TECNOLOGÍA DIGITAL

Alfonso Ayala Sánchez

I. Introducción

Actualmente el mundo se encuentra en el inicio de una nueva etapa de desarrollo. Muchos escritores, críticos e investigadores han denominado a esta fase, que incluye los últimos años del siglo XX y los primeros del siglo XXI, como la era de la información.[1] Este periodo también conocido como la era digital, se caracteriza por la habilidad de los individuos de transferir información libremente, y al mismo tiempo, de tener acceso casi instantáneo a un acervo de conocimientos que anteriormente sólo se encontraban en grandes bibliotecas, museos o en las universidades más prestigiadas del planeta.[2] La era de la información ha sido posible gracias a la proliferación de tecnologías emergentes de la información y comunicación, y la capacidad que dicha tecnología le confiere al usuario para romper las barreras de la distancia, el tiempo, el lugar, y las restricciones físicas para procesar información y tomar decisiones inherentes a la condición humana.[3]

De acuerdo a Daniel S. Papp y David S. Alberts,[4] los últimos 150 años pueden considerarse como un periodo continuo de revolución de la información con tres fases distintivas:

- La primera fase de la revolución de la información moderna comenzó a mediados del siglo XIX y se extendió por aproximadamente 100

[1] Stewart, Thomas A., "Welcome to the Revolution", en Alberts, David S. y Papp, Daniel S. (comps.), *The Information Age: An Anthology on its Impact and Consequence,* CCRP Publication Series, 1997, pp. 5-12, *http://www.dodccrp.org/files/Alberts_Anthology_I.pdf.*

[2] Information Age, *Wikipedia*, *the free encyclopedia. http://en.wikipedia.org/wiki/Information_Age.*

[3] Papp, Daniel S. *et al.*, "Historical Impacts of Information Technologies: An Overview", Alberts, David S. y Papp, Daniel S. (comps.), *The Information Age: An Anthology on its Impact and Consequence,* CCRP Publication Series, 1997, pp. 13-35, *http://www.dodccrp.org/files/Alberts_ Anthology_I.pdf.*

[4] *Idem.*

años, y tuvo como característica principal el ampliar las comunicaciones en todo el mundo. Durante este periodo se desarrolló la tecnología para generar electricidad de forma masiva y para transportarla a grandes distancias. Los principales inventos fueron el telégrafo, el teléfono y la radio.

- La segunda fase se extiende desde la mitad del siglo XX hasta el inicio de la década de 1980. Es en este periodo que se inventa la televisión, la primera generación de computadoras (enormes y muy lentas para los estándares actuales) y los satélites, lo que trajo como consecuencia que los eventos de importancia mundial se transmitieran de manera casi inmediata a una gran cantidad de observadores.
- La tercera fase, que es en la que nos encontramos, implica un cambio en el modelo económico, pasando de uno centrado en los avances heredados por la Revolución Industrial a otro basado en la manipulación de la información. Esta etapa, caracterizada por la continua innovación de la tecnología digital, comenzó a finales de 1970 con la invención de las microcomputadoras, mejor conocidas como computadoras personales. Esta fase es a la que comúnmente se hace referencia como la era digital.

Las computadoras personales cambiaron profundamente el mundo moderno. Su desarrollo fue posible gracias a la invención de la tecnología de circuitos integrados (o microchips) que redujo de manera sustancial el tamaño y el costo de los aparatos. Una ventaja adicional la representó el hecho de que desde el inicio contaron con sistemas operativos relativamente interactivos y amigables con el usuario, lo que sin duda ayudó a que rápidamente fueran adquiridas por laboratorios y centros de cómputo universitarios.[5] Ya desde 1973 la minicomputadora Xerox Alto representó un hito en el desarrollo de las computadoras personales al contar con una interfaz gráfica, un monitor de alta resolución, una memoria con gran capacidad de almacenamiento tanto interno como externo, un mouse y un software propio.[6] El subsiguiente desarrollo de los microprocesadores permitió abaratar aún más la producción de las microcomputadoras, pues incorporaron las funciones de la Unidad Central de Procesamiento (CPU) de la computadora en un solo circuito integrado.

