VOTO ELECTRÓNICO POR INTERNET Y RIESGOS PARA LA DEMOCRACIA (II)

LUIS MIGUEL GONZÁLEZ DE LA GARZA

SUMARIO

Fecha recepción: 1.02.2009
Fecha aceptación: 19.10.2009

VOTO ELECTRÓNICO POR INTERNET Y RIESGOS PARA LA DEMOCRACIA (II)

POR

LUIS MIGUEL GONZÁLEZ DE LA GARZA

Doctor en Derecho Constitucional
(UNED)

Como continuación de la primera parte de nuestro artículo, en esta segunda sección consideramos aquellos elementos de naturaleza sistemática que entendemos de mayor relevancia en relación con el sufragio electrónico remoto o por Internet, así como las conclusiones de la primera y la segunda parte del estudio.

4. EXPERIENCIAS DEL VOTO ELECTRÓNICO REMOTO

En nuestro estudio hemos contemplado el análisis de tres experiencias de voto electrónico. En primer lugar, hemos considerado la experiencia de voto electrónico en Estonia[1]. El esquema fundamental del proceso de sufragio electrónico remoto es conceptualmente sencillo: un ordenador personal doméstico,

[1] Normas fundamentales sobre el voto electrónico remoto: **1**) *Riigikogu Election Act,* 12.06.2002.(RT I 2002, 57, 355) y (RT I 2006, 30, 231), arts. 44 Electronic voting y 48 Counting of electronic voting; **2**) *Local Government Council Election Act,* 27March 2002. (RT I 2002, 220), art. 43 Electronic voting; **3)** *President of the Republic Election Act,* 10 April 1996. (RT I 1996, 30, 595); **4**) *Referendum Act,* 13 March 2002. (RT I 2002, 30, 176), art. 37 Electronic voting; **5)** *European Parliament Election Ac*t, 18 December 2002.(RT I 2003, 4, 22).

del titular del derecho de sufragio, con conexión a Internet, solicita de las autoridades electorales estonas su registro para votar on-line. La autoridad de registro electoral, valida tal registro y el votante, dentro de los plazos legales al efecto procede a emitir su voto mediante una conexión telemática con el servicio Web electoral para las elecciones parlamentarias Estonas. El votante, como en una página Web normal, selecciona su opción de sufragio y vota, el servicio Web, le informa de que ha votado correctamente y concluye así la experiencia de voto. Las acciones anteriores, naturalmente muy resumidas, se hacen posibles merced a una tarjeta de identidad con chip criptográfico que poseen los ciudadanos Estones, amén de un lector de tarjetas que les es facilitado a los votantes por la Administración Electoral, para que el votante lo instale en su ordenador personal, junto con el software electoral apropiado.

Ahora bien, ¿se encuentra el ordenador *privado* del votante libre de software malicioso, virus, gusanos, troyanos, rootkits, o *sniffers,* que permitan garantizar jurídicamente que el sufragio ha sido libremente determinado, o éste ha podido ser modificado por una aplicación maliciosa instalada previamente en el ordenador del titular del derecho de sufragio? ¿Cómo puede la Administración Electoral verificar que el software electoral —que la misma proporciona vía remota, es decir, suministrado a través de un medio de comunicación completamente inseguro como es Internet— se ha instalado y configurado correctamente; que, a su vez, no entra en conflicto con ninguna otra aplicación residente en el ordenador del titular del derecho al voto, o que, finalmente, no está siendo obligado ese *software electoral a seguir un curso de acción indeseado,* debido a la actividad fraudulenta de software malicioso? Supongamos que el software electoral funciona correctamente y que ha sido debidamente instalado, ¿garantizaría ese proceso la integridad del sufragio? ¿Cómo puede la Administración Electoral asegurar que el votante que mantiene con aquella una comunicación electoral, es el legítimo titular del derecho al voto? ¿Cómo se respeta y garantiza, en estos supuestos, el denominado *principio de personalidad del voto*? Un hijo podría votar por su padre, con o sin su conocimiento, tan sólo haciendo uso de la tarjeta de identificación de su padre, supuestos ambos en los que el voto habría sido registrado válidamente por la Administración Electoral con pérdida del sufragio del legítimo titular. O mujeres a las que sus maridos les privasen del voto mediante la utilización de sus tarjetas de identificación, en nuevas fórmulas de violencia doméstica ¿De qué forma se garantiza el secreto si en un mismo ordenador votan varias personas con derecho al voto?

La mayoría de las preguntas enunciadas carecen de solución, o más precisamente, de una solución que resuelva el problema que se plantea de forma «*óptima*». Si como señalara sensatamente Burdeau: «*toda complicación es un vicio en*

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

materia electoral»[2], nos hallamos en presencia de sistemas transidos de vicios de muy diversas especies. A partir del momento en el que nos alejamos de las soluciones óptimas por otras que lo son menos o, sencillamente, no lo son en absoluto. En ésta expresión se residencian muchos problemas relevantes en relación con el sufragio electrónico. En efecto, podemos afirmar que una solución a un problema no es óptima cuando disponemos de un modelo funcionalmente equivalente en el que la situación que se resuelve sí lo es, así, por ejemplo, si estudiamos el secreto del sufragio que representa la introducción de un sobre electoral en una urna convencional y exponemos tal fórmula como aquella que es capaz de disociar completamente la relación que vincula el sentido del sufragio con su autor, dispondremos de una solución óptima, apropiada para que cualquier otra fórmula de sufragio alcance un óptimo idéntico o superior al examinado. Si cualquier técnica electrónica hace posible la reconstrucción del sentido del sufragio, asociándose éste a sus titulares, las garantías técnicas se encontrarán por debajo de las exigencias que la técnica presencial es capaz de satisfacer, destruyendo por completo —en tal modalidad de sufragio—, la determinación de tal acto de voto. En el primer supuesto, nos encontramos ante la adecuación entre un principio jurídico y una técnica que nos permite afirmar que garantiza absolutamente el secreto del sufragio, en la segunda manifestación, por el contrario, la adecuación entre el principio y su plena optimización es débil y el secreto se puede destruir mediante la reconstrucción de los datos que asocien sentido del voto y titular del mismo.

El sistema de voto electrónico remoto Estonio, como todos los sistemas de voto electrónicos, no puede ser considerado desde una perspectiva ingenua o no técnica. Cada uno de los elementos que hemos considerado como una secuencia integral y ordenada de actividades, en realidad, esconde una descripción técnica compleja que subyace a ésta y la hace más o menos segura en virtud de diversas consideraciones que se hayan tenido en cuenta para su desarrollo. Así, los límites de seguridad de cada tecnología participante, las metodologías empleadas en los diseños de las comunicaciones, el tipo de software electoral desarrollado, su calidad, control y supervisión, el tipo de errores que puedan producirse directamente o en la interrelación con otras aplicaciones, etc., son factores que definen la seguridad e integridad del proceso de sufragio en su conjunto.

Un diseño de voto electrónico *remoto,* bien desarrollado, es un reto de una gran complejidad y en el que, de partida, hay que renunciar a obtener una *fiabilidad equivalente* a la de un proceso de sufragio presencial. Dadas, tan sólo, las

[2] G. Burdeau,«*Derecho Constitucional e Instituciones Políticas*», Editora Nacional, Madrid, 1981, Pg. 182.

características nativas de las tecnologías inseguras en presencia, cuando se estudian en detalle tales experiencias empíricas de sufragio se aprecia que se han elaborado, en primer lugar, *en una especie de vacío jurídico* (creándose normas *ad-hoc* muy abiertas, una especie de *remisiones en blanco* a la normativa técnica sin más, como se aprecia en el supuesto de las normas electorales Estonas, en materia de sufragio electrónico remoto, lo que *no sucede* desde luego con la regulación jurídica del voto electrónico *presencial* en los Estados Unidos, Acta HAVA). Posteriormente se observa que se han elaborado con métodos de garantía insuficientes o claramente deficientes y que, tras una aparente consistencia publicitaria del proyecto, existen verdaderas lagunas de inseguridad en las que, finalmente, las mejores prácticas y el interés general son descuidados por razones comerciales. Esto sucede en la experiencia piloto de sufragio electrónico en relación con el referéndum sobre el Tratado por el que se establece una Constitución para Europa, como comentamos con detalle en el estudio que se desarrolló por el Observatorio de Voto Electrónico de la Universidad de León. También se produjo en el sistema norteamericano de voto electrónico denominado SERVE[3], así como en el reciente proyecto IVAS[4]. En cada uno de estos programas, la buena voluntad superó ampliamente a las posibilidades técnicas, fruto de lo cual se abrieron graves brechas de seguridad en el proceso de voto electrónico, con lo que la seguridad e integridad del mismo se vió sacrificada. No es por ello posible construir alternativas al voto presencial basadas en *el voluntarismo*, ya que, generalmente, conducen o pueden conducir a sufrir experiencias desastrosas.

El proyecto desarrollado en España y que estudió con todo detalle y rigor académico el observatorio para el voto electrónico (OVSE) de la Universidad de León, demuestra que la falta o ausencia de pautas descriptivas de lo que un proceso de sufragio «*debe ser*» conducen a que la industria proporcione herramientas destinadas inicialmente a cubrir esa supuesta necesidad, el «*ser*». Sin embargo, ésta es precisamente la metodología más incorrecta de abordar la aproximación a los fenómenos de voto electrónico y se demuestra con ello,

[3] SERVE es el acrónimo de «Secure Electronic Registration and Voting Experiment». Realizamos un comentario extenso de este sistema, desarrollado por el SPRG (Security Peer Review Group), grupo de expertos seleccionados por el FVAP (Federal Voting Assistance Program) para el análisis del programa de voto, para el Departamento de Defensa y el Gobierno de los Estados Unidos. Su director Aviel D. Rubin (Universidad Johns Hopkins) nos ha autorizado en la investigación a traducir, publicar y comentar su estudio.

[4] Department of Defense: Expanding the Use of Electronic Voting Technology for UOVACA citizens. As Required by Section 596 of the National Defense Authorization Act for Fiscal year 2007, Do. 4000 Defence Pentagon, Washington D.C., May 2007.

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

cómo cuando la dirección de ajuste sigue la dirección: *tecnologías disponibles – sistema electoral*, los principios esenciales de transparencia, objetividad, integridad, neutralidad y legitimidad, quedan dañados o desconocidos gravemente. El proyecto SERVE, por su parte, comparte con el proyecto español la dirección de ajuste *tecnología disponible – sistema electoral,* razón que justifica en amplia medida su fracaso. Telegráficamente diremos que el sistema SERVE pretendía ser una herramienta de sufragio electrónico remoto que empleaba Internet como medio de comunicación entre los votantes y las diversas administraciones electorales federales, en las que los votantes se encontraban censados y registrados para el sufragio. La idea que se deseaba alcanzar con el programa era que los militares y personal de servicio no militar dispusieran de la capacidad operativa de sufragio desde cualquier lugar del mundo a través del proyecto de voto electrónico remoto. Ahora bien, una vez que empezó a analizarse científicamente el conjunto de instrumentos en los que consistía el sistema de sufragio, pudo confirmarse —como exponemos detalladamente en el estudio— que las soluciones adoptadas abrían muy importantes brechas de seguridad para la integridad del proceso de voto, de forma que el proceso podría ser fácilmente manipulado desde las perspectivas que se detallan en el estudio, y que no podemos considerar aquí. Naturalmente, y tras poner de manifiesto los defectuosos instrumentos en que consistía el sistema de voto, el Gobierno no tuvo más remedio que suspender y retirar el programa, ya que su funcionamiento habría expuesto el sufragio de los titulares del derecho al voto a riesgos potenciales y amenazas, que hacían del programa experimental un sistema mucho más vulnerable a la manipulación fraudulenta que el simple voto por correo postal. Algunos de los errores detectados fueron:

a) Los sistemas DRE´s (registro electrónico directo) han sido ampliamente criticados por deficiencias de seguridad y vulnerabilidades.

b) El software que gestionaba todos los procesos de SERVE era totalmente cerrado y propietario.

c) El software fue insuficientemente analizado durante las fases de *cualificación* y *certificación* (fases, por otro lado, reguladas jurídicamente de modo defectuoso).

d) El sistema era especialmente vulnerable a diversas formas de ataque.

e) Los sistemas DRE´s no fueron sometidos a auditorias que asegurasen, entre otras cosas, la confidencialidad del proceso de votación.

f) En adición a lo anterior, y debido a que SERVE era un sistema basado en PC´s convencionales o domésticos, por lo tanto su seguridad era muy reducida, y por otra parte, en Internet existen numerosos problemas de seguridad funda-

mentales que hacen del sistema una herramienta vulnerable a una amplia variedad de bien conocidos defectos de seguridad, entre los cuales se encuentran:

— Ataques desarrollados por parte de personal interno de las empresas constructoras de los múltiples sistemas de los que se componen tales procesos.
— Ataques de denegación de servicio DoS[5].
— Suplantación de identidad/personalidad —*spoofing*—.
— Compra venta de votos automatizada (a gran escala).
— Ataques de virus y código malicioso a los sistemas basados en PC´s.

