

[27] McGaley M. , Gibson J.P. *Electronic Voting: a safety critical system*. Marzo 2.003 . National University of Ireland

[28] Commission on Electronic Voting. *Secrecy, accuracy and testing of the chosen E.V. System*. 2.004 . www.cev.ie

[29] Austrian Computer Society (OCG). *E-voting action plan*. 2.003 . www.e-voting.at

la huella dactilar integrada en una tarjeta (*smart card*), para las elecciones al parlamento Europeo en 2.004. En las últimas elecciones presidenciales del 2.007 también se utilizaron urnas electrónicas por parte de 1,5 millones de personas de un total de 44, 5 millones. Se registraron problemas sobre todo con los votantes de mayor edad.

España también ha desarrollado pruebas de voto electrónico[30], pero todas ellas no vinculantes ya que no lo permite la legislación electoral. En Febrero de 2.005 se desarrollo la primera prueba de voto electrónico por Internet que resultó ser un fracaso técnico y de participación [31].

Italia , de forma muy similar a Francia, también utilizó el voto electrónico no vinculante y a pequeña escala en colegios electorales.

Eslovenia y **Hungría** elaboraron una normativa previa sobre voto electrónico en 2.003 pero no consiguieron la aprobación de sus respectivos parlamentos.

Estonia es un país pionero en el uso vinculante y flexible del voto por Internet. Ya en el otoño del 2.005 se realizó una prueba piloto avanzada en unas elecciones locales, utilizando *smart cards* con firma electrónica. Posteriormente en las elecciones parlamentarias del 2.007, 30.275 personas votaron por Internet (3,5% de la población). En cualquier caso este es un caso muy especial y difícil de extrapolar, debido a la alta penetración de Internet en la sociedad y a la posibilidad de utilizar la tarjeta de identificación con clave privada y pública. [20] [32] [33]

La **Unión Europea** desarrolló un proyecto denominado *EU CyberVote Project* [34] durante los años 2.002 y 2.003. El objetivo era verificar las garantías de privacidad y seguridad en una votación en línea sobre Internet utilizando terminales fijos y móviles. Fue desarrollado por las empresas más reconocidas de telefonía y tecnología, muchos suponen que no podría haber sido de otra forma. Las conclusiones son que el prototipo diseñado *CyberVote prototype* funciona en condiciones normales tanto desde terminales fijos como móviles, como se puso de manifiesto en varias pruebas, pero es imposible garantizar su fiabilidad en votaciones reales y en ambientes no controlados, es decir allí donde están presentes los grandes riesgos en materia de seguridad de Internet.

---

[30] Riera A. , Cervelló G. *Experimentation on secure Internet voting in Spain* 2.004 Scytl, S.A.

[31] Panizo L. (coordinador). *Así, no*. Febrero 2.005 . www.votoelectronico.es/informes

[32] Madise Ü. , Martens T. *E-voting in Estonia 2.005.The first practice of country-wide binding Internet voting in the world*. 2.006 Tallinn Univ. Of Tech.

[33] Maaten E. *Towards remote e-voting: Estonian case* 2.004 Elections Dep. of Estonian

[34] http://www.eucybervote.org

Por otra parte el Consejo de Europa (CoE) constituyó en Noviembre de 2.002 un grupo de expertos denominados IP1-S-EE para fijar estándares para el voto electrónico (*e-enable voting*). Posteriormente se constituyeron dos subgrupos, uno de aspectos legales y operacionales y otro técnico. Pero se verificaron muchas más dificultades de las inicialmente esperadas. Cada país expresó expectativas diferentes en marcos legales distintos y con niveles de seguridad que la industria no podía en aquel momento satisfacer. Además la neutralidad tecnológica fue planteada en varias ocasiones en el núcleo de la discusión. El principal avance fue reconocer la necesidad de una cooperación muy estrecha entre los expertos legales y los técnicos. A raíz de estas reuniones se produjo la aparición de unas recomendaciones publicadas en septiembre de 2.004, por parte del Consejo de Ministros del Consejo de Europa, denominadas Rec(2004)11 [32] . Estas se desarrollan sobre dos principios generales: el voto electrónico ha de ser tan fiable y seguro como un proceso de votación en el que no se utilice tecnología y , además, debe de ser un canal adicional y opcional de voto.

Los **Estados Unidos de América** son un caso único en el mundo debido a la gran complejidad de su sistema electoral, en el que cada Estado e incluso cada Condado determina la forma y los recursos electorales a utilizar. En las elecciones presidenciales de noviembre de 2.000, casi el 70% de los votantes utilizó la vía electrónica para emitir su voto, contando con anticuados mecanismos como la tarjeta perforada, aunque también se utilizó el voto con lectura óptica y la máquina electrónica de registro automático (DRE). En los últimos comicios nacionales de los EEUU, celebrados en el año 2.004, la mayor parte de los votantes emplearon sistemas automatizados; 13,7% de los ciudadanos votaron con tarjetas perforadas; 14% empleó sistemas similares a la manivela de hace más de 100 años; 34,9% sufragó en equipos de lectura óptica y 29,3% empleó para sufragar equipos desarrollados bajo el concepto del Registro Electrónico Directo**.** El principal inconveniente de estos sistemas es la confianza ciega que se deposita en los expertos que supervisan los procesos y la falta de mecanismos de verificación, lo que pone en tela de juicio su validez . Uno de los fallos más destacables de estos sistemas es el que tuvo lugar en el estado de Florida, donde la falta de normativa y control , unido a una tecnología obsoleta (tarjeta perforada), propició que