[5] "History of Personal Computers", *Wikipedia*, *the Free Encyclopedia*. *http://en.wikipedia. org/wiki/History_of_personal_computers*

[6] Rheingold, Howard, "Tools for Thought: the History and Future of Mind-Expanding Technology", *The MIT Press,* 2000, p. 360.

Como resultado de la reducción tanto del precio como del tamaño de las computadoras personales, muchas familias de clase media en los países desarrollados pudieron tener acceso a ellas, con lo que su uso se masificó para inicios de la década de 1990. Este hecho coincidió con la creación, por parte del científico británico Timothy Berners-Lee, del sistema de documentos de hipertexto conocido como *World Wide Web*, lo que popularizó el uso del sistema global de redes computacionales interconectadas conocido como Internet, y la convirtió en una verdadera red mundial. La Internet, sucesora de la ARPANET, fue ideada por los militares norteamericanos como una red que pudiera conectar un gran número de computadoras a fin de resistir un ataque al sistema de comunicaciones de Estados Unidos. Las primeras aplicaciones para Internet creadas por DARPA fueron el correo electrónico y los protocolos de transferencia de archivos. Sin embargo, con el tiempo, este sistema de defensa se introdujo en algunas universidades, con lo que su aplicación militar dio paso a una de carácter civil. Pocas personas imaginaron en ese entonces el enorme impacto que la red de redes tendría en la civilización actual.[7]

Gracias a la masificación del uso de las computadoras personales y del Internet, se volvió indispensable digitalizar toda la información posible. La creación de procesadores de texto, escáners y programas digitalizadores de audio y video, entre otros, han permitido almacenar y al mismo tiempo distribuir cantidades enormes de información que de otra manera sería imposible hacer llegar a muchos usuarios. Libros completos se distribuyen de manera libre por la red; música, películas, programas de cómputo, son adquiridos ya sea sin costo o mediante un pago menor del que si se comprara el artículo en forma material. Y ahora, gracias a la convergencia digital, el desarrollo de la fibra óptica y la comunicación satelital, un mismo dispositivo puede funcionar como teléfono, televisor y computadora. Sin duda el mundo moderno no podría entenderse sin estas nuevas tecnologías.[8]

Estos cambios han creado una generación de jóvenes que se desenvuelve naturalmente con estas tecnologías porque creció con ellas y las ha hecho propias, y está obligando al resto de la sociedad a adoptarlas, o correr el riesgo de quedarse rezagados y al margen de los cambios culturales que se están generando en todos los ámbitos.[9]

7 Information Age, *op. cit.*

8 Negroponte, Nicholas, *Being Digital*, Nueva York, Alfred A. Knopf, 1995, pp. 11-20.

9 *Ibidem*, pp. 89-92.

La política como parte integral del quehacer social humano, no puede ser indiferente ante los sucesos actuales. Puesto que las ventajas que los aparatos digitales ofrecen son significativas, cada vez con mayor frecuencia los políticos utilizan estas tecnologías para darse a conocer o propagar sus ideas. Las Tecnologías de Comunicación e Información (TIC's) tienen un enorme potencial para el fortalecimiento de la participación ciudadana y la configuración de la democracia en la medida en que facilita la recopilación, difusión, intercambio y coordinación de la información pública relevante así como de las ideas.[10]

Como ejemplo del papel actual que juegan las nuevas tecnologías en los procesos electorales recordemos que el ahora presidente de los Estados Unidos, Barack Obama, cambió la manera en la cual se utiliza la Internet para fines electorales: recurrió a los medios sociales para conectar directamente con las personas que lo apoyaban desde abajo, desde el inicio del proceso electoral, algo que a la postre resultó vital para el éxito de su campaña.[11] Y este año, al hacer pública su pretensión de reelegirse, decidió hacerlo a través de un video subido al servidor de YouTube.[12]