La retirada del programa fue la conclusión lógica de la puesta de manifiesto de las vulnerabilidades detectadas por el equipo de evaluación de seguridad. Se pretendió emplear tecnologías económicas, fácilmente disponibles e inadecuadas, para un proceso en el que tan sólo empleando tecnología especializada y muy sofisticada —*lo que supone además prescindir de Internet como red de comunicaciones*— se hubiese podido desarrollar algún tipo de modalidad de voto experimental; el hecho, finalmente, es que no fue así. Pese a desechar aquel proyecto, el Gobierno de los Estados Unidos, a través del departamento de defensa, presentó recientemente el programa IVAS (*Integrated Voting Alternative Site*). La idea que lo anima es la misma que en el proyecto SERVE, pero simplificando algunos aspectos de seguridad que lo hacen tan crítico para la integridad del proceso de sufragio como el sistema SERVE. En tal sentido se pronunciaron David Jefferson (Lawrence Livermore National Laboratory), Aviel D. Rubin (Johns Hopkins University) y Barbara Simons (IBM Research former President). El informe de estos reputados expertos —que consideramos extensamente en nuestro estudio— está persuadiendo actualmente al Gobierno de los Estados Unidos para su retirada definitiva[6].

Los problemas observados sucintamente, de naturaleza tecnológica, están actualmente bien identificados —son el fundamento— de todos los estudios que se manifiestan, tanto en máquinas de voto presencial, como en máquinas de voto remoto. Las regulaciones jurídicas en los Estados Unidos han sido incapaces de prescribir regulaciones que se dirijan directamente a neutralizar las inadecuaciones técnicas, ya que el enfoque metodológico de libre mercado es un enfoque *con*

[5] Sobre este tipo de ataques de «*bloqueo de redes por saturación*» puede verse: Stephen Northcutt. Judy Novack, «*Detección de intrusos*», Guía avanzada, 2ª Edición, Prentice Hall, 2001, Madrid, Págs. 260-275.

[6] Estos autores fueron los creadores del estudio SERVE, los cuales lograron que el Departamento de Defensa y el Gobierno acordase retirar el programa, como ya se ha señalado.

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

dirección de ajuste tecnologías disponibles-sistema electoral. La ruptura de este enfoque puede mitigar, en parte, los problemas de seguridad actualmente bien comprendidos y estudiados. La Recomendación del Consejo de Ministros, que veremos seguidamente, adopta una dirección de ajuste correcta, en sus elementos normativos fundamentales: *sistema electoral-tecnología disponible.*

5. RECOMENDACIÓN DEL CONSEJO DE MINISTROS SOBRE LAS NORMAS LEGALES OPERATIVAS Y TÉCNICAS PARA EL VOTO ELECTRÓNICO, DE 30 DE SEPTIEMBRE DE 2004

Europa, con el desarrollo de esta Recomendación, ha afrontado el desafío jurídico y técnico del voto electrónico de un modo, a nuestro juicio, ejemplar. Hay que señalar, no obstante, que la Recomendación tiene como precedente en los EE.UU., el Acta de Ayuda a votar al votante americano (Help America Vote Act, Public-Law 107-252 107th, de 29 Oct. 2002, H.R.3295). Precedente que se pone de manifiesto en la adopción, por la Recomendación europea, de soluciones ensayadas precisamente en el Acta Hava. El Acta Hava tuvo como propósito fundamental regular jurídicamente la ordenación de lo que podríamos denominar: *una remodelación esencial* del sistema de voto electrónico norteamericano, en el sentido de que la misma tuvo por objeto recepcionar y ordenar la regulación de las máquinas de voto electrónico de *tecnología digital*, en sustitución de las tecnologías electro-mecánicas. En general, el Acta, hasta la fecha, ha desarrollado su cometido con un grado relativamente bajo de eficiencia, no ha sido capaz de asegurar la integridad del voto, razón por la que en estos momentos se debate en el Senado de los Estados Unidos dos legislaciones de enmienda concurrentes, la *Ballot Integrity Act of 2007*, promovida fundamentalmente por el congresista Rush Holt y otros, así como la *Voter Confidence and Increased Accessibility Act of 2007*, patrocinada por la Senadora Dianne Feinstein. Ambos proyectos tratan de corregir los efectos más indeseables del Acta Hava, ya que la misma ha generado una profunda preocupación en los EE.UU., debido a su insuficiente regulación, fundamentalmente, de los procesos de certificación, descertificación y recertificación de las tecnologías de voto, así como debido a su incapacidad legal para promover, con el debido detalle y rigor, la inspección exhaustiva de las tecnologías de voto electrónico (software y hardware electoral, entre otros aspectos importantes).

La Recomendación Europea es un texto que parte de una posición ventajosa con respecto al Acta Hava y, en ese sentido, su capacidad de regular procesos de sufragio electrónico presenciales y remotos es más congruente con los principios a los que debe adaptarse el régimen electoral electrónico. Por otra parte,

trata los aspectos centrales sobre los que en un futuro se basarán las legislaciones nacionales, con una aproximación prudente y no desconocedora, en ese sentido, de la complejidad que implica un desarrollo de la naturaleza que supone la recepción de los modelos de sufragio electrónico. Así, establece la letra i): *El e-voting (voto electrónico en adelante) deberá respetar todos los principios de las elecciones democráticas y referéndum. El voto electrónico deberá ser tan fiable y seguro como las elecciones democráticas y referéndum en las que no se empleen medios electrónicos. Este principio general abarca todas las cuestiones electorales, tanto si se mencionan o no en los apéndices.*

La prescripción que consideramos, como principio hermenéutico general, que afecta a toda la Recomendación, nos parece del máximo interés y valor, ya que obliga al legislador a aceptar como parámetro de comparación, para contrastar las equivalencias, los sistemas de sufragio presencial nacionales. De esa forma se hace posible establecer un mecanismo de garantía que asegure la transparencia, la objetividad, la integridad, la igualdad y la neutralidad entre las diversas técnicas de sufragio, de modo que la técnica presencial, como nosotros también sostenemos, —en el caso español la LOREG— se constituye en patrón de referencia contra el que se establezcan los requisitos de garantía que han de garantizar los sistemas de sufragio electrónicos, presenciales y remotos. La Recomendación efectúa, por otra parte, un tratamiento homogéneo e integral de los elementos fundamentales que pueden configurar inicialmente los procesos de sufragio electrónico, es decir, enumera los principales aspectos que una legislación de desarrollo ulterior no habrá de desconocer. Así, la Recomendación aborda el *sufragio universal*, en sus cuatro primeros artículos, definiendo las condiciones operativas de los sistemas de voto que hagan estos instrumentos compatibles con la universalidad pretendida, lo que incluye el tratamiento de la discapacidad genéricamente considerado.

En relación con el *sufragio igualitario*, éste se considera en los artículos 5 a 8 de la Recomendación. La idea fundamental de la sección es evitar los problemas relacionados con el sufragio doble o efectuado por diversas vías concurrentes que podrían dar origen a situaciones de anulación del sufragio. La *libertad de sufragio* está contemplada en los artículos 9 al 15. La sección estudia y regula aquellos aspectos que pueden tener incidencia en la libertad de formación de la voluntad del votante. El tema es extenso, dado que las técnicas que pueden desarrollarse entre modalidades de voto, como el voto electrónico presencial y el remoto, conducen a exigencias totalmente distintas. Elaborar y describir los métodos mediante los cuales puede asegurarse la libertad de sufragio no es tarea sencilla y comprende, fundamentalmente, tres pasos a desarrollar (desde la vertiente ecléctica de la teoría de la dirección de ajuste).

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

1) Aislar, en el marco del proceso de voto presencial, la metodología empleada para asegurar la libertad de sufragio, lo que nos permite obtener una idea básica apta para establecer una fuente de equivalencia.

2) Disponer de un conocimiento técnico de cómo las máquinas de voto electrónico administran el proceso de sufragio en cada una de las diversas modalidades de voto, desde el presencial, en máquinas electrónicas, al voto electrónico remoto desde ordenadores personales.

3) Precisar las técnicas de adaptación y equivalencia procedimental entre el proceso referente y los procesos referidos. La adecuación derivará ordinariamente de las posibilidades de adaptación de las tecnologías concurrentes en relación con el proceso patrón de referencia.

Debemos señalar aquí, como ya hemos indicado, que las tecnologías actualmente disponibles impiden obtener un nivel de equivalencia homologable al obtenido en base a los sistemas institucionales de naturaleza presencial.

La Recomendación también se ocupa del *secreto del sufragio* en sus artículos 16 a 19. La preocupación de la Recomendación es garantizar que en las distintas fases del sufragio electrónico no sea posible conocer, por ninguna parte implicada en el proceso de sufragio, el sentido del voto del votante, así como impedir que puedan establecerse correlaciones indeseables capaces de hacer posible averiguar tanto el sentido del voto, como el titular del mismo. La posibilidad de dar sentido y contenido a tales principios rectores se halla en dependencia directa tanto del rigor en la adaptación al nivel de equivalencia de los procesos de sufragio electoral convencional (presencial), como *a las posibilidades técnicas que cada tecnología pueda ofrecer*. Como sabemos, el secreto será mejor garantizado en los sistemas de voto electrónico presenciales, si bien existen diversas técnicas que permiten desvelar tal secreto en ese tipo de tecnologías. Los problemas más importantes, no obstante, surgen en el ámbito del voto electrónico remoto, dado que, a diferencia del voto electrónico en máquinas presenciales, el titular del derecho iniciará en todos los supuestos de voto electrónico remoto una comunicación telemática, en todo caso, mediante una dirección IP estática o dinámica (DHCP), y una dirección MAC asociada (datos que deben formar parte de la categoría propuesta de «*datos electrónicos de naturaleza electoral*» —recordamos que la dirección IP (lógica) ha de considerarse un dato de carácter personal—[7], en un futuro también lo será previsiblemente la dirección úni-

[7] Tal y como señala, en nuestro país, la Agencia de Protección de Datos en su informe nº 327/2003.

ca MAC (física)[8]) que permiten averiguar en la inmensa mayoría de los casos el titular del equipo informático (actualmente tal dato de carácter personal, no supone sin más una asociación univoca, ya que el ordenador podría estar instalado en un domicilio y ser empleado para el sufragio por diversos miembros de la unidad familiar). Aún cuando las normas de voto electrónico tratarán de separar el sentido del voto del votante, según expedientes técnicos disponibles, la mayoría de estos procesos *son reversibles*, lo que puede permitir a quien disponga de los medios adecuados *reconstruir* lo que en los sistemas presenciales se garantiza de modo absoluto: *la ruptura de la conexión sentido del voto y titular del derecho de sufragio*. En una urna convencional, una vez que el sobre electoral cae al interior de la misma, queda disociado de modo absoluto toda posibilidad de reconstruir el sentido de la relación votante-sentido de su voto.