[32] http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/01_recommendation/04E-voting%20Rec%20Spanish%20-Traducci%C3%B3n%20Rec%202004%2011%20Comit%C3%A9%20Mins%20Consejo%20Europa.asp

muchos votantes no pudieran saber con certeza qué opción era la que habían marcado. Otro caso muy relevante fue el de compañía Diabold y más concretamente su sistema AccuVote. El profesor de la Universidad Johns Hopkins, Avi Rubin, analizó el código fuente y determinó la falta de seguridad en el sistema, accediendo al portal FTP de la empresa [33]. Posteriormente se fueron sumando más verificaciones negativas hasta el punto, que el Secretario de Estado de California, Kevin Shelly, retiró el certificado a 14.000 de estas máquinas y ordenó una investigación por supuesto fraude de la compañía . Los informes coinciden: "El uso de código fuente propietario, que está oculto y es complejo en sí, hace que sea extremadamente difícil determinar la ausencia de código malicioso en el firmware". [34]

En los EEUU existe un debate muy enriquecedor sobre el uso de la tecnología en los procesos electorales. Desde finales del 2.006 funciona en la Universidad Johns Hopkins un centro de estudio destinado a incrementar la confianza en las tecnologías del voto electrónico. El proyecto está destinado a abordar las inquietudes del público con respecto al empleo creciente de urnas electrónicas en los comicios locales, estatales y nacionales. Es importante resaltar que esta no es una propuesta privada. La iniciativa denominada "*Accurate*" (exacta), que por sus siglas en inglés significa elecciones correctas, funcionales, confiables, auditables y transparentes, recibirá un aporte de 7,5 millones de dólares por parte de la Fundación Nacional para las Ciencias de EEUU. [35]

Con el respaldo de la Ley denominada Ayude a América a Votar (HAVA), promulgada en el año 2.002, los gobiernos municipales y locales de EEUU están debatiendo sobre la conveniencia de aumentar la tecnología en los comicios previstos para el año 2.008. Todo indica que Estados Unidos se desplazó hacia la votación electrónica en las elecciones públicas antes de que la tecnología estuviera lista y que se hizo sin estudios ni pruebas previas. Básicamente, el proyecto, liderado por Rubin, analizará las máquinas y la programación de votación electrónica, incluida la criptografía, que se utiliza para garantizar que los electores mantengan su privacidad, así como, los métodos utilizados para verificar que los ordenadores totalicen con precisión todos los votos legítimos; otros miembros del equipo se encargarán de los aspectos legales y de las políticas públicas que hayan recibido poca atención en la transición a la votación electrónica.

---

33 www.cs.uiowa.edu/~jones/voting/dieboldftp.html#rebuttals
34 www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf
35 www.verifiedvotingfoundation.org/article.php?id=6289

Para intentar disminuir las dudas sobre los sistemas automatizados los investigadores de la universidad Johns Hopkins consideran necesario abrir los procesos de prueba de los sistemas a la observación por parte de los ciudadanos y organismos independientes, establecer procesos permanentes de análisis, facilitar los estudios independientes, ejecutar auditorias aleatorias de las máquinas para comprobar que nadie haya manipulado el software utilizado, realizar muestreos en sitios aleatorios y en un número específico de máquinas el día de las elecciones para comprobar que cada sistema registra los votos de manera adecuada, impedir que el código fuente de los equipos pueda ser modificado, exigir una revisión de las pantallas en todos las máquinas de votación para minimizar la posibilidad de votos ocultos u otras anomalías y contar con la impresión de un registro físico permanente, independiente del recibo entregado al elector al momento de votar para la verificación de su voto. Claro que todo esto puede hacer que el proceso automatizado se convierta en más complejo que el manual , ya que requerirá la verificación manual sobre el proceso automatizado, es decir dos procesos en uno, y por tanto se puede convertir en más complejo y lento . Cabe destacar que el profesor Rubin ha publicado recientemente (año 2.006) un libro titulado "*Brave new ballot"* [38]en el que literalmente dice: " Imagine por un momento que usted vive en un país donde nadie está seguro de cómo se cuentan los votos y no existen registros fiables para realizar un recuento. Imagine que las máquinas cuentan los votos pero nadie sabe como lo hacen. Ahora imagine que alguien descubre que estas máquinas son vulnerables a ataques, pero las agencias responsables no toman las medidas necesarias para hacerlas seguras. Si usted vive en U.S.A. no necesita imaginárselo. Esta es la realidad del voto electrónico en este país".

Por último U.S.A. tuvo una experiencia de voto remoto en 2.004 denominado SERVE [36] que fue desarrollado por el Departamento de Defensa para votar desde fuera del país. El sistema esperaba 100.000 votos en una primera fase para llegar a 6 millones, con un coste estimado de 24 millones de dólares. Después de un análisis de su seguridad por parte de David Jefferson [37] en el que se ponían en entredicho muchos de los aspectos de seguridad del sistema, el proyecto se detuvo.

Canadá sigue la estela de los EE.UU. en esta materia. Aunque a nivel federal no se utiliza el voto electrónico, sí se hace en las municipales y locales en algunas ciudades

[38] www.bravenewballot.org/
[36] http://servesecurityreport.org/
[37] www.ejfi.org/Voting/Voting-35.htm

desde 1.990. Carece de estándares pero utiliza los norteamericanos. Cada provincia escoge su tecnología y tiene sus propias normas.