Las instituciones electorales en los países democráticos también han tratado de aprovechar las oportunidades que esta era digital brinda, si bien muchas veces no con el éxito deseado. Aunque el uso de las nuevas tecnologías en el ámbito electoral ofrece enormes posibilidades de participación a los ciudadanos, hasta hace poco existían restricciones logísticas que limitaban su utilización debido a la falta de un software que brindara suficiente seguridad y de un hardware que fuera amigable con el usuario. Sin embargo, los avances recientes en los instrumentos digitales han permitido que un número cada vez mayor de ciudadanos participe de forma más directa e inmediata en las elecciones, lo que supone un progreso para los sistemas democráticos en el mundo.

No obstante, el libre acceso a la información aunado a la aparición de las redes sociales plantean nuevos retos tanto para los partidos políticos tra-

[10] Kossick, Robert M., "The Role of Information & Communication Technology in Strengthening Citizen Participation & Shaping Democracy: An Analysis of Mexico's Initial Experience & Pending Challenges", *Information Technology in Developing Countries,* vol. 13, núm. 1, 2003, pp. 1-43, *http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan009905.pdf.*

[11] Mehta, Seema, "The Rise of the Internet Electorate", *Los Angeles Times*, 18 de abril de 2011, *http://www.latimes.com/news/nationworld/nation/la-na-social-media-V20110418*

[12] Barack Obama 2012 Campaign Launch Video – "It Begins With Us". *http://www.youtube.com/watch?v=f-VZLvVF1FQ.*

dicionales como para los gobiernos democráticos y sus instituciones electorales. En un mundo en crisis donde los representantes de los partidos políticos muchas veces son vistos como los generadores de los conflictos, como ineptos o como los testaferros de intereses antidemocráticos y de poderes fácticos, un grupo cada vez mayor de ciudadanos está canalizando su participación a través de grupos sin vinculación partidista, que parecen responder de forma más adecuada a la ciudadanía, lo que está poniendo en crisis al sistema político-electoral de muchos países. Las instituciones electorales no deben de quedar al margen de los cambios tecnológicos, a riesgo de ser percibidas como obsoletas, además de onerosas. Si se manejan apropiadamente las tecnologías digitales pueden ser utilizadas para alcanzar a grupos que no están en contacto con la vida política, incluyendo a la juventud, los grupos marginados y las minorías.[13]

II. Fraude y tecnología digital

En los países con sistemas de gobierno democráticos, las elecciones libres son una parte fundamental de la vida política nacional. Mediante elecciones la ciudadanía decide qué grupos detentarán el poder por un determinado periodo de tiempo, y puede influir en las políticas públicas, aunque sea de manera limitada. Es por estas razones que algunos grupos de interés, ya sean políticos o económicos, han tratado en diversos países a lo largo de la historia, de obtener el poder de forma fraudulenta, cuando no francamente violenta. El fraude electoral, como concepto criminal, involucra una irregularidad sustantiva relativa al acto de votar (como el soborno, la intimidación o la falsificación), que tiene el potencial de manchar una elección.[14]

Aunque las acciones consideradas como violaciones electorales varían dependiendo de la legislación de cada país, de manera general se pueden catalogar como delitos los siguientes:

Compra de votos, que consiste en pagarles a los votantes para registrarse a votar o para participar en una elección, con la intensión de favorecer a un candidato en particular.

Intimidación de los votantes, en un contexto criminal, consiste en impedir que un votante participe en una elección a fin de que uno de los candidatos con-

[13] Negroponte, Nicholas, *op. cit.*, pp. 163-171.

[14] Donsanto, Craig, "Corruption of the Election Process under U.S. Federal Law", Álvarez, R. Michael *et al.*, (comps.), *Election fraud. Detecting and deterring electoral manipulation*, Washington D. C., Brookings Institution Press, 2008, pp. 21-36.

tendientes reciba menos votos, o de forzar a un votante a participar en dicha elección mediante amenazas de represalias físicas o económicas.