La Recomendación incide también sobre la *transparencia,* en sus artículos 20 a 23. Esta es considerada como aquella cualidad que permite que del sistema de voto electrónico tengan conocimiento los destinatarios y usuarios del mismo. Es indudable que tal pretensión es una condición necesaria, más no suficiente, para que los electores puedan acceder a estas tecnologías, ahora bien, los problemas que se desprenden de la transparencia tienen un alcance muy superior al establecido inicialmente por la Recomendación[9], la cual también comprende en su artículo 21 que el funcionamiento de un sistema de voto electrónico *deberá estar públicamente disponible*. Este segundo aspecto es fundamental, en cualquier sistema de sufragio electrónico. No podemos aquí abordarlo, en modo alguno, por las limitaciones de espacio, si bien advertimos que el artículo debe ser considerado un criterio esencial en relación con el sistema de sufragio electrónico, en el sentido de que hace posible disponer de la información esencial que permita valorar la adecuación entre los diversos sistemas electrónicos y los principios a los que deberán de adaptarse éstos rigurosamente. Como señala Dieter Nohlen: «La manipulación potencialmente irrestricta de elementos técnicos tendiente a buscar determinados efectos y a atenuar o evitar otros se ve restringida sin embargo por el imperativo de mantener hasta cierto punto la sencillez, la simplicidad del sistema electoral. *Hay que respetar el factor humano*. El sistema electoral debe ser inteligible, humanamente viable. Este aspecto constituye una de las fuentes de

[8] La dirección MAC, «Dirección de Control de Acceso al Medio», es un identificador único que actúa como una especie de número de serie para dispositivos hardware, que opera en la capa 2 —acceso al medio— del modelo OSI de 7 capas.

[9] El concepto de transparencia en materia de sufragio electrónico remoto es un concepto amplio y transversal, tanto al proceso tecnológico como a los destinatarios de la información que se pretende informar.

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

legitimidad del sistema electoral, recurso necesario para el ejercicio de su función global en un sistema político[10]».

La *verificación* y la *contabilización* son también consideradas por la Recomendación en los artículos 24 a 27. Fundamentalmente estos artículos regulan las condiciones en las que las tecnologías han de ser evaluadas por las Administraciones públicas encargadas de su verificación. En materia de voto electrónico estas condiciones son fundamentales para garantizar que tales tecnologías cumplen con los requisitos de adecuación que habrán de ser definidos en las normas de desarrollo correspondientes. La *de lege ferenda* LODREL sería la norma de definición apropiada que regulase tales aspectos, sin perjuicio de que normas de rango reglamentario desarrollasen el contenido de las disposiciones contenidas en la Ley Orgánica del Régimen Electoral Electrónico.

La regulación de los aspectos relacionados con la *fiabilidad* y la *seguridad* se consignan en los artículos 28 al 35 de la Recomendación, tratan de ofrecer una regulación de los aspectos relacionados con el fraude en materia de voto electrónico en sus dimensiones operativas presencial y remota. En tales artículos, se establecen principios generales, que habrán de adoptarse como medidas de seguridad en los ámbitos citados, sin embargo, su articulación es insuficiente ya que se precisan mayores grados de concreción, por una parte, y una especificación clara de las técnicas a las que hace referencia la regulación. En el ámbito de las *normas operativas,* la Recomendación establece los aspectos relacionados con la notificación, en los artículos 36 a 38. Bajo ese epígrafe se consideran aquellos aspectos fundamentales —en relación con la publicidad— de los procesos de sufragio, es decir, que los ciudadanos tengan fiel conocimiento de las actividades que en torno al sufragio electrónico desplieguen las Administraciones electorales, con la finalidad de asegurar una satisfactoria comunicación con los destinatarios de la normativa, de forma que puedan conocer sus derechos y sus deberes en relación con las tecnologías electrónicas. El *registro* de votantes se considera en los artículo 39 a 41. Estos artículos hacen referencia a los sistemas de registro electrónico, no ordenan expresamente su existencia, como es lógico, pero promocionan la adopción de la legislación interna que los hagan posibles, definiendo tan sólo algunos aspectos de procedimiento esenciales.

En relación con los *candidatos,* éstos son contemplados en los artículos 42 y 43, promoviéndose la introducción de las denominadas nominaciones *on-line*, que no podemos estudiar aquí (remitimos a la investigación). Con respecto a la *votación*, la misma es contemplada en los artículos 44 a 52. La regulación que

[10] Dieter Nohlen, «*Sistemas electorales y partidos políticos*», FCE, México, 2004, Págs. 159-160 (las cursivas son nuestras).

sobre el voto efectúa la Recomendación hace referencia a los aspectos procesales generales que han de satisfacerse para el cumplimiento de concretos principios, como el de igualdad en la representación de todas las opciones de voto por medio de los dispositivos usados para emitir el sufragio electrónico, que deberán ser igualitarios (art. 47). En análogo sentido, se pretende que en todas aquellas actividades en las que aparezcan o en las que concurran los diversos candidatos se sea cuidadoso en la presentación de las opciones de voto, de modo que no se produzca discriminación entre las opciones concurrentes. La idea básica de la sección es la equiparación estricta entre candidaturas, con la finalidad de evitar posibles fraudes de discriminación que puedan tener su origen en determinadas fórmulas de manipulación electoral pensadas para favorecer y, en su caso, perjudicar a concretos grupos políticos o candidatos individuales.

El tratamiento de los *resultados electorales* se comprende en los artículos 53 a 58 de la Recomendación. La sección se ocupa de ordenar la actividad con respecto a los plazos temporales de escrutinio del sufragio, también a impedir que el sufragio pueda ser contabilizado de modo que pueda revelar las elecciones de los votantes. Las opciones de asistencia al escrutinio, también son contempladas en la misma, sin embargo, en materia de voto electrónico y, como estudiamos con detalle en otro lugar, carece prácticamente de sentido tal tipo de operaciones que resultan ser *injertos* de técnicas presenciales en el plano del escrutinio informático, con lo que el resultado es una estéril operación de control, ya que los procesos de escrutinio electrónicos son completamente opacos, y carece de sentido lógico agrupar cualquier número imaginable de instrumentos de control presencial *analógicos* para la fiscalización de una tecnología que únicamente puede controlarse conforme a sus propios postulados técnicos *digitales*. La *auditoría* de tales datos se contempla en los artículos 59 y 60. La Recomendación establece como primer aspecto relevante que el voto electrónico debe ser auditable, circunstancia, por otro lado, lógica, señalando que los datos de auditoría servirán, entre otras cosas, para revisar los circuitos técnicos de sufragio. Dentro del apéndice III, dedicado al establecimiento de requisitos de voto, se aborda, en primer lugar, aquéllos relacionados con la *accesibilidad.* Se entiende la accesibilidad en ésta sección como la propiedad que deben reunir los instrumentos destinados al voto que favorezcan la interacción eficiente y sencilla entre los votantes (haciendo particular alusión a aquellos que muestren diversos tipos de discapacidad) y los diversos sistemas de sufragio electrónico. Aquí, la división entre sistemas de voto electrónico presencial y voto electrónico por Internet es importante, porque, en el primer supuesto, el votante encontrará en los funcionarios electorales un auxilio que puede ser esencial para perfeccionar la actividad de votación. Circunstancia que no se produce en los supuestos de voto

electrónico por Internet, en los que los funcionarios electorales pierden su sentido al realizarse el acto de votación de modo completamente electrónico y autónomo.

La *interoperabilidad* se regula en las letras C a D de la Recomendación. Es relevante señalar la opción que la Recomendación defiende *al adoptar estándares abiertos,* ya que de esa forma se garantiza que no se produzcan condicionamientos de naturaleza tecnológica que pueden ser muy perjudiciales en materia de voto electrónico. Por otro lado, este tipo de estándares hacen posible con mayor facilidad el estudio de la estructura del procesamiento de la información electoral. La Recomendación, inicialmente, propone el estándar EML (Election Markup Language/ Lenguaje de marcas para elecciones). En el marco de las operaciones del sistema de sufragio electrónico, la Recomendación regula, en sus artículos 69 a 76, los requisitos para la infraestructura central y cliente en entornos controlados, es decir, por entornos controlados hemos de entender: voto electrónico presencial en secciones electorales, en tal sentido, la logística que afecta a este tipo de tecnologías ha de ser regulada adecuadamente para un despliegue eficiente de la misma, lo que significa que es preciso desarrollar planes y programas de contingencia, diseñar y ordenar la planificación de las instalaciones de voto electrónico, etc., que no podemos aquí sino tan sólo enunciar.

Los requerimientos de seguridad, referentes a las etapas de pre-votación, votación y post-votación se especifican en los artículos 77 a 85 de la Recomendación. La misma establece un conjunto consistente de pautas de seguridad que representan lo que podríamos denominar un elevado estándar de control. Las exigencias que invocan los artículos en las que éstas se desarrollan tratan de garantizar, en las máquinas de voto, la mayor resistencia posible al fraude. A partir de éstas premisas se pretende construir sistemas que las hagan plenamente efectivas, lo que, como sabemos, constituye un reto excepcionalmente difícil de alcanzar en el plano del voto electrónico presencial y, prácticamente imposible, en el sufragio electrónico por Internet. Los artículos 86 a 88 regulan los requisitos en las etapas de pre-votación, así como para los datos comunicados a la etapa de votación. En estos artículos se pretende mantener y garantizar la autenticidad, disponibilidad e integridad de los registros de votantes y de las listas de candidatos. Los requisitos, en la etapa de votación y en relación con los datos comunicados durante las etapas post electorales, se establecen en los artículos 89 a 96. Bajo el epígrafe anterior se reúnen una serie de exigencias operativas, que los sistemas de voto electrónico presenciales y remotos deben satisfacer, así, por ejemplo, el artículo 92 establece: «que se deberán proporcionar suficientes medios para garantizar que los sistemas que son empleados por los votantes para emitir su voto pueden ser protegidos contra influencias que pudieran modificar el voto».

Con posterioridad a la votación, se contemplan una serie de exigencias de seguridad que se consignan en los artículos 97 a 99 de la Recomendación. Tales exigencias se concentran en preservar los datos obtenidos en las etapas anteriores, con la finalidad de disponer de ellos y ser empleados como fuente de prueba y verificación del sufragio en la tarea de auditoría. La auditoría, propiamente dicha, se regula en los artículos 100 a 108. Se consideran, no obstante, cuatro secciones que son: 1) General, arts. 100 a 101; 2) Registro, arts. 102 a 103, apartados: a), b) y c); 3) Monitorización, arts. 104 a 106; y 4) Verificabilidad, arts. 107 a 108. En relación con el proceso general, el artículo 100 diseña las bases de un sistema de auditoría exigente en relación con los sistemas lógico, técnico y de aplicación. Por su parte, el artículo 102 establece que el sistema deberá ser abierto y exhaustivo, e informará activamente sobre potenciales problemas y amenazas. El hecho de definir un sistema abierto significa que podrá ser inspeccionado técnicamente por organismos e instituciones autónomas e independiente, amén de por las públicas, y que tal información —del máximo valor (es decir, aquella información que proviene de tales fuentes *neutrales* de inspección)— será consecuentemente hecha pública. No existe un modo mejor de que la auditoría pueda ser llevada a cabo, ya que tal regulación impide que se mantenga en secreto cualquier tipo de error, defecto de funcionamiento o ataque sufrido por los sistemas de sufragio, con lo que la confianza pública en las tecnologías podría desarrollarse en base a datos reales y veraces del estado de la investigación ofrecidos por la auditoría, lo que, por otro lado, es plenamente compatible con el artículo 20.1 d) de nuestra Constitución. Los artículos 109 a 110 protegen los sistemas de auditoría contra ataques que pretendan comprometer, alterar o perder los datos del registro de sufragio.