Venezuela es un caso muy especial, ya que lleva muchos años utilizando con mayor o menor fortuna, el voto electrónico basado en DRE. Este país tuvo algún problema por el procedimiento de verificación del votante mediante lectura de huella dactilar con una máquina denominada "captahuellas" o "cazahuellas". Se plantearon problemas muy interesantes debido a la sospecha de que se pudieran relacionarse las listas de votantes al pasar en un determinado orden y el propio voto emitido en una DRE de la empresa Smartmatic, que se depositaba en orden secuencial. De forma, que en las elecciones del 2.005 se retiraron cautelarmente , pero se volvieron a utilizar en Diciembre de 2.006, argumentando que se había roto la secuencialidad utilizando un procedimiento de recolocado seudo-aleatorio en grupos de 10. El despliegue tecnológico en las elecciones de este país es uno de los más complejos, ya que además de las urnas que emiten un boleto en papel que se introduce en una urna convencional para proceder, en algún caso determinado por sorteo, a su recuento manual (verificación por papel) , también se utilizan las mencionadas máquinas "captahuellas" para verificar la identidad de los votantes mediante enlaces satelitales que permiten verificar en "tiempo real" este extremo. En cualquier caso el recuento resulta lento y complejo debido al diseño del mismo y a la necesidad de realizar la auditoria manual en alguna de las urnas.El proceso va siendo refinado en las sucesivas ocasiones mediante observaciones externas. [39]

Brasil aprobó en octubre de 1995 una nueva Ley Electoral en la que se definieron las directrices del voto electrónico con la intención de reducir el fraude electoral y minimizar el tiempo de escrutinio. La votación se lleva a cabo a través de una especie de cajero automático con una pantalla, en el que van apareciendo los candidatos y en la que los votantes pueden realizar su selección oprimiendo un botón. Al concluir la jornada electoral, se bloquea el equipo mediante una clave y se imprimen los resultados, a la vez que se obtiene una copia de los mismos sobre un soporte digital (disquete u otro) que se traslada inmediatamente a un Centro de Recuento para su tratamiento. La urna electrónica fue el único método de votación en las elecciones a presidente de la República en octubre de 2002 y fue empleado con éxito por 115 millones de votantes.

[39] www.eueomvenezuela.org

En **Méjico**, al igual que otros países, depende de los Institutos o Comisiones Electorales de los Estados la definición del uso de las diversas tecnologías para el voto. Los Estados de Coahuila, Distrito Federal y San Luis de Potosí tienen urnas electrónicas que ya han sido utilizadas en algunos procesos electorales. En este caso cabe destacar que los desarrollos son propios y los equipos son totalmente auditables . Estas sin duda son dos ventajas fundamentales que tienen pocos países. Únicamente , si se lograra la colaboración entre los diversos Estados y las Universidades, se podría mejorar el diseño y minimizar costes.

Australia empezó a utilizar máquinas de voto electrónico desde Octubre de 2.001 [34] en las elecciones parlamentarias, que las utilizaron más de 16.000 votantes. Posteriormente (2.006) el gobierno del Estado de Victoria introdujo en las elecciones estatales una prueba general con voto electrónico. Para este año la Comisión Electoral Australiana ha decidido introducir en 29 localidades el voto electrónico para que puedan utilizarlo 300.000 discapacitados visuales [41]. También se va a desarrollar otra prueba de voto remoto a la que tendrán acceso los militares y personal civil desplazado fuera del país en misiones oficiales. Por lo que sabemos el proceso está siendo llevado a cabo lentamente y con acierto. Es otro modelo a seguir.

India es un caso excepcional tanto por el número de electores , 668 millones, como por ser pionera en el uso del voto electrónico (¿alguien ha pensado en hacer papeletas para todos estos electores con la multitud de partidos políticos que se presentan?). Ya en el año 2.004 se distribuyeron por encima de un millón de EVM (*electronic voting machines)* que suministraron 2 empresas del propio país, con un diseño sobrio, un coste de fabricación reducido y de manejo sencillo. La puesta en marcha del voto electrónico en todo el país se hizo de forma paulatina y comenzó en 1.989. De esta forma se fue aprovechando la experiencia para aumentar año a año el número de máquinas. Este es un buen ejemplo de cómo hacer las cosas, sobre todo si tenemos en cuenta que el voto tradicional en este caso sería muy complejo por no decir inviable. Más que nunca tienen sentido las palabras de David L. Dill, que es catedrático de la Universidad de Stanford y presidente fundador de la asociación Verified Votting Foundation. En sus declaraciones

[34] Boughton C. *Maintaining democratic values in e-voting with eVACS* 2.005 Software Improvements

[41] www.aec.gov.au/Voting/e_voting/low_vision.htm

asegura que el verdadero propósito de unas elecciones no es que los ganadores asuman que han ganado, sino convencer a los perdedores que han perdido.[40]

El trabajo de los investigadores.

Desde el año 2.004 los esfuerzos de los investigadores de todo el mundo para conseguir mejoras en las características de los sistemas de voto electrónico se han incrementado de forma importante. Basta buscar en las bases de datos de los mejores sitios de investigación del mundo para darse cuenta. En este caso la información se buscó en IEEE, ACM , Elsevier y E-Voting.cc. Después de filtrada y organizada descubrimos que casi el 25% de los trabajos desde el 2.004 se centran en conseguir que el uso de Internet para el voto electrónico reúna todas las condiciones básicas enunciadas en el apartado de ventajas e inconvenientes . Después, con un 15% cada uno, están los relacionados con los diversos sistemas de criptografía para mejorar la seguridad de los procesos y los que tratan de los problemas de identificación del votante. Después con un 10% cada uno, aparecen las investigaciones sobre la mejora de las DREs y la propia gestión de los procesos electorales basados en tecnología. Por último, aparecen varios tipos de trabajos dispersos como: propuestas para solucionar la coerción y el soborno, procedimientos para análisis del código de las aplicaciones de voto electrónico y diseño de otros procedimientos de voto apoyados en tecnología. Repasemos las principales propuestas.