Votación ilegal, cuando un votante que no está habilitado para votar en una elección se hace pasar por otro votante que sí puede hacerlo pero que no acudirá a sufragar en dicha ocasión.

Alteración ilegal de las urnas, cuando el personal encargado de las casillas modifica de alguna manera los votos, ya sea introduciendo irregularmente boletas marcadas para diluir los votos válidos con inválidos, entregando falsas tabulaciones de los votos emitidos o previniendo que sufragios válidos sean contabilizados.

Fraude en el registro de votantes, ya sea al presentar nombres o direcciones ficticios ante el padrón electoral, al permitir que individuos inhabilitados para votar lo hagan (como menores de edad o presos), o inscribir en el registro de votantes a migrantes ilegales con el fin de alterar la elección.[15]

Como un número importante de irregularidades implican la alteración o incluso la desaparición de boletas electorales, desde hace varias décadas existe un debate sobre cómo lograr que los procesos electorales sean más seguros sin que se pierda el elemento de secrecía del voto. Y es aquí donde las tecnologías digitales han comenzado a jugar un papel cada vez más importante.

Si bien es verdad que de manera general los ciudadanos ven de forma positiva la utilización de tecnologías digitales en los procesos electorales, debido a algunas malas experiencias previas existe un cierto temor de que estos aparatos terminen siendo más fácilmente alterables que las antiguas boletas de papel, pues en muchos casos no existen medios materiales para corroborar la veracidad y la cantidad de votos emitidos a favor de un candidato en particular.[16]

Es de llamar la atención que la mayor suspicacia hacia las nuevas tecnologías provenga no de la ciudadanía en general o de los especialistas electorales, sino de la comunidad de técnicos y expertos informáticos, pues ellos argumentan que los cuerpos electorales están sobreestimando la confiabilidad de la tecnología digital y simplemente asumen que resolverá los problemas existentes, y al mismo tiempo ignoran el potencial que existe para

15 *Idem.*

16 Ansolabahere, Stephen *et al.*, "Residual Votes Attributable to Technology", *The Journal of Politics*, vol. 67, núm. 2, 2005, pp. 365-389.

la aparición de consecuencias no previstas y nuevas vulnerabilidades.[17] Los funcionarios electorales tienden a racionalizar que los sistemas costosos y modernos sólo necesitan ser adquiridos e implementados, y que los problemas al momento de votar serán mínimos, algo que ha demostrado ser un error si no va acompañado de una capacitación importante de los funcionarios de casilla.[18]

Como resultado del deseo de reducir al mínimo las posibilidades de la comisión de fraude electoral, la aplicación alrededor del mundo de nuevas tecnologías en materia electoral ha buscado aumentar la confiabilidad, la transparencia, abatir el abstencionismo y reducir la cantidad de votos nulos en los comicios. Entre las principales innovaciones tecnológicas, ya aplicadas a elecciones en diversas partes del mundo, podemos encontrar las siguientes:

[17] Moynihan, Donald P., "Building Secure Elections: e-Voting, Security and Systems Theory", *Public Administration Review*, vol. 64, núm. 5, 2004, pp. 515-528.

[18] Álvarez, R. Michael *et al.*, "Studying Elections: Data Quality and pitfalls in Measuring the Effects of Voting Technologies", *VTP Working Paper*, núm. 21, 2004, pp. 1-19, *http://www.vote. caltech.edu/drupal/files/working_paper/vtp_wp21.pdf.*

Dispositivos de escaneo óptico y digital. Pueden ser utilizados en las casillas de votación o en un área de conteo designada para escanear las papeletas de votación. Normalmente se utiliza para mejorar la exactitud del proceso de recuento y reducir los posibles errores manuales. Sin embargo, la calidad del conteo depende de que la boleta de votación haya sido marcada correctamente y de la calidad de la tinta utilizada por el votante.[19]

Figuras 1-4
Diversos dispositivos de escaneo óptico y digital
(imágenes de libre distribución en Internet)

19 Álvarez, R. Michael y Hall, Thad E., *Electronic Elections: The Perils and Promises of Digital Democracy*, Princeton University Press, 2008, pp. 114-124.