Para concluir el breve y sintético resumen de la Recomendación, —que comentamos con detalle en otra parte— ésta contempla con alguna escasez los procesos de certificación en los artículos 111 a 112. La certificación es *una pieza clave* de cualquier sistema de sufragio electrónico, ya que se ocupa de evaluar la adaptación de los dispositivos técnicos destinados al sufragio electrónico al conjunto extenso de requerimientos técnicos y operativos que habrán de ser definidos para poder, de esa forma, garantizar que tales máquinas satisfacen las especificaciones descritas en la Recomendación que hemos contemplado. Pensamos que cualquier proyecto de voto electrónico debe ajustarse a las recomendaciones consideradas. Éstas, en su mayoría, aciertan a nuestro juicio con el nivel de exigencias requerido para los formatos de voto electrónico presencial, ajustándose a pautas de control rigurosas. Nuestro comentario armoniza las recomendaciones consideradas con el Acta Hava, así como con la *Ballot Integrity Act of 2007* y con la *Voter Confidence and Increased Accessibility Act of*

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

2007. Estos proyectos de Ley corrigen tanto el Acta HAVA 2002, como la Recomendación del Consejo de Ministros del año 2004, con valiosas consideraciones de regulación del sufragio electrónico presencial que tienen plena vigencia y utilidad en la adecuación de la Recomendación a postulados más garantistas con el derecho fundamental al sufragio.

De la combinación de las diversas regulaciones, obtenemos un valioso cuerpo de principios normativos que no pueden ser desconocidos por el legislador nacional, en cualesquiera experiencias que sobre el voto electrónico presencial puedan plantearse en un futuro. No podemos afirmar lo mismo en cualesquiera experiencias que contemplen el sufragio electrónico mediante el uso de Internet ya que, a nuestro juicio, las nuevas legislaciones norteamericanas lo rechazan, de igual modo que en los estudios SERVE e IVAS, respectivamente, de un modo absoluto y debidamente fundamentado. En ese sentido, la Recomendación del Consejo de Ministros ha excedido en su regulación las posibilidades que la técnica hace verdaderamente operativas y, por lo tanto, fomenta en los Estados miembros una confianza inapropiada en un tipo de procesos que no se encuentran en condiciones de ofrecer un conjunto de garantías homologables a las del voto ordinario presencial.

6. VOTO ELECTRÓNICO PRESENCIAL Y MÁQUINAS DE VOTO

Como indicamos en la introducción del artículo, no es posible avanzar, en materia de voto electrónico, sin conocer el despliegue tecnológico y las investigaciones[11] que sobre el mismo se han desarrollado en los últimos años, y que ac-

[11] Estudios que comprende ésta sección citados por título, autores y centro de producción: «*Election Reform and Electronic Voting Systems (DRE's); Analysis Security Issues*» Eric A. Fischer, November, 2004 CRS Report of Congress RL 32139. Congressional Research Service. The Library of Congress U.S.A.; «*Overview of Attack Trends*», CERT Coordination Center, 2002 Carnegie Mellon University; «*Diebold Tsx Evaluation —Securiy Alert*», May 11, 2006 Critical Security Issues with Diebold Tsx, a BlackBox Voting Project, prepared by: Harri Hursti: www.blackboxvoting.org; «*Expert Report /Conroy et al vs Dennis*» Report of Colorado direct recording electronic (DRE) case, September 5, 2006 University of Iowa; «*The Machinery of Democracy: Voting System Security, Accesibility, Usability and Cost*» The Brennan Center of Justice and NYU School of Law. Direct Project: Lawrence Norden, 2006; «*Programe Architecture, local elections, Flanders*» EDS Telindus, 2006; «*Trusted Agent Report, Diebold AccuVote-TS Voting System*» Department of Legislative Services, prepared by: RABA Technologies by: Dr. Michael A. Wertheimer (Director), January 20, 2004; «*Security Analysis of the Diebold AccuVoting TS machine*» Ariel J. Feldman, J. Alex Halderman and Edward W. Felten; Center for information Technology Policy and Dept of Computer Science. Princeton University, September 13, 2006: «*Security Assessment of the Diebold*

tualmente se siguen realizando en materia de máquinas de voto electrónico. Inicialmente, y en los Estados Unidos, existe una muy amplia variedad de sistemas de voto electrónico, lo que supone una excesiva fragmentación de un auténtico mercado de equipos de votación. Pese a la abundancia de nombres, siglas y fabricantes nos encontramos en todos los supuestos con dos bloques de construcción fundamentales, un ordenador con arquitectura PC, dedicado a funciones electorales, y el software electoral, que representa, como sabemos, la lógica operativa del sistema en su conjunto (este software generalmente será un sistema operativo Windows CE, versiones 3.0 a 4.0, y las aplicaciones de software de voto propiamente dichas). Las variaciones se producen fundamentalmente en el método de introducir los datos de sufragio en las diversas máquinas de voto. Fundamentalmente se presentan tres opciones como las más extendidas:

1) Las máquinas de voto electrónico de registro electrónico directo (DRE´s).
2) Las máquinas de escáner óptico (PCOS).
3) Las máquinas de registro electrónico directo, que disponen simultáneamente de prueba de registro en soporte de papel (V/VPT).

Las máquinas de registro electrónico directo, han sido, y son, las que más problemas han generado en relación con el sufragio electrónico debido a que en éstas el votante ha de *presumir* que su voto ha sido debidamente contabilizado. El votante interacciona con una máquina de pantalla táctil, en la que se selecciona una opción y, supuestamente, ésta será registrada y contabilizada como un voto válido, sin embargo, diversas e importantes investigaciones han demostrado que es muy sencillo manipular este tipo de máquinas de voto electrónico, de

Optical Scan voting terminal», A. Kiayias, L. Michel, A. Russell, A A. Shvartsman, A. Korman, Seen N. Shashidrar, N. Walluck , Ucon VoTeR Center and Computer Science and Engineering; University of Connecticut, October, 30, 2006. «*Ceci n`est pas une urne*» On the Internet Assamblée del Française de l´étrangers; Andrew W. Appel, Jue 14, 2006 Roquencourt, France; «*Security Analysis of the Diebold AccuBasic Interpreter*», Wagner David, Jefferson David, Bishop Mat, Karlov Chris, Sastry Naveen, Voting System Technology Assessment Advisory Board (VSTAAB) University of California, Berkeley, Febraury 14, 2006. «*Source Code Review of the Diebold Voting System*». Ariel J. Feldeman y otros. University of California. Berkeley, July 20, 2007. «*Source Code Review of the Hart InterCivic Voting System*». Dan S. Wallach y otros. University of California. Berkeley, July 20, 2007. «*Source Code Review of the Sequoia Voting System*». Chris Karloff y otros. University of California. Berkeley,July, 20, 2007. «*Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine*», Andrew W. Appel, Brian W. Kernighan, Maia Ginsburg, y otros, Princeton University, October 17, 2008. (Para un estudio detallado de estas investigaciones y otros trabajos que aquí no se incluyen, remitimos a nuestra monografía).

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

diversas maneras (los métodos detallados se describen en otro lugar de nuestra investigación) lo que ha llevado a los ciudadanos y legislaturas de diversos Estados, California entre otros, a solicitar al gobierno federal que esta tecnología sea retirada de los procesos de certificación de máquinas de voto regulados por el Acta HAVA.

Por su parte, las máquinas de escáner óptico basan su principio de funcionamiento en la lectura (escaneado) de una tarjeta electoral de papel, en la que el elector, manualmente, realiza su designación política e introduce la misma, a través de la tarjeta, en la que se ha consignado tal información en el lector de la máquina de voto, que registra electrónicamente el sufragio. La ventaja de ésta tecnología se basa en que al introducir en el interior de la máquina el soporte original del voto, junto con la contabilización electrónica del sufragio que proviene de aquélla, se hace posible que, en los supuestos de sospecha de fraude o manipulación, éstas papeletas puedan ser contabilizadas manualmente a fin de detectar el presunto fraude, teniendo validez los datos de recuento manual en tales supuestos de fraude. Es decir, si no existe sospecha de fraude o impugnación en su caso, los datos de voto electrónico escrutado serán finalmente los contabilizados electrónicamente, no los datos de recuento manual. El problema de tales máquinas es que, una actividad fraudulenta que no revele en los sistemas de calibración y verificación su presencia, lograría que los datos contabilizados sean únicamente los electrónicos, no el soporte físico (los datos consignados en la papeleta electoral) de los que estos son tomados.

Por último, las máquinas más recientes y, las inicialmente menos problemáticas, son las máquinas de registro electrónico directo con registro de auditoría en papel. Tales máquinas son técnicamente parecidas a las máquinas DRE´s en su configuración electrónica, pero se diferencian de aquellas en que las V/VPT generan simultáneamente a la selección efectuada por el votante, un registro en papel, que el elector puede comprobar directamente, si bien éste no la puede tocar ni retener. La papeleta impresa es una prueba de la selección realizada por el votante, que valida y observa directamente cómo queda almacenada en un depósito de papeletas integrado en la máquina de voto electrónico.

Las tres técnicas han demostrado ser vulnerables a diversos tipos de ataques cuyo objetivo era favorecer a candidatos en perjuicio de otros, en ese sentido, en nuestra investigación estudiamos los más importantes estudios realizados sobre máquinas de votación electrónicas. Por ejemplo, el estudio RABA, en relación con la investigación de la Universidad Johns Hopkins, el estudio de las máquinas Accu-Vote TS, preparado por la Universidad de Princeton, o el estudio de las máquinas Diebold de escáner óptico, preparado por la Universidad de Berkeley,

amén de otros, como el estudio del centro Brennan para la Justicia y la Universidad de Nueva York, y el preparado por la Comisión Carter-Baker, que consideran el sufragio electrónico desde una perspectiva más amplia y que no podemos resumir aquí. Es preciso ser consciente de que una de las amenazas más serias de fraude puede provenir, no sólo, de la manipulación del software sino, también, de la manipulación del hardware de las máquinas de voto como exponemos con más detalle en otro lugar y, en particular, de los propios *microprocesadores* si se desarrollasen para fabricar máquinas de voto *ad hoc*. El riesgo de tales microprocesadores se basaría en que se disociarían el componente software del hardware en el plano de la seguridad, es decir, de nada serviría un programa software de voto electrónico libre de errores, y potencialmente seguro, si el hardware (que comprende también todo tipo de equipos periféricos funcionalmente necesarios para la conducción del sufragio: concentradores, enrutadores, Módems xDSL, impresoras, scanners, etc.) contiene *circuitos maliciosos* capaces de robar claves, modificar parámetros gestionados por el software electoral, alterar las secuencias legítimas de los procesos de cifrado y descifrado, etc. Este riesgo existe, no es una probabilidad remota, como demuestra, contundentemente, el grupo de trabajo liderado por el profesor Samuel T. King de la Universidad de Illinois[12], el cual ha desarrollado tales circuitos integrados que pueden ser instalados en máquinas de voto y sortear con éxito las medidas de seguridad software por sofisticadas que éstas sean, frustrando completamente la pureza y legitimidad del proceso de sufragio electrónico y dificultando, a su vez, su detección por los servicios ordinarios de inspección y auditoría de las máquinas de voto. La única ventaja de éste tipo de manipulaciones es la consistencia temporal de la prueba del fraude, circunstancia distinta en los supuestos de software, ya que el software puede ser borrado en cualquier momento. Tales *circuitos maliciosos* han venido empleándose hasta ahora en aspectos de seguridad nacional relacionados con la inteligencia. De lo anterior se desprende, necesariamente, y en el plano jurídico, la necesidad de una revisión y reforma de la legislación de patentes nacional (Ley 11/1986, de 20 de marzo, de Patentes y Reglamento para su aplicación, RD 2245/1986, de 10 de octubre) e internacional, que no podemos abordar aquí, en el sentido en el que éstas tengan aplicación a los sistemas de voto electrónico, es decir, la legislación de patentes debe comprender excepciones y limitaciones específicas de análisis público riguroso cuando los dispositivos electrónicos protegidos por el derecho de patentes tengan

[12] Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang y Yuanyuan Zhou, «*Designing and implementing malicious hardware*», University of Illinois at Urbana Champaing, Urbana, IL 61801, U.S.A., Septiembre de 2008.

cualquier tipo de aplicación en los dispositivos destinados a tareas de sufragio electrónico público.