Mejora del voto por Internet.

En general la mayor parte de los autores proponen procedimientos basados en criptografía que aseguran el anonimato, unicidad del voto y verificabilidad del mismo, pero que no solucionan de forma simultánea otro tipo de problemas como el *no authorized proxy* que es la emisión de un voto de alguien que ha decidido no participar en los comicios [35] . Otro autor [36] propone una solución para este problema

[40] rules.senate.gov/hearings/2005/Dill062105.pdf
[35] Ray I. et al *An anonymous electronic voting protocol for voting over the Internet* 2.002 IEEE
[36] Baiardi F. et al *SEAS, a secure e-voting protocol: design and implementation*. 2.005 Elsevier

denominándolo SEAS. No obstante la propuesta no resuelve la compra de votos ni la trazabilidad de la dirección IP del voto por lo que proponen votar desde quioscos. Uno de los problemas más comunes y de más difícil solución es el que proviene del ataque por denegación de servicio, por lo que varios autores concluyen que Internet no es adecuado para el voto electrónico [37] . Otros autores dan soluciones más globales para el *i-vote* proponiendo verificación individual y de esta forma evitando teóricamente la extorsión y la compra del voto [38], además le añaden sistemas de intervención y de autoridad electoral, uso de tarjetas criptográficas para identificar al votante garantizando el anonimato del voto. Lo denominan Votescript. [39] Otro tipo de propuestas pasan por reconocer que Internet es de por si un canal inseguro y para minimizar esta realidad proponen soluciones novedosas, como el denominado *repeated vote-casting* , es decir la posibilidad de votar repetidamente y hacerlo sobre diferentes medios (Internet, urna electrónica, móvil, …) y que sólo cuente el último de los emitidos. Este procedimiento, que utiliza un sistema doble de cifrado simétrico, intenta evitar la posibilidad de compra y venta de votos y permite aumentar la confianza del votante respecto a la integridad del proceso electoral. [40] Quedan desechadas antiguas propuestas que estimaban suficiente el uso de canales seguros tipo SSL , ya que sirven para evitar la intrusión en el mensaje pero es insuficiente para certificar el emisor , el receptor y el propio mensaje. También hay una buena parte de las soluciones que sólo ofrecen modelos teóricos basados en criptografía, pasando por alto aspectos menos especializados pero de más compleja solución .[41] [42] [43]

Da la impresión que la mayor parte de los esfuerzos contemplan las posibles soluciones o mejoras parcialmente, debido probablemente a la complejidad de abordarlo globalmente. Por otra parte se constata que la mayor parte de las propuestas no se apoyan en el esfuerzo de otros, con objeto de desarrollar soluciones conjuntas en un

---

[37] Schryen G. *How security problems can compromise remote Internet voting systems*. 2.004 .E-Voting.cc
[38] Acker B. Van *Remote e-voting and coercion: a risk-assessment model and solutions* 2.003 E-Voting.cc
[39] Gómez Oliva A. et al *Contributions to tradicional electronic voting systems in order to reinforce citizen confidence*. 2.006. E-Voting.cc
[40] Skagestein G. et al *How to create trust in electronic voting over an untrusted platform* 2.006 E-Voting.cc
[41] Benaloh J. *Simple verifiable elections* 2.006 Microsoft Research
[42] Delaune S. *Coercion-resistance and receipt-freeness in electronic voting* 2.006 IEEE
[43] Dini G. *Increasing security and availability of an Internet voting system* 2.002 IEEE

tema tan complejo como el voto remoto utilizando Internet. Parece que una solución completa está lejos.

Identificación del votante

En este caso las propuestas están más unificadas y parece que hay un acuerdo tácito de no utilizar el uso de sistemas basados en la biometría [44] por los riesgos que comportan. Se recomienda el uso de tarjetas de identificación electrónica basadas en clave pública y privada, ya que estos sistemas de claves asimétricas permiten enviar la parte pública por cualquier canal sea o no seguro. Los mecanismos de anonimato mediante "firma ciega" [45] , que son complejos en su implementación, tienen el inconveniente de que el usuario no sabe lo que firma , aunque puede obtener un recibo impreso de su voto. Por tanto parece que la tendencia más razonable es identificar al votante mediante una tarjeta de identificación (con par de claves, pública y privada) que le permita utilizar cualquier medio , incluido el voto remoto. Un buen estudio a este respecto es el de Kofler [46] en el que matiza que muchos de los problemas del voto electrónico (secreto, personal y libre) son los mismos que los del voto por correo.