Equipos electrónicos de grabación directa (Direct Recording Electronic Computers o DRE's). De manera simplificada, son máquinas o computadoras encargadas de registrar los votos y al mismo tiempo de almacenarlos. El usuario emite su voto al pulsar una pantalla táctil (con una pluma especial o con sus dedos) o al teclear uno o más botones. Comúnmente los DREs se encuentran instalados en los colegios electorales o las casillas de votación.[20]

Figuras 5-8
Diversos tipos de DRE's (imágenes de libre distribución en Internet)

20 *Idem*.

Internet. Existen diversas modalidades:

- Votación remota de Internet: se realiza mediante una computadora que no está bajo el control físico de la autoridad electoral, a través de una conexión de Internet.
- Votación en quioscos de Internet: el voto se emite en lugares designados previamente utilizando una computadora bajo el control físico del instituto electoral mediante Internet.
- Votación en las casillas electorales: la emisión del voto se realiza en las casillas normales el día de la elección, pero en vez de utilizar las antiguas boletas de papel, se usan computadoras con conexión de red.[21]

III. Voto electrónico

Adicional a los problemas ya mencionados relativos al fraude electoral, el voto tradicional presenta una serie de inconvenientes de orden administrativo, tales como los altos costos de impresión y seguridad de las boletas, el traslado de las mismas desde todas las casillas de los distintos distritos electorales hasta el centro de recepción de la autoridad electoral, y la lentitud de los conteos realizados por los funcionarios de casilla, los cuales muchas veces cometen errores.[22]

Otro tipo de problemas con las boletas de papel involucran a los propios electores, ya que en muchas ocasiones las papeletas causan confusión en el usuario, quien termina votando por candidatos diferentes a los de su preferencia, anulando su voto al seleccionar más de una opción, o votando por los candidatos colocados en la parte de arriba de la hoja de votación (el ya mencionado *falloff*). Por último, existe el problema de la falta de accesibilidad del voto en papel para aquellas personas que presentan alguna discapacidad visual o motriz.[23]

Los problemas antes expuestos pueden resolverse utilizando las tecnologías digitales de votación para que los ciudadanos emitan su sufragio, lo que se conoce como voto electrónico o *e-voting*. En principio, las urnas electrónicas hacen más fácil y seguro el conteo de los votos, eliminando los gastos

[21] Álvarez, R. Michael y Hall, Thad E., *Point, Click & Vote: The Future of Internet Voting*, Washington D. C., Brookings Institution Press, 2004, pp. 4-7.

[22] Liburd, Soyini D., "An N-Version Electronic Voting System", Massachusetts Institute of Technology, *VTP Working Paper*, núm. 17, 2004, pp. 9 y 10, *http://www.vote.caltech.edu/drupal/files/ thesis/n_version_evs.pdf.*

[23] *Ibidem*, pp. 11 y 12.

de traslado y seguridad. También ayudan a crear una interfaz más accesible para el usuario, permitiéndole cambiar el tamaño de la letra y los colores, además de que los elementos multimedia pueden traducir los contenidos para que puedan ser utilizados por personas con capacidades diferentes.[24]

A pesar de todas estas ventajas, existe en algunas personas la idea de que los diversos tipos de voto electrónico presentan vulnerabilidades que terminarían por alterar el resultado de las elecciones.[25] En 2001, investigadores del *Caltech/MIT Voting Technology Project* enumeraron las preocupaciones de seguridad concernientes al voto electrónico por parte de los ciudadanos:[26]

- La pérdida de apertura, al ya no poder ver el conteo de los votos.
- La pérdida de la habilidad para muchas personas de involucrarse en el proceso electoral.
- La pérdida de la separación del control del proceso, pues toda la preponderancia de la elección recae sobre la máquina de votación o su controlador.
- La falta de sistemas de redundancia y de una verdadera auditabilidad.
- La falta de control público.