Hay que considerar también —con independencia de lo señalado anteriormente— que las tecnologías empleadas en el voto electrónico presencial *no son neutrales* en relación con la facilidad de incurrir en errores accidentales en su manipulación por el votante, lo que afecta a determinados colectivos de ciudadanos que pueden sufrir *discriminación* por tal factor, como demostraron Tomz y Van Howelling, que puede ser, además, fuente generadora de procesos de voto nulo (pérdidas de voto «sub o sobre votaciones»). Existe un concepto, destinado a estudiar y determinar tales discrepancias entre el voto intentado y el realmente contabilizado, denominado «*ratio de voto residual*» que, tal y como es definido por el Dr. David Kimball es: «*la diferencia entre el número de votos depositados en una máquina de voto electrónico y el número de votos válidos depositados en un contexto particular.*[13]» Tal parámetro, que es considerado como la más simple y mejor medida de la *efectividad* de un sistema de voto electrónico, permite estudiar cómo el diseño de las máquinas de voto incide y afecta directamente a la efectividad del proceso de sufragio; diversos tipos de máquinas ofrecen diversos *ratios de voto residual.*

Sin embargo, lo que todos los estudios que desarrollamos demuestran, es que todas estas máquinas son gravemente vulnerables al fraude electoral, no desde una perspectiva teórica, sino práctica. Cada estudio que consideramos se basa en el desarrollo de ataques empíricos reales de manipulación de tales máquinas, realizados por equipos de trabajo de las Universidades indicadas, que logran llevar a cabo con éxito, y relativa facilidad, la manipulación electoral deseada. La pregunta que es preciso formular, a la vista de tan tremendos resultados es: ¿por qué es tan sencillo desarrollar ataques exitosos contra las máquinas de voto presencial? La respuesta, o al menos una parte de la respuesta, tiene que ver con el problema teórico de la dirección de ajuste.

Quizás el problema fundamental que nos ocupa se encuentra en determinar cómo ha llegado la idea del voto electrónico a ser considerada por la sociedad como útil y, en ese sentido, no se origina desde el proceso electoral hacia la tecnología disponible, sino desde la tecnología disponible hacia el proceso electoral. Indudablemente, las direcciones de ajuste[14] son aquí fundamentales, porque, en

[13] D.C. Kimball, K. Martha, «Ballot initiatives and Residual Ballots in the 2004 Presidential Elections», *Annual Meeting of Southern Political Science Association,* Atlanta, GA, (January, 2006) Pg. 6 y ss.

[14] La idea, claramente, se relaciona con la dirección de la secuencia lógica de acciones apropiadas a un sector de regulación, con arreglo a unos principios que han de ser preservados como

función de qué dirección de ajuste se elija para derivar de ella postulados generales y consecuencias prácticas, las que son propias de cada ámbito definirán, verosímilmente, el modo de construcción del sistema de sufragio que se proponga como válido. Desde *la dirección de ajuste del sistema electoral,* son las exigencias de control riguroso frente al fraude (lo que implica la participación ciudadana en funciones de control) y la publicidad procedimental las claves fundamentales sobre las que se construye todo el proceso a su alrededor, lo que marca y fija exigencias muy rigurosas a las que se debe adaptar cualquier proyecto que pretenda prosperar, respetando esas estrictas exigencias, el resultado reclamaría prescindir de redes abiertas, diseñar sistemas (ordenadores) robustos, no propietarios, a fin de que la inspección pública más completa fuera siempre posible. El software electoral, igualmente, debería atenerse a unos principios rigurosos de apertura, publicidad y diseño a prueba de fallos y, si tales condiciones no se pueden conseguir, bien porque los costes económicos son impracticables, bien porque la tecnología disponible no ofrece la posibilidad técnica requerida, el proyecto deberá esperar a que las nuevas tecnologías —siempre en constante evolución— resuelvan los problemas actualmente irresolubles. Pero los principios de este enfoque de ajuste no pueden, ni deben, relajarse, son *estrictos*. Debido a que, además, existe un procedimiento validado y eficiente que satisface plenamente los requisitos a los que debe ajustarse el voto, para poder calificarlo de limpio, procedimentalmente justo y plenamente garantista, es decir, el sistema institucional presencial que asegura la *integridad* y la *neutralidad* del proceso de votación.

Si nos situamos, por el contrario, en la dirección de ajuste de las «*nuevas tecnologías*» de la sociedad de la información, es decir, desde una perspectiva fundamentalmente privada, dado que la tecnología pertenece o es fundamentalmente explotada por organizaciones de mercado, éstas, desde una lógica lucrativa, proponen al mercado político un *nuevo instrumental* para satisfacer una serie de exigencias regulares, como son, entre otras, el proceso electoral (que *ne-*

---

señalara correctamente Deutsch: « Las decisiones se hacen a menudo en secuencias. Primero se decide acerca de las preferencias, propósitos o metas generales en cuanto a alguna clase de problemas. A esto se le llama una decisión de *política*. Luego las decisiones se ocupan de los medios y métodos de ejecución de la política. La diferencia que existe entre la política y su ejecución se asemeja a la que existe entre la estrategia y la táctica. La estrategia consiste en el establecimiento de series de metas u objetivos de largo plazo; la táctica consiste en seleccionar y aplicar los medios de corto plazo para su realización. Generalmente, la estrategia escudriña más lejos en el futuro e implica la fijación de una clase más grande de metas, mientras que en la táctica denota la elección de una clase más limitada de pasos intermedios dentro de la clase más amplia», K.W. Deutsch, «*Política y Gobierno* «, FCE, México, 1976, Pg. 193.

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

cesariamente se privatiza en ese marco teórico). Ahora bien, la adaptación de estas organizaciones hacia las exigencias que establece el proceso electoral, no tienen un sencillo encaje o ajuste *porque la seguridad y la publicidad no son condiciones específicas que hayan sido, en las recientes décadas de evolución de estas tecnologías y mercados, condiciones naturales de su evolución.* Las organizaciones industriales protegen sus invenciones en un mercado competitivo, mediante patentes y protección intelectual, y la adaptación entre enfoques radicalmente distintos produce desajustes que se pueden traducir en sistemas o máquinas que producen un alto riesgo para el correcto funcionamiento del proceso electoral —como tendremos ocasión de ver en lo que resta del capítulo—. Los problemas que venimos exponiendo derivan precisamente de lo que hemos señalado aquí. Las empresas y organizaciones industriales ofrecen un tipo de producto, que es una adaptación de un sistema de propósito general, no pensado para satisfacer exigencias de seguridad compatibles con el rigor que exige el voto electrónico remoto, es decir, los PC (su arquitectura de los años 80) no se desarrollaron para tareas de alta fiabilidad y seguridad, como tampoco lo fueron, ni lo son, la inmensa mayoría de los sistemas operativos hoy disponibles en el mercado, como Microsoft Windows, Linux, IOS (Internetwork Operating System, de CISCO), etc. Es fácil observar cómo, en los últimos años, esas empresas comienzan a diseñar sus sistemas operativos con mejores mecanismos de seguridad, pero se encuentran muy lejos de las exigencias del enfoque de ajuste del sistema electoral. Que, por otra parte, exige condiciones rigurosas de *análisis* e *inspección* de las tecnologías implicadas, lo que es también incompatible con ésta segunda dirección de ajuste.

Una tercera posición, pretendidamente ecléctica, es aquélla que intenta integrar a través de una técnica necesariamente de «parcheo» la adaptación entre las dos filosofías en oposición. Decimos de «parcheo» porque intenta, con la tecnología disponible, «reforzar la seguridad», pero sin renunciar a un diseño de hardware PC arcaico o vetusto e insuficiente y conservando, por otra parte, íntegramente los derechos de propiedad intelectual e industrial sobre lo que no sea estrictamente necesario no revelar de los programas y aplicaciones que operan en tales máquinas (como los sistemas operativos), efectuando, por ejemplo, divisiones arbitrarias en determinadas tecnologías fundamentales, como es la tecnología de software. Así, el Acta de Integridad del voto de 2007, pretende, en tal sentido, establecer una división entre «software electoral» y «otros tipos de software» que funcionen en las máquinas de voto electrónico. Como si se tratara de categorías de software que trabajasen en compartimentos estancos, pretendiendo, fundamentalmente, proteger los sistemas operativos propietarios (Microsoft) de revelar el código fuente del software que se instalará en las máquinas de voto.

Ya hemos argumentado, en otra parte del trabajo, el porqué ésta división es inadecuada para obtener el necesario nivel de escrutinio público de las aplicaciones software de voto, sin el cual no es posible garantizar —en parte al menos— la seguridad, el secreto, la neutralidad y la integridad del proceso de voto electrónico.

Hay que tener en consideración, en la reflexión que realizamos, cuando hacemos referencia a Microsoft o a CISCO (en el ámbito de los sistemas operativos y, en menor medida, en el área de los navegadores Web y de los *sistemas operativos de redes*) que estamos hablando de «monopolios de facto», *que obviamente representan una condición de dependencia tecnológica, incompatible con los principios a los que debe adaptarse cualquier tipo de solución que pretenda participar en un nuevo marco jurídico público electoral, como señala expresamente la Recomendación del Consejo de Ministros sobre el voto electrónico*. Probablemente, la aprobación de instrucciones políticas que contemplen el uso de *software de fuente abierta* OSS sea la única medida eficaz para verdaderamente romper una práctica monopolística consolidada que los diversos sistemas legales (Estadounidense y Europeo) han sido incapaces de resolver adecuadamente. Una forma pues de «limitar el privilegio monopolista» de los sistemas operativos es que las Administraciones públicas apoyen decididamente la adquisición de soluciones software abiertas[15], de modo que una nueva etapa de búsqueda de la competencia en un nuevo mercado, no necesariamente inspirado únicamente por el ánimo de lucro, permita reconstruir las bases de una competitividad no monopolista (remitimos al comentario de la letra «C» de la Recomendación sobre las normas legales y operativas para el voto electrónico, de 30 de septiembre de 2004). La solución que se presenta está lejos de ser óptima para el enfoque de la dirección de ajuste de los principios del sistema electoral, pero puede generar grandes beneficios al mercado que provee estos dispositivos. El perjuicio —pensamos— se encuentra en la parte de un electorado que puede ver reducida su legítima expectativa de garantía, pureza y neutralidad del proceso electoral, y asumir nuevas formas de corrupción de muy difícil solución, por una parte, así como soportar nuevas fuentes de discriminación de otra. Debemos recordar, que incluso siguiendo la dirección de ajuste correcta: *sistema electoral-tecnología disponible*, los problemas estructurales nativos o intrínsecos carecen de solución adecuada. Tan sólo reformando profundamente la ingeniería de los procesos que

[15] En ese sentido, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE núm, 150, de 23 de junio), apuesta decididamente en la letra i) de su artículo 4º por impulsar el empleo, por parte de las Administraciones Públicas, de estándares abiertos.

hemos señalado en este estudio sería posible alcanzar niveles de seguridad superiores a los actuales, como recientemente señaló la Comisión de Ciencia y Tecnología de la House of Lores británica, lo que coincide plenamente con las recomendaciones del estudio SERVE, o con los estudios de la OSCE/ODHIR[16] que no podemos sino señalar aquí.