Criptografía para ocultar el voto

La parte más compleja del voto electrónico está en el núcleo del mismo, es decir en su esencia de secreto. Por tanto muchos de los estudios del voto electrónico se refieren al uso de la criptografía desde el mismo momento de votar hasta que se realiza el recuento. Todas las propuestas intentan cumplir, al menos teóricamente, con los requisitos de: secreto del voto, privacidad, exactitud, integridad del proceso, unicidad del voto (con matices [47]), legitimidad, sistema robusto y verificabilidad universal. Por todo ello las soluciones son complejas y variadas. [48] Algunos autores proponen esquemas criptográficos más sencillos basados en agentes *offline* que parecen cubrir todos los aspectos de seguridad con garantías. [49]

---

[44] Hof S. *E-voting and biometrics systems?* 2.004 E-Voting.cc
[45] Kang S. *A study on the electronic voting system using blind signature for anonymity* 2.006 IEEE
[46] Kofler R. et al *The role of digital signature cards en electronic voting* 2.044 IEEE
[47] Volkamer M., Grimm R. *Múltiple casts in online voting: analyzing chances* 2.006 E-Voting.cc
[48] Wang C. , Leung H. *A secure and fully private Borda voting protocol with Universal verifiability* 2.004 IEEE
[49] Sandikkaya M. , Orencik B. *Agent-based offline electronic voting* 2.006 IEEE

Estudios y propuestas sobre las DREs

Son importantes y serias las contribuciones en esta materia que aportan los investigadores, sobre todo de los EE.UU. En este caso las soluciones válidas son menos complejas, ya que procesos como el de la identificación y el recuento están desconectados de la red y se realizan aparte. En general los autores concluyen que las debilidades de los sistemas basados en las DREs no se deben a problemas técnicos , sino más bien al mismo procedimiento de los comicios .La mayor parte están de acuerdo en las ventajas de la copia impresa del voto, aún tenido en contra los problemas de usabilidad creados. Este tipo de soluciones son las recomendadas por el movimiento HAVA (ayuda a América a votar) en U.S.A. [50] También es cierto que hay científicos experimentados que niegan que estos equipos puedan ser utilizados, ya que un análisis a fondo del código fuente, deja en entredicho aspectos como el acceso no autorizado, uso inadecuado de los sistemas de cifrado, posibles vulnerabilidades si se conecta a la red y desarrollo de software de baja calidad [51] Sin duda es cierto , pero lo es sobre una máquina en concreto y en un momento determinado. Este tipo de trabajos son muy importantes para detectar las deficiencias y corregirlas y no para anular el resto de los esfuerzos sobre la materia. El análisis del código es realmente complejo, e incluso algunos expertos han llegado a decir que imposible si se quiere garantizar su fiabilidad y precisión al 100% [52] Pero está claro que en la tecnología no hay nada 100% fiable.

Gestión de los procesos electorales

Los papeles sobre investigación en voto electrónico dejan claro que la seguridad del voto depende de dos aspectos bien diferenciados: la parte técnica y el procedimiento. En general el segundo está más descuidado ya que se "heredó" de los procesos electorales clásicos por lo que algunos detalles son insuficientes para garantizar la seguridad en el voto electrónico. Por ejemplo, hay ausencia de suficientes procedimientos de control sobre los suministradores del equipamiento , sobre los encargados de la supervisión y es necesaria la mejora de los procesos en sí, así como formar al votante y a los agentes

[50] Fisher E. *The direct electronic voting machine (DRE) – Controversy* 2.005 Congressional Research Services
[51] Kohno T. et al *Análisis of an electronic voting system*
[52] Rubin A. *Brave new balllot* 2.006 Morgan Road Books

implicados y por último definir con claridad el papel de cada agente en el proceso electoral. [53] [54]

Según Lambridoudakis [55] concluyen en que los esquemas tradicionales de autenticación y autorización no cubren completamente los requisitos de seguridad del voto electrónico, por lo que es necesario ampliar estos modelos de autenticación y autorización ,de forma que regulen las acciones permitidas sobre el sistema. Para ello será necesario definir claramente los casos de uso, roles y permisos de cada participante en el proceso.

Otras propuestas

En otra serie de papeles menos habituales aparecen una serie de propuestas muy importantes para el desarrollo adecuado del voto electrónico.

Una de ellas, es la posibilidad de utilizar máquinas con "código abierto" (*open source)* y de esta forma facilitar la verificación del código por terceros, mejorando la verificación del sistema en general. Esto está siendo planteado por diversos países , evitando el efecto "caja negra" con el que las empresas entregan las urnas electrónicas. Dentro de esta posición hay varios desarrolladores que han propuesto soluciones "abiertas" que merece la pena estudiar . [56] Por último, un aspecto que cada día está adquiriendo mayor relevancia, la accesibilidad a la máquina, entendiendo esta como las facilidades dadas al colectivo de ciudadanos con alguna diversidad funcional o discapacidad (ceguera, visión deficiente, dificultades motoras , etc.). Esta también ha sido una de las recomendaciones del HAVA a los desarrolladores de máquinas DREs y está siendo tomada en consideración en la mayor parte de los países. [57] Este es uno de los aspectos en los que el voto electrónico tiene claras ventajas sobre el voto tradicional.

---

[53] Xenakis A. *A generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process* 2.006 E-Voting.cc

[54] Xenakis A. *Procedural security in electronic voting* 2.006 E-Voting.cc

[55] Lambridoudakis C. et al *Electronic voting systems: security implications of the Administrative Workflow* 2.003 IEEE

[56] Keller A. *A PC-based open-source voting machine with an accesible voter-verifiable paper-ballot* 2.005 USENIX Association

[57] Hernson P. *The importance of usability testing of voting systems*. 2.006 University of Maryland

La importancia de los estándares

Primero las recomendaciones y posteriormente los estándares son de una importancia vital para organizar el uso adecuado y normalizado del voto electrónico en todo el mundo. Lo que ocurre es que difícilmente se puede recomendar y mucho menos fijar unos estándares si previamente no se tiene experiencia suficiente, de ahí la importancia de las pruebas y de su análisis. Intentar fijar unas estándares a cumplir, antes de haber experimentado o bien utilizando la experiencia de los demás, puede ser un desastre en cualquier tipo de desarrollo o innovación.