7. CONCLUSIONES

El artículo que aquí concluye ha pretendido mostrar una serie de extremos que afectan profundamente al proceso de votación y al sistema electoral en su conjunto. Este tipo de estudios no han sido necesarios, tan sólo, porque la técnica electoral no ha experimentado modificaciones procesales relevantes en los últimos doscientos años. Sin embargo, la pretensión de incorporar o «*injertar*» la tecnología informática en el voto presencial, y la telemática en el voto por correspondencia, representan ambas opciones serias modificaciones de la concepción del sufragio activo, como mínimo en las dimensiones que hemos tratado de recoger aquí.

Nuestras conclusiones, a la vista de los datos expuestos, son la inadecuación del sistema de voto electrónico (presencial y remoto mediante Internet) con los principios a los que debe ajustarse estrictamente el régimen electoral para predicar de él su *confiabilidad,* es decir, estas técnicas no permiten asegurar la integridad y neutralidad del proceso electoral y, por lo tanto, su empleo genera inseguridad, sin aportar ventajas significativas en ningún sentido relevante. Tal vez sí la sensación de satisfacción de un prurito por adaptar las nuevas tecnologías emergentes a los sistemas electorales, como condición subjetiva e ideológica de progreso, amén de favorecer una industria con pretensiones de conquistar un espacio libre de procesos comerciales y mercantiles, que es exactamente lo que ha sido el sistema electoral en estados como el español, el francés, el inglés o el italiano, entre otros.

El voto electrónico *presencial* se halla en una etapa de su desarrollo inmadura. Pese a ello, se ha empleado y emplea —a nuestro juicio de modo imprudente—, y tal inmadurez se traduce en un abundante número de problemas de diversa naturaleza que hemos considerado con algún detalle. Por su parte, el voto electrónico remoto no es que se halle en una etapa o estado de inmadurez, se trata de una modalidad técnica de ejercicio del sufragio que normativamente habría

[16] OSCE/ODHIR Election Assesment Mission Report, «*The Netherlands*», Parliamentary Elections, 22 november 2006. Puede también consultarse en: www.osce.org/odhir

de estar prohibida, como recomiendan un heterogéneo conjunto de estudios de la máxima solvencia técnica y jurídica como, entre otros, el desarrollado por el centro Brennan de justicia, la Comisión de reforma electoral Carter-Baker, así como por la legislación de enmienda del Acta HAVA, la *Ballot Integrity Act of 2007,* y por la *Voter Confidence and Increased Accesibility Act of 2007*.

En todos los casos se prohíbe la conexión de las máquinas de voto electrónico instaladas en cualquier ámbito de la jurisdicción federal a Internet, dado que se reconoce, como un hecho incontrovertible, que se trata de una red de comunicaciones no apta para su uso en la transmisión de información electoral (como también se reconoce, implícitamente, en la Recomendación Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa *a los ataques contra los sistemas de información*)[17]. Se prohíbe igualmente todo tipo de comunicaciones inalámbricas (Wifi) en relación con el voto electrónico presencial, ya que tal tipo de comunicaciones por radio *son un vector idóneo para la manipulación y el fraude electoral* (hay que recordar cómo en los Países Bajos se retiró un tipo de máquina de voto electrónico, la SDU, por sufrir el problema técnico denominado «TEMPEST» que no podemos explicar aquí). De igual modo, se pretende resolver un problema muy grave que afecta igualmente tanto al voto electrónico presencial como al remoto, la necesidad imperativa de que las máquinas de voto electrónico produzcan un registro en papel (exactamente igual que una papeleta electoral convencional) por todas las nuevas generaciones de máquinas de voto electrónico tipo V/VPT. La razón es clara, no existe confianza por parte de los votantes y de las administraciones públicas de que los registros electrónicos almacenados en éstas sean veraces. Razón por la cual se pretende que cada votante individual tenga la oportunidad personal de verificar, por sí mismo, que su voto registrado electrónicamente se corresponde, absolutamente, con un registro idéntico en una papeleta electoral que se producirá en el acto de votación. El voto electrónico será registrado en formato digital (binario) y la papeleta se conservará en un depósito material de papeletas de voto. De ese modo, el votante inicialmente sabrá que, al menos, la papeleta que él ha tenido la capacidad de crear y observar directamente su depósito, verdaderamente recoge fielmente su voluntad.

Lo anterior debe hacer reflexionar. La idea que se pretende trasladar es que los votantes recuperen su confianza en un sistema de voto electrónico que ha generado una inseguridad jurídica tal que, tanto la opinión pública, como sus representantes políticos se ven en la necesidad de rectificar las normas jurídico-

[17] DOE. L69/67 16.03.2005.

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

electorales de voto electrónico del año 2002. Si en esas nuevas especificaciones jurídicas, que protegen la integridad y confiabilidad en el sufragio electrónico presencial, dotado de un conjunto de garantías infinitamente superiores a las del *voto electrónico remoto*, en el que *no existe papeleta alguna en la que confiar, como última expresión de la garantía de transparencia y objetividad del proceso de sufragio* en la conservación de la voluntad del elector, es absolutamente razonable la limitación o prohibición de tal modalidad de sufragio, ya que Internet no garantiza la integridad y el secreto de las votaciones.

Es cierto que nos hallamos en los comienzos de una revolución tecnológica y de la información, y sucede que la pretensión de extender ésta al máximo número de aplicaciones funcionales o ámbitos de aplicación es, a lo que parece, una pretensión humana muy común. El problema reside en que en el área de la que nos ocupamos tal aplicación es completamente disfuncional con los principios que históricamente han regido tan delicado sector de funcionamiento de la democracia. El sistema electoral configurado por la Constitución y por la LOREG es, en efecto, una institución jurídico política muy delicada (y equilibrada), de la que no ha sido necesario ser conscientes, hasta el momento presente, debido a la inexistencia de ningún otro proceso equivalente que pudiese disputar en modo alguno la hegemonía procesal garantista que tal institución ha representado y representa para *la estabilidad del proceso democrático*, ya que la disponibilidad y exclusividad de la técnica personal de su composición única, existente durante siglos, no permitían la presencia de ningún otro método que asegure con efectividad las garantías de neutralidad, integridad, seguridad y fiabilidad de la institución electoral, garantías que pivotaban armónicamente sobre la composición de la Administración Electoral y sobre un elemento de extraordinario valor como es la Mesa electoral.

Como hemos sostenido, consideramos que la participación en éstas podría ser interpretada como un derecho fundamental de configuración legal, de estructura eminentemente procesal, que hace posible garantizar fundamentalmente la *neutralidad* e *integridad* del completo proceso de sufragio al asegurar jurídicamente la participación de los ciudadanos en la institución electoral. Los sistemas de voto electrónico eliminan o suprimen la necesidad material de las mesas electorales y, con ello, se traslada el control de integridad a un conjunto de sistemas privados, máquinas y software de proceso de datos, que es exactamente en lo que consisten las máquinas de voto presenciales o remotas. La *neutralidad* del proceso electoral, con el desplazamiento de los ejes de la seguridad, operado por las máquinas de proceso de datos, queda materialmente desvirtuada. La neutralidad de la Mesa electoral queda garantizada por su composición plural: modo de nombramiento de sus miembros (el azar) y metodología rigurosa y ga-

rantista del proceso de voto. Condiciones que no encuentran equivalente en los sistemas de voto electrónico, fundamentalmente anónimos, altamente irresponsables y con lógicas operativas opacas. Sin olvidar la *intrínseca fragilidad* del funcionamiento del software de tales máquinas, que carece técnicamente de solución.

La *publicidad,* un elemento particularmente relevante de todo el proceso de voto manual y presencial, se pierde, igualmente, en todas las modalidades de voto electrónico. Y el único modo de intentar alcanzar medidas muy inferiores de publicidad —no iguales o superiores que sería lo mínimamente exigible de un sistema con vocación que reemplazar a otro— exige adoptar un tipo de planteamiento inicial en materia de voto electrónico difícilmente asumible, y que, aunque lo fuera, quedaría igualmente muy por debajo de las garantías que asegura el proceso de sufragio electoral presencial ordinario. El planteamiento se basa en el problema teórico de la *dirección de ajuste* y sus premisas, postulados generales e implicaciones que no reiteraremos. Si bien, es preciso recordar, que la dirección de ajuste correcta es: *sistema electoral vigente y sus principios estructurales – voto electrónico en cualesquiera de sus dimensiones operativas*, lo que representa, necesariamente, una compleja, delicada y costosa tarea de readaptación o rediseño de instituciones de control de voto electrónico desde sus principios elementales, hasta su consolidación en modelos técnicos compatibles y homologables jurídicamente con los principios directrices del sufragio presencial. Éste enfoque es complejo, debido a que exige crear *ex novo* un amplio conjunto de instituciones que han de adaptarse y asegurar uniformemente los principios sumariamente enumerados, y para su consecución es necesario afectar a la configuración de derechos constitucionales como tuvimos ocasión de considerar.

Por lo que la dirección de ajuste correcta cederá, previsiblemente, al segundo enfoque, la dirección de ajuste con sentido: *tecnología disponible - sistema electoral* (que es en buena medida el problema que se sufre en los Estados Unidos), en la que éste último prácticamente se ve forzado a adaptarse a aquella tecnología con el sacrificio inevitable de la mayoría de los principios esenciales señalados. La posición ecléctica será, tal vez, a la que se llegará con el devenir del tiempo si los fracasos aconsejan a los poderes públicos retirar una introducción apresurada de tales tecnologías, y la opinión pública es consciente de los riesgos reales que implica el uso de tecnologías que facilitan el fraude y la manipulación electoral, como lo hacen estas tecnologías cuando son manifestación de la dirección de ajuste *tecnología disponible-sistema electoral*. En cualesquiera de los tres supuestos, se pierde una importante esfera de participación de los ciudadanos en el correcto y neutral funcionamiento del proceso electoral, una limitación en su capacidad de participación activa y jurídicamente relevante, que será posible-

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

mente bien aceptada por los miembros mayoritarios y menos conscientes del riesgo. Los anteriores argumentos son, tan sólo, una proyección especulativa de *la teoría de la decisión bajo incertidumbre*[18] en la que comparamos las «peores consecuencias», y elegimos aquella alternativa que tenga *la mejor peor consecuencia* (según el criterio maximin). Tales argumentos no tienen, ni deben necesariamente de coincidir con el *deber ser jurídico* como factor ordenador de la sociedad según un modelo constitucional específico.

Desafortunadamente, la pérdida de ciertos derechos fundamentales se produce con la aquiescencia, o más bien, con la *indiferencia de sus beneficiados*. Como señalara Friedrich: «El fracaso de los hombres en todas partes para apreciar los derechos que poseen, o bien de estar al corriente de ellos, crea grandes obstáculos para su ejecución[19]». Tal vez, ello sea debido a una débil estructura de la sociedad política incapaz de percibir los riesgos, a menudo difíciles de apreciar y comprender, en detrimento de efímeras y etéreas ventajas impulsadas con pasión y recursos por promotores indebidamente informados o con intereses económicos no confesados. Es de interés señalar, en ese sentido, cómo la sociedad norteamericana —incluyendo en ese concepto la extensa y vasta red de asociaciones civiles y la Universidad— ha impulsado, intensa y decididamente, las reformas de la legislación HAVA. Cómo se han creado y organizado grupos de presión, control y responsabilidad, orientados directamente contra la legislación que estaba y está perjudicando la confianza legítima en el proceso electoral en los Estados Unidos. En España, el equivalente sería el proyecto OVSE que hemos considerado, sin embargo, apenas se registra preocupación en la sociedad o en la doctrina jurídica general, a salvo honrosas excepciones, que debería ocuparse de las implicaciones derivadas *de las tecnologías* que hemos venido considerando. De lo anteriormente enunciado podemos extraer una serie de breves postulados generales:

1. A nuestro juicio, la participación ciudadana en los asuntos públicos podría ser interpretada como derecho fundamental de configuración legal al que pertenece, en interpretación expansiva, la participación jurídicamente garantizada en la configuración orgánica de la Administración Electoral.
2. El legislador tiene la potestad de limitar el uso de la informática, para garantizar el libre ejercicio de los derechos de los ciudadanos, entre los que se encuentra el derecho a participar en la Administración Electoral.

[18] Jon Elster, «*El cambio tecnológico, investigaciones sobre la racionalidad y la transformación social*», Gedisa, Barcelona, 2000, Pg. 166 y ss.

[19] C.J. Friedrich,«*La Democracia como forma política y como forma de vida*», Op.Cit., Pg. 210.

3. La *neutralidad* del proceso electoral se basa, precisamente, en garantizar la composición personal de las citadas mesas electorales (integradas por ciudadanos legos) como técnica de control del poder o forma de separación de poderes *lato sensu*, sin perjuicio de los diversos componentes de la Administración Electoral (juntas electorales).
4. Los sistemas de voto electrónico exigen el desarrollo de costosas estructuras institucionales de nueva planta de las que, prácticamente, no existe experiencia. Tales estructuras deben proceder de una legislación orgánica de desarrollo LODREL (Ley Orgánica del régimen electoral electrónico) que tome, como base interpretativa, la LOREG como concreción de la articulación de los principios electorales fundamentales en un cuerpo normativo de referencia esencial, junto con la Constitución.
5. Es preciso efectuar modificaciones en la Ley de Propiedad Intelectual (RDL 1/1996, de 12 de abril), ordenando el sistema de propiedad intelectual en lo que afecte al concepto normativo de *lege ferenda* de «*software electoral*». Mediante la adición, al artículo 100 de la LPI, de un nuevo número, el 5bis. Sí bien será útil incorporar soluciones de software de código abierto en los sistemas de voto electrónico, con la finalidad de garantizar una inspección completa, detallada, rigurosa y pública de todo el software que tenga aplicación en cualquier sistema informático destinado al sufragio electrónico, sin excepciones de ninguna especie.
6. Es inadmisible la exención de responsabilidad de los fabricantes de *software electoral,* en relación con los productos defectuosos por estos fabricados. Y, por lo tanto, cualquier aplicación comercial con pretensión de participar en un proceso público electoral, debe satisfacer el requisito de la responsabilidad, por defectos o negligencias en su elaboración, que provoquen daños en los hipotéticos sistemas de sufragio en los que estos puedan incorporarse. *No puede haber participación sin responsabilidad,* circunstancia que debe ser interpretada de acuerdo con el artículo anterior. Condiciones, ambas, de obligado cumplimiento y que afectan tanto a los sistemas operativos como a los navegadores Web.
7. En análogo sentido al punto quinto, y de *lege ferenda,* en los supuestos de voto electrónico remoto, sería recomendable la creación de nuevas categorías de datos en el marco inicial (sin perjuicio de lo que se dirá más adelante) de la Ley de protección de Datos (L.O. 15/1999, de 13 de diciembre y en sus normas de desarrollo) que contemplasen un nuevo tipo de datos, los«*datos electrónicos de naturaleza electoral»,* con la

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

finalidad de ordenar su regulación normativa unitaria (al incluir los datos de tráfico asociados) asegurando un tratamiento específico con arreglo a su naturaleza especial.

8. El voto electrónico remoto afecta, indefectible y gravemente, a la seguridad nacional de cualquier Estado que haga uso de las redes *públicas y privadas* que conforman Internet mediante el uso de los protocolos TCP/IP, ya que se *externaliza* (en determinados supuestos) el proceso de sufragio electoral *más allá de las fronteras nacionales. El Estado no puede garantizar los circuitos virtuales por los que los «datos electrónicos de naturaleza electoral» circularán, lo que impide controlar la seguridad que sobre tales datos es preciso mantener en cualquier formato de sufragio electoral*. Razón por la que, unido a los anteriores argumentos, estados como los Estados Unidos lo prohíben. Lo anterior supone explícitamente que tales datos se encuentran previamente cifrados, lo que aún en tales supuestos no rebaja el riesgo asociado a tal *externalización* del proceso de sufragio electrónico remoto. Ya que tales datos podrían ser interceptados, descifrados y finalmente modificados. Amén de lo anterior, desde el entorno Web internacional, siempre se podrán recibir ataques de denegación de servicio, que pueden colapsar las redes nacionales, produciendo la privación selectiva del voto de los votantes.
9. Mediante la reconfiguración esencial del hardware y del software de comunicaciones electrónicas, es decir, no haciendo uso de Internet y de la tecnología de protocolos TCP/IP (lo que incluye reformular la arquitectura de los ordenadores PC) se podría considerar estudiar la viabilidad de fórmulas de voto electrónico, siempre que los sistemas informáticos experimentasen las reformas necesarias orientadas a la seguridad que demanda todo sistema que pretenda adaptarse a las exigencias que el proceso de voto remoto exige, entre ellas, asegurar la publicidad del proceso de sufragio en sí mismo considerado, lo que incluye, naturalmente, la vital fase de escrutinio del sufragio, lo que, como sabemos, con las tecnologías disponibles no es posible.
10. Existe un riesgo real de concentración de poder, por parte de los Gobiernos, si se suprimen *instituciones neutrales* como las mesas electorales, órgano ciudadano discontinuo de control extenso y público, que asegura la pureza, integridad, autonomía y neutralidad del proceso electoral. Recordemos que más de 200.000 ciudadanos asumen la responsabilidad de garantizar la neutralidad, transparencia e integridad tanto del proceso de votación como del escrutinio del sufragio. La participación ciudadana en la Administración Electoral se constituye, a nuestro juicio,

en una genuina fórmula de «*control del poder*», radicada en el *momento* de inicio de la cadena de procesos jurídicos que concluyen en la selección *neutral* de los elegidos. Es por ello, de tanto interés teórico y práctico, salvaguardar esta manifestación de democracia participativa en función de control, ya que del correcto desarrollo procesal que implica tal actividad deriva la legitimidad *política* del proceso electoral y la pacífica y ordenada confianza en que se ha desarrollado de un modo íntegro y justo. Se pueden poner en grave riesgo los logros alcanzados hasta el momento presente, *si se privatiza una parte del proceso electoral*, que a nuestro juicio y, como vimos cuando consideramos el problema de los servicios públicos y de soberanía (del que el régimen electoral general indudablemente formaría parte) podría constituir una actividad inconstitucional.

11. En los sistemas de voto electrónico el escrutinio pierde por completo las fundamentales cualidades de «transparencia» y «publicidad», lo que facilita la posibilidad del fraude electoral a gran escala. Los procesos electrónicos no pueden superar ésta condición técnica de supervisión del proceso de votación, así como del escrutinio. Por otra parte, los ciudadanos —que no formen parte de la Administración Electoral— pierden su capacidad normativamente establecida de *impugnación directa* de las irregularidades que puedan producirse en los procesos de sufragio y escrutinio. Circunstancia que supone necesariamente —conjuntamente con lo señalado en los anteriores puntos— una limitación, y restricción de su capacidad de fiscalización pública autónoma (no como miembros, en este supuesto, de la Administración Electoral, sino como miembros del *cuerpo electoral*). En relación con los partidos y asociaciones políticas, que tienen en los Apoderados e Interventores mecanismos idóneos de control de la integridad del proceso, estos, en los formatos de voto electrónico remoto, perderían absolutamente su capacidad de control y fiscalización, ya que desaparecerían con la supresión de las mesas electorales.
12. Es cierto, que el sufragio electrónico remoto, (no el presencial que presenta otros tipos de peculiaridades) con diversas modulaciones, reintroduce dos formas atenuadas de discriminación: el *sufragio capacitario* y el *sufragio censitario*. Bien que entendiendo estos conceptos en el marco en el que han sido definidos. *El voto electrónico remoto externaliza a la sociedad política una parte importante de los costes económicos derivados del proceso electoral*. La *universalidad del sufragio* puede verse afectada por condiciones como la capacidad: no todos los ciudadanos y, en

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

particular, colectivos necesitados de protección, población de mayor edad, fundamentalmente, disponen de una cualificación mínima para ejercer con libertad y plena consciencia una tarea compleja como es el voto electrónico remoto, por otro lado, un mayor número de ciudadanos puede no disponer de la tecnología necesaria y suficiente (ordenador personal, software adecuado, periféricos apropiados, línea telefónica xDSL, energía eléctrica y sistemas de respaldo de energía backup), dado que ésta no es asequible a todas las economías y, aún cuando lo fuese, disponer de la tecnología no supone en ningún sentido reunir la cualificación necesaria para satisfacer las exigencias de *un uso correcto* de la misma. El adiestramiento no se vende con la tecnología. No es ajena pues, a ésta parcela de regulación democrática, tener en clara consideración y, en relación con los colectivos más desfavorecidos, el «*utilitarismo negativo*» como factor de evitación y corrección de la discriminación, sostenido por autores como Ilmar Tammelo, Karl Popper o Arthur Kaufmann.

13. Los fenómenos como: *la compra-venta del sufragio, el voto por terceros* (el irresoluble problema de la garantía del respeto absoluto del principio de *personalidad del voto*), y las nuevas formas de *coacción de los votantes*, no encuentran soluciones satisfactorias que permitan asegurar y garantizar su imposibilidad material efectiva, fundamentalmente, en el marco del voto electrónico remoto, en el cual es posible que un hijo menor de edad vote por su padre, por su madre o por sus hermanos. El marido por la esposa, con o sin su consentimiento (nuevas formas de violencia doméstica), así como que los mayores sean privados de su derecho *coactivamente* en instituciones públicas o privadas, donde son almacenados (la edad no priva del voto, pero las minusvalías y las situaciones de especial sujeción o dependencia, pueden privar de libertad a quienes las sufren, accediendo coaccionados o siendo engañados por desaprensivos delincuentes).
14. Si como señalara Russell Hardin: «tomamos con seriedad la máxima que afirma que lo que es obligatorio debe también ser factible», los principios que inspiran el régimen electoral constitucional, interpretados como mandatos de optimización al legislador, son completamente factibles en concretos modelos institucionales, pero no en otros. Lo son, como hemos visto, en el formato mediado por los seres humanos y articulados a través de instituciones jurídicas, y no lo son en formatos electrónicos *virtuales,* en los que la participación humana es inexistente. Inexistencia que no hace factible llevar a cabo los mandatos que esta-

blece la Constitución de forma integral en materia de régimen electoral.