Como ya hemos comentado anteriormente la Comisión de Ministros del Consejo de Europa presentó en Septiembre de 2.004 unas recomendaciones para el voto electrónico. Nadie duda del trabajo desarrollado y de la importancia que tienen, sobre todo en una agrupación de países tan compleja como la Unión Europea. Esto se hizo después de que varios países desarrollaran pruebas a todos los niveles y se llevaran a cabo estudios sobre el tema. A pesar de todo, las recomendaciones realizadas por un grupo de expertos han sido criticadas debido a la pobre expresión de sus contenidos y la necesidad de mejorar la forma en que se expresan. Es probable que una simple reestructuración sea un buen comienzo para el proceso de mejora. [58] Por otra parte , como cualquier otro tipo de recomendación, esta debe ser optimizada obteniendo información sobre su aplicación en las pruebas de los diversos países. Sin duda es un punto de partida.

Por otro lado, es importante destacar el caso de los EE.UU. de América, en el que la Comisión Electoral Federal y posteriormente la EAC (Comisión de ayuda a la elecciones) determinaron unos estándares que no expresan un conjunto coherente de requisitos para los sistemas de voto electrónico. Por esta razón las certificaciones que se han obtenido bajo este estándar han sido defectuosas. “Sin un modelo de los riesgos y del sistema, los estándares de votación no pueden asegurar la integridad ni la exactitud del proceso de votación” , concluye un trabajo de Earl Barr [59]. La moraleja de esta opinión se apoya en que nadie puede verificar que un sistema no tiene defectos, incluso si todo el código fuente de la aplicación de voto está disponible. Esta es la misma opinión que la expresada por Avin Rubin y su equipo. Es cierto que es bueno aplicar la duda metódica en cualquier proceso y más en este, pero no es menos cierto que si se

[58] McGaley M. , Gibson J.P. *A critical análisis of the Council of Europe Recommendations on e-voting*. 2.005 NUI Maynooth (Ireland)

[59] Barr E. , Bishop M. , Gondree M. *Fixing Federal E-voting standards* 2.007 Communications of the ACM

aplican herramientas y procesos de diseño del software involucrado en un proceso electoral de forma correcta, el resultado no tiene porque ser defectuoso. Por otra parte como decía David Hume: "Afirmaciones extraordinarias requieren evidencias extraordinarias". De esta forma podemos estar de acuerdo con los que concluyen que el sistema de voto perfecto no existe, como tampoco existe en ninguna otra aplicación de la tecnología. En cualquier caso, estamos de acuerdo en que es necesario volver a escribir los estándares pensando en los riesgos, en colaboración con los fabricantes, la Administración, los expertos en ordenadores ,así como los ciudadanos y de esta forma delimitar los riesgos contra los que sería necesario protegernos. Es necesario ir más allá del camino que se ha utilizado hasta ahora para abordar el diseño de los sistemas de voto electrónico y utilizar técnicas de alta precisión para garantizar que estos cumplan con las garantías necesarias.
La definición de los estándares en el voto electrónico es uno de los temas más complejos y una asignatura pendiente en todo el mundo.

Intereses comerciales en el voto electrónico

En la mayoría de los países que utilizan el voto electrónico, han estado presentes, de una u otra forma, las empresas que desarrollan, fabrican o venden servicios relacionados con este. En ningún caso vamos a valorar sus desarrollos o su trabajo, que sin duda ha sido esencial para el aumento de las experiencias en todo el mundo, pero creemos que hay también otras opciones que no tienen por que ser incompatibles. En algunos países , por ejemplo U.S.A. , las investigaciones punteras, por ejemplo los centros de excelencia en materia de seguridad interna (*Homeland security*) e incluso en otros ámbitos menos críticos, se lleva a cabo en las Universidades de primera línea en colaboración con el Gobierno. Esta unión entre Universidades, centros de Investigación y Gobierno, pueden dar resultados espectaculares en el avance de las técnicas de voto electrónico. Otro caso sería dejar a las empresas su comercialización y distribución. De esta forma el diseño no estaría determinado por parámetros comerciales y podría estar más abierto a la revisión e inspección de terceros, es decir se le dotaría de transparencia. Tenemos que evitar los conflictos entre lo comercial y lo democrático . Los problemas de los secretos de empresa, patentes, derechos adquiridos, etc. ,no deben afectar a nuestra democracia.

Como concluye Margaret McGaley: “negocios hay muchos, pero democracia solo una”[60]

Otras posibilidades del voto electrónico

Es fácil imaginar un escenario en el que las infraestructuras desplegadas para el voto electrónico remoto se convirtieran en permanentes, en una especie de “infraestructuras estratégicas” para conocer la opinión de los ciudadanos de forma continua . Es evidente que esto cambiaría muchos aspectos políticos y sociales que están fuera del ámbito de este trabajo, pero sería una forma de rentabilizar socialmente el coste de estas infraestructuras tecnológicas.

Por otra parte está claro que el voto electrónico es utilizado hoy en día, en otros usos fuera del voto legislativo, en entornos como el empresarial, financiero, asociativo, universitario, organizativo, etc. Una de las principales ventajas es que los requisitos necesarios no son , en principio, tan elevados como en el primero por razones obvias de mantenimiento de los principios democráticos (aspecto crítico sin duda) [61]

Conclusiones

Es fácil apreciar la falta de sinergia a la hora de desarrollar sistemas de voto apoyados en la tecnología. Una de las consecuencias es la diversidad de soluciones presentes en el mercado, no sólo en el plano tecnológico si no también en el de los procedimientos de gestión de los comicios.