15. La seguridad jurídica, art. 9.3 de la CE (como valor fundamentador de los derechos, en expresión de Peces-Barba) supone la creación y mantenimiento de un ámbito de certeza, que, en materia de régimen electoral, ha encarnado adecuadamente la LOREG en nuestro país. Certeza de saber a qué atenerse, con la pretensión de eliminar dudas sobre la legitimidad del proceso de sufragio y favoreciendo un clima de confianza entre electores y elegibles. El derecho ha de asegurar esa certeza, porque como señalara Konrad Hesse, en el Estado de derecho es el Derecho el que da forma y medida al Estado, a su eficacia y a la vida colectiva que se desarrolla en su seno. La pretensión de ensamblar piezas tan problemáticas, como las que hemos venido examinando, en el marco de un hipotético régimen electoral electrónico, no es tarea sencilla, ni exenta de graves riesgos para la seguridad jurídica, que son la antítesis, en efecto, de la certeza que el derecho debe garantizar.
16. Una de las misiones esenciales de una de *lege ferenda* LODREL debería ser, con independencia de disciplinar normativamente el vasto conjunto de materias que forman —como hemos tenido la oportunidad de comprobar— el núcleo del régimen jurídico de la institución del sufragio electrónico, disciplinar igualmente una serie de materias conexas (puntos **5** y **7**) de gran importancia para el voto electrónico remoto, que actualmente podrían ser reguladas en normas autónomas, tales como la Ley de propiedad Intelectual (RDL 1/1996, de 12 de abril) en relación con todas aquellas materias referentes al concepto que hemos denominado «*software electoral*», o la elaboración de una nueva categoría jurídica de «*datos electrónicos de naturaleza electoral*» propios, inicialmente, de la regulación de la Ley Orgánica de Protección de Datos (L.O. 15/1999, de 13 de diciembre). Así como la descripción y tratamiento de nuevas conductas y elaboración de tipos penales, que deberían o podrían encontrar en la LODREL adecuado acomodo normativo. Un adecuado encaje de estas materias conexas, en el marco general del régimen electoral electrónico, pensado con vocación de regulación unitaria de un fenómeno y materia compleja y multidisciplinar, podría beneficiarse de proporcionar al mismo una *coherencia* de regulación normativa valiosa y necesaria.
17. El voto electrónico remoto, al hacer uso de Internet como vehículo de comunicación del sufragio, tiene *la capacidad potencial de alterar* —tan sólo en los supuestos de voto electrónico integral— la configuración Administrativa de las circunscripciones electorales, haciendo posible el

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

concepto teórico de «*circunscripción administrativa virtual electrónica*». Merced a lo cual, podrían diseñarse nuevas modalidades de circunscripción que pudiesen resolver vetustos problemas, como el de la *igualdad* del sufragio, por ejemplo. Ahora bien, simultáneamente, se abrirían nuevas fuentes de inestabilidad política, derivadas de la determinación de los criterios de regulación de tales circunscripciones administrativas virtuales, tales como: adaptación de los candidatos de los partidos políticos a la nueva estructura, segregar y reagrupar colectivos de ciudadanos en base a nuevos criterios de organización «*topológica*», reordenación de las estructuras de partido en relación con las exigencias de las nuevas demarcaciones virtuales (hemos de pensar, no obstante, que estas modificaciones no son onerosas temporal o espacialmente, pues son tan virtuales, como lo sería la estructura impuesta). En conexión con lo anterior, habría que situar las *problemáticas desviaciones* derivadas de la posibilidad de conocer (descubrir) el sentido del voto de los electores, en el marco de *inseguridad* de los sistemas de voto electrónico remoto; lo que complicaría tales diseños virtuales de las circunscripciones electorales. Es decir, la «creatividad institucional» dispondría de un medio *dúctil,* capaz de dar respuesta a algunas exigencias en materia electoral irresueltas en base a los actuales regímenes de voto presencial, si bien, en el otro extremo de la balanza, se abren, a su vez, más que temibles amenazas que pueden poner en riesgo el sistema completo de elección de candidatos y, con ello, graves problemas para garantizar la estabilidad democrática, que es uno de los objetivos prioritarios a los que debe atender un régimen electoral nacional. Este problema tiene su origen en la pérdida de la neutralidad de la Administración Electoral electrónica, ya que de ella desaparece toda la organización administrativa de control y regularidad de base personal, que aseguran la integridad del proceso de voto, y que integraba la Administración Electoral presencial, lo que sería causa, y en parte efecto, de la ductilidad anteriormente señalada.

18. El voto electrónico por Internet debe quedar, en virtud de los anteriores considerandos, expresamente prohibido. Dado que no es posible garantizar, en base a tal tecnología, los principios esenciales que debe respetar, en todo caso, el sistema electoral nacional. La ***Universalidad*** no queda garantizada, si el sufragio se condiciona a una técnica específica de voto electrónico remoto. La ***Igualdad*** de sufragio experimenta modulaciones que la desvirtúan fundamentalmente en los supuestos de voto electrónico remoto. El voto ***Directo*** deja de serlo si puede ser

transferido «*virtualmente*». La ***Libertad*** de sufragio deja de ser tal libertad, si la formación de la voluntad del votante no puede ser asegurada jurídicamente. Por último, el voto ***Secreto*** tampoco lo será, si se puede interceptar, descubrir o conocer mediante cualquier técnica el contenido del sufragio. Por otro lado, es prudente dedicar por parte de la doctrina mayor atención al fenómeno que hemos pretendido describir, ya que, con o sin las modificaciones técnicas que lo transformen en una herramienta válida para el sufragio, en el medio plazo, se presentará como una *opción política de difícil contención*. Ya que como señalara atinadamente Constant: «*Siempre que se presenta una posibilidad de ganancia, la industria se aprovecha y, bajo cualquier gobierno que no sea una absoluta tiranía, la industria es invencible*».

19. Es de la máxima importancia que los líderes políticos recuerden permanentemente aquellos argumentos prudentes que Voltaire le dirigía a Rousseau y Rousseau a Voltaire sobre, posiblemente, dos de las causas fundamentales de los errores en el raciocinio de los hombres. Señalaba Voltaire: «*Los grandes crímenes han sido cometidos por célebres ignorantes. Lo que hizo y lo que hará siempre de este mundo un valle de lágrimas es la insaciable avidez y el irremisible orgullo de los hombres*». Por su parte, respondía Rousseau: «*Busquemos la primera fuente de los desórdenes de la sociedad y encontraremos que todos los males de los hombres proceden del error más bien que de la ignorancia, y que lo que sabemos nos perjudica mucho menos de lo que creemos saber*». Es obligación de las autoridades públicas no presumir sino saber, no creer sino conocer, ya que Voltaire y Rousseau tenían ambos razón: el orgullo de la ignorancia basado en lo que se cree saber, conduce a errores a menudo catastróficos, evitables, si una honesta y sana duda se impone *profilácticamente* sobre lo que se desconoce. La *autorestricción* debe ser una fórmula objetiva de aproximación a una problemática como la que hemos venido exponiendo. En palabras más directas y gráficas de Jefferson: «*Es mejor mantener al lobo fuera del corral que confiar en ponerle bozal una vez dentro*».

© UNED. *Revista de Derecho Político*
N.º 77, enero-abril 2010, págs. 213-249

Title

«ELECTRONIC VOTING BY INTERNET AND RISKS FOR THE DEMOCRACY II».

Summary

1.INTRODUCTION. 2.STRUCTURE OF THE ARTICLE. 3.GENERAL CONSIDERATIONS ON THE ELECTRONIC REMOTE VOTE IN RELATIONSHIP WITH THE ORGANIC LAW OF THE ELECTORAL GENERAL REGIME. 3.1.ELEMENTS OF THE ELECTRONIC REMOTE VOTE. 3.2. IMPLICATIONS FOR THE SAFEGUARD OF THE GUARANTEES OF THE VOTE. 3.3. A PROPOSAL OF SOLUTION. 3.4. ¿IT ITS POSSIBLE TO INTERPRETING AS FUNDAMENTAL RIGHT OF LEGAL SETUP THE CIVIC PARTICIPATION IN THE ELECTORAL ADMINISTRATION?. 4. EXPERIENCE OF THE ELECTRONIC REMOTE VOTE. 5. RECOMMENDATION OF THE COMMITTEE OF MINISTERS ON LEGAL, OPERATIVE AND TECHNICAL STANDARDS FOR THE ELECTRONIC VOTE ON SEPTEMBER 30, 2004. 6. ELECTRONIC PRESENT VOTE AND MACHINES OF VOTE. 7. CONCLUSIONS.

Palabras clave

Voto electrónico; voto electrónico mediante Internet; derecho de participación política; democracia electrónica; software electoral; administración electoral; mesa electoral; datos de tráfico electoral; neutralidad del sistema electoral; seguridad del sistema electoral; fraude electoral electrónico; sufragio electrónico; censo electoral electrónico; máquinas de voto; discriminación electoral; desigualdad electoral; secreto del voto; dirección de ajuste; circunscripción electoral; circunscripción virtual electrónica; proceso electoral; separación de poderes; propiedad intelectual; protección de datos; garantía institucional; robo de votos; alteración de votos; venta del voto; compra venta del voto; coacción electoral; suplantación de identidad; elecciones libres.

Key words

Electronic vote; electronic vote by Internet; right of political participation; democracy; electronic democracy; electoral software; electoral administration; polling station; data of electoral traffic; neutrality of electoral system; electoral system security; electoral electronic fraud; electronic voting; electronic electoral census; vote machines; electoral discrimination; electoral inequality; secrete of the vote; wrap address;

electoral district; electronic virtual district; electoral process; separation of powers; intellectual property; data protection; institutional guarantee; robbery of votes; alteration of votes; sale of the vote; sale and purchase of the vote; electoral coercion; supplant of identity; free elections.

Resumen

El objeto de este trabajo es poner de manifiesto la inadecuación que existe entre los sistemas de voto presencial y manual, y las fórmulas de voto electrónico remoto o mediante Internet. Del estudio de ambas técnicas, completamente distintas, surgen importantes problemas en relación con el modo y forma de preservar las garantías jurídicas entre las dos estrategias de sufragio electoral. El proceso electoral convencional ha garantizado históricamente, con efectividad, el respeto de un conjunto de importante exigencias amparadas por la Constitución: libertad de sufragio; igualdad de voto; y secreto, entre otros principios relevantes. El problema que estudiamos es determinar cómo pueden garantizarse estos principios mediante el uso de tecnologías propietarias, que además no han alcanzado el grado de madurez técnica imprescindible para asegurar tales principios, al menos con tanta efectividad, si no más, que la alcanzada en el marco del sufragio presencial y manual.

De la inadecuación entre ambas técnicas, surgen problemas de discriminación, pérdida del voto, concentración del poder por parte de los Gobiernos. Es decir, efectos de la pérdida de seguridad, eficiencia y neutralidad del proceso de voto. La participación de los ciudadanos en la Administración Electoral, como expresión de una fórmula cualificada de participación de los ciudadanos en los asuntos públicos, puede desaparecer, con el perjuicio que tal medida representaría para la limitación de tal derecho fundamental, que además es el fundamento del funcionamiento neutral y eficiente de la Administración Electoral. Una pérdida doble del derecho de participación, que en el marco jurídico del sufragio se transforma en derecho a controlar la pureza e integridad del proceso electoral.

Abstract

The object of this work is to show the purpose of adequateness that exist between the systems of actual and manual vote, and the formulas of remote electronic vote or by means of Internet. From the study of both techniques, completely different, important problems arise in connection with the mode and shape of preserving the juridical guarantees between the two strategies of electoral suffrage. The conven-

tional electoral process has guaranteed historically, with effectiveness, the respect of an important set of exigencies protected by the Constitution: freedom of suffrage; vote equality; and secret ballot, among other excellent principles. The problem which we studied is to determine how these principles can be guaranteed by means of the use of proprietary technologies that in addition, have not reached the degree of technical maturity essential to assure such principles, with as much effectiveness, if not more, than the reached one within the framework of the actual and manual suffrage.

From the purpose of adaptation between both techniques, discrimination problems arise: loss of the vote; concentration of the power on the part of the Governments. That is to say, effects of the lost of security, efficiency and neutrality of the vote process. The participation of the citizens in the Electoral Administration, like expression of a qualified formula of participation of the citizens in the subjects public, can disappear, with the damage that such measurement would represent for the limitation of so fundamental right, that in addition, it is the foundation of the neutral and efficient operation of the Electoral Administration. A double lost of the right to participation, that within the juridical framework of the suffrage it is transformed also into right to control the purity and integrity of the electoral process.