Es importante realizar un análisis comparativo de las experiencias obtenidas en:

- proyectos piloto privados
- países que ya han introducido el voto electrónico
- países con administraciones electorales con pruebas avanzadas
- trabajos de investigación de las diversas Universidades y centros de desarrollo
- empresas del sector

[60] McGaley M. , McCarthy J. *Transparency and e-voting democratic vs. Comercial interests* 2.004 NUI Maynooth (Ireland)

[61] Rüdiger G. et al *Security requirements for non-political Internet voting* 2.006 E-Voting.cc

Los pasos recomendables para implementar las técnicas de votación electrónica deberían ser:

- aclarar que el voto electrónico un medio más y por tanto opcional
- comenzar con grupos identificados, que por alguna razón no participan habitualmente (discapacitados, problemas de desplazamiento, …)
- utilizar sistemas con un diseño sencillo, que permita su uso por parte de cualquiera con un mínimo de entrenamiento
- dar este entrenamiento a usuarios y gestores
- ir paso a paso analizando las fortalezas y debilidades del sistema

En las primeras fases del paso al voto electrónico conviene mantener la presencia de los votos en papel. En las últimas fases es importante diseñar pensando en la movilidad, evitando las restricciones de espacio y tiempo.

Es muy recomendable poner en marcha reuniones, foros, mesas de trabajo entre estados y naciones con objeto de intercambiar información y experiencias que ayuden en el desarrollo adecuado del voto electrónico.

Todo desarrollo en esta materia a de ser considerado en el contexto que está situado y tener presentes las cuatro dimensiones: legal, política, social y tecnológica. También hay que considerar desde el comienzo el nivel del proyecto que se pretende desarrollar.

Es necesario desarrollar un esfuerzo importante por partes de los investigadores, apoyados por su Gobierno, en realizar comparativas serias y reales entre la seguridad de los sistemas tradicionales de voto y los basados en tecnología, con el fin de fijar el nivel de seguridad aceptable dentro de criterios democráticos. Tener en cuenta que otros canales de participación, como el voto por correo, tampoco son fiables, pero consideramos más esencial facilitar el acceso a la urna que los criterios extremos de seguridad que se intentan imponer al voto electrónico y que no existen en otros canales.

En los sistemas de voto tradicional se producen pequeños errores de forma continuada y el uso de la tecnología puede incrementar estos errores de forma muy importante. Para evitarlo conviene ir paso a paso y en una primera etapa utilizar técnicas de verificación por parte del votante como las de papel. La tecnología bien usada y desarrollada puede convertirse en un aliado poderoso para reducir los riesgos.

Intentar convencer a la gente que las máquinas son seguras no es la mejor forma de introducir el voto electrónico. Es preferible hacer todo el proceso “transparente” desde

el comienzo y asegurarse de dotar a las urnas de mecanismos de recuento fiables, rápidos , claros y verificables.
Es imprescindible utilizar sistemas que permitan auditorias mediante verificación por parte del votante y que estas reúnan condiciones de accesibilidad.
Una de las facetas más descuidadas del diseño es la usabilidad y es básica para evitar el voto nulo.
Como este tipo de soluciones de voto están apoyadas en computadores , para conseguir un desarrollo con éxito de los estándares, tenemos que contar necesariamente con los tecnólogos , científicos, ingenieros y matemáticos.
Facilita enormemente el voto en urna electrónica y el voto por Internet, el uso de tarjetas de identificación del votante con parámetros biométricos y soporte para claves asimétricas.
Los mayores expertos en tecnología reconocen que esta tiene dificultades y limitaciones en campos como la privacidad, seguridad y libertad. Después de 30 años de mejoras en la criptografía alguno de los investigadores están cambiando de punto de vista y dicen que hay que reconocer la realidad de las "estructuras sociales" en contra del ideal de la verdad única de la física y las matemáticas.
Conviene dejar claros los riesgos en la seguridad del votación electrónica , sin caer en extremos. Es muy aconsejable utilizar "código fuente abierto" en los desarrollos y máquinas "transparentes" para facilitar las inspecciones y certificaciones. Se desaconseja el uso de equipos con estructura de "caja negra".
Con la experiencia adquirida es necesario abordar el desarrollo de estándares serios que permitan certificaciones fiables.
De las experiencias mundiales podemos sacar alguna conclusión:

- No hay tendencias únicas en el voto electrónico, incluso en los países con más experiencia.
- Los países que han intentado implementar sistemas a gran escala, sin debate previo ni transparencia suficiente, se han encontrado con la posición de varios sectores.
- Se producen cambios de opinión de forma continua en este tema, lo que demuestra que no ha sido introducido correctamente.
- En muchos países no se han resuelto algunos de los aspectos del voto electrónico (legal, tecnológico, social, político) debido a que no se ha explicado claramente los ventajas y el interés público.

- Los mejores desarrollos se han obtenido gracias a una estrecha colaboración y entendimiento mutuo entre los expertos tecnológicos y los jurídicos, para posteriormente incluir a los legisladores, políticos y público en general.

Recordar que todo es cuestión de confianza (¿no confiamos en los medios de pago electrónicos, porque nos lo han demostrado?).

Fuentes de información

Bibliografía:

- Rubin , Aviel D. *Brave new ballot* . New York , 2.006 Morgan Road Books
- Alvarez, R. Michael , Hall , Thad E.*Point, clic and vote. The future of the Internet voting*. Washington, D.C. , 2.004 . The Brookings Institution
- Krimmer, Robert (Ed.) *Electronic voting 2.006 (Proceedings)*. Bregenz (Austria), 2.006 GI-Edition

Enlaces en Internet:

- http://www.eucybervote.org/reports.html
- http://www.electoralcommission.org.uk/elections/modernisingelections.cfm
- http://www.informationhere.info/internet-estonia.htm
- http://www.wired.com/politics/security/news/2007/03/72846
- http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/01_recommendation/04E-voting%20Rec%20Spanish%20-Traducci%C3%B3n%20Rec%202004%2011%20Comit%C3%A9%20Mins%20Consejo%20Europa.asp
- http://en.wikipedia.org/wiki/2004_United_States_presidential_election_controversy%2C_voting_machines#Specific_issues_relating_to_Diebold_machines_and_practices
- http://www.verifiedvotingfoundation.org/article.php?id=6289
- http://www.bravenewballot.org/praise/
- http://avi-rubin.blogspot.com/
- http://evoting.twoday.net/
- http://www.vote.caltech.edu/links
- http://lorrie.cranor.org/voting/hotlist.html
- http://www.j-dom.org/h/n/LINKS/evoting/ALL///

- http://lorrie.cranor.org/voting/hotlist.html
- http://premium.vlex.com/actualidad/especiales/Voto_Electronico/2500-VEL,05.html
- http://www.dosdoce.com/voto.htm
- http://www.edemocracia.com/biblioteca/jornadas/escorial.html
- http://evoto.org/index.php?id=pufs&texto=PUF%20(FAQ)...&pinta=pufs
- http://www.oea-rite.org/PagEst_Not_VEOtroPais.htm
- http://www.essvote.com/HTML/home.html
- http://avirubin.com/vote/
- http://evoting.twoday.net/
- http://www.odpm.gov.uk/index.asp?id=1133623
- http://www.social-informatics.net/evoting.htm
- http://www.social-informatics.net/evotingnews.html
- http://grouper.ieee.org/groups/scc38/1583/index.htm
- http://www.eucybervote.org/publications.html
- http://www.sos.cs.ru.nl/research/society/voting/index.html
- http://www.votescam.com/Marylandevoting.php
- http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html
- http://www.upassoc.org/upa_projects/voting_and_usability/uk-evoting.html
- http://www.propolisclub.net/experiencias.asp?tematica_id=5
- http://www.deliberate.com/w4g/conf97/fullfreedom.html
- http://www.deliberate.com/index.html
- http://www.edemocracy.gov.uk/default.htm
- http://www.edemocracy.gov.uk/glossary.htm
- http://www.mla.gov.uk/
- http://www.cs.ut.ee/~lipmaa/crypto/link/protocols/voting.php
- http://ksghome.harvard.edu/~pnorris/Articles/Articles%20conference%20papers.htm
- http://www.notablesoftware.com/evote.html
- http://www.bluescreendemocracy.org/archive/1988/aug/saltman.php
- http://lorrie.cranor.org/
- http://www.win.tue.nl/~berry/
- http://www.vototelematico.org/

- http://www.venezolano.web.ve/archives/733-Informe-de-la-OEA-sobre-elecciones-parlamentarias-en-Venezuela.html
- http://www.cne.gov.ve/noticiaDetallada.php?id=3608
- http://avirubin.com/vote/response.html
- http://www2.diebold.com/checksandbalances.pdf
- http://www.fec.gov/hava/hava.htm
- http://www.ss.ca.gov/elections/elections_vst_summit.htm
- http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf
- http://xw2k.sdct.itl.nist.gov/lynne/votingProj/main.asp
- http://www.nsrl.nist.gov/vote.html
- http://vote.nist.gov/
- http://www.eucybervote.org/reports.html
- http://www.geneve.ch/evoting/english/welcome.asp
- http://www.eac.gov/election_resources/vss.html
- http://www.eac.gov/voting_standards.asp
- http://enight.dos.state.fl.us/dreinfo/dreinformation.shtml
- http://grouper.ieee.org/groups/scc38/
- http://www.cev.ie/htm/report/view_report.htm
- http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/
- http://guidelines.kennesaw.edu/vvsg/intro.asp
- http://guidelines.kennesaw.edu/vvsg/glossary.asp
- http://www.eac.gov/voting_sys_cert.htm
- http://www.vototelematico.org/
- http://vote.nist.gov/
- http://infodoc.escet.urjc.es/ted/
- http://www.eueomvenezuela.org/contacto.html
- http://www.w3c.es/Eventos/2007/eGov/
- http://www.votoelectronico.pt/index.php?option=com_content&task=category&sectionid=6&id=79&Itemid=84
- http://www.brunazo.eng.br/voto-e/textos/index.htm
- http://www.whitehouse.gov/pcipb/
- http://habitat.igc.org/wealth-of-networks/ch-07.htm

- http://www.infosentry.com/US_Public_Opinion_Toward_Voting_Technology_20040301.htm
- http://arstechnica.com/articles/culture/evoting.ars/1
- http://www.wheresthepaper.org/BrennanCtr11_16FullFace.htm
- http://www.cibersociedad.net/textos/articulo.php?art=72
- http://www.ordinateurs-de-vote.org/About-us.html
- http://www.wijvertrouwenstemcomputersniet.nl/English
- http://aceproject.org/ace-en/focus/e-voting/countries
- http://www.social-informatics.net/evoting.htm
- http://www.electoralcommission.org.uk/
- http://www.votoelectronico.es/