El investigador Michael Shamos analizó algunos de los argumentos que se han presentado en contra del *e-voting*, resumiéndolos de la siguiente manera:[27]

- Las máquinas de votación electrónicas son "cajas negras", cuyo funcionamiento es opaco para el público y cuya retroalimentación con el votante es generada por la propia caja negra. Por tanto, el saber si las máquinas están funcionando correctamente no puede ser verificado independientemente.
- Ninguna cantidad de auditorías al código pueden detectar todos los programas maliciosos o los errores en el sistema.

24 *Idem.*

25 *Ibidem*, pp. 13 y 14.

26 Baltimore, David y Vest, Charles M., *Voting: What is, What Could be,* Caltech/MIT Voting Technology Project, 2001, pp. 1-92, *http://vote.caltech.edu/drupal/files/report/voting_what_is_ what_could_be.pdf.*

27 Shamos, Michael I., "Paper Versus Electronic Records – An Assessment", *Proceedings of the 14th ACM Conference on Computers, Freedom and Privacy*, Berkeley, 2004, pp. 1-27, *http://vote.nist.gov/threats/papers/paper_v_electronic_records.pdf.*

- Los *hackers* han demostrado ser lo suficientemente hábiles como para irrumpir en numerosos sitios web, ilustrando la vulnerabilidad de los medios electrónicos.
- Las compañías que fabrican la urnas electrónicas pueden estar dirigidas por individuos con intereses partidistas definidos, y esos individuos pueden ordenar que las máquinas sean programadas para grabar y contar votos de una manera tendenciosa.
- Han habido muchas fallas involucrando máquinas para votar en elecciones alrededor del mundo que han resultado la pérdida permanente de votos, lo que posiblemente haya cambiado los resultados electorales, ilustrando la fragilidad de la tecnología para votar.

Esta serie de argumentos en contra de la utilización de nuevas tecnologías de votación refleja un temor por parte de la mayoría de la población que es común a todas las tecnologías desarrolladas en la Era Digital: la indefensión ante máquinas tan complejas que el usuario difícilmente puede entender su funcionamiento en su totalidad.

Por lo tanto, en este punto los operadores pertenecientes a los institutos electorales desempeñan un papel clave en las elecciones. Si ellos realizan correctamente su trabajo de auxiliar a la gente que todavía no está familiarizada con los nuevos sistemas, muchas de las reticencias pueden ser superadas. Pero si su propia capacitación no fue la apropiada, la presión en un momento de incertidumbre, el desconocimiento del correcto funcionamiento de las máquinas o las actitudes negativas hacia los procedimientos indicados con anterioridad, además de las soluciones improvisadas, pueden ocasionar un problema muy serio que ponga en duda la votación.[28] Los sistemas de votación democráticos deben de tener ciertos estándares de seguridad, secrecía, confiabilidad, precisión, eficiencia, integridad y equidad, por lo que los retos administrativos de los regímenes democráticos son mucho más complejos que simplemente la implementación de nuevas tecnologías digitales.[29]

Sin embargo, no basta sólo con preparar mejor a los funcionarios de casilla. La duda válida sobre la confiabilidad del conteo de los votos debe de ser atendida. Algunos promotores del voto electrónico como Rebecca Mer-

[28] Selker, Ted, "Processes Can Improve Electronic Voting: a Case Study of an Election", *VTP Working Paper*, núm. 19, 2004, pp. 1-10, *http://www.vote.caltech.edu/drupal/files/working_ paper/vtp_ wp19.pdf.*

[29] Norris, Pipa, *E-Voting as the Magic Ballot? The Impact of the Internet on Electoral Participation and Civic Engagement,* Harvard University, John F. Kennedy School of Government, 2004, pp. 1-21.

curi[30] y R. Michael Álvarez han propuesto utilizar los votos impresos como un candado de seguridad: el voto es impreso en papel para que la persona pueda verificar su voto, con lo cual el sistema le da un rastro auditable al votante y éste puede retirarse tranquilamente de la casilla sabiendo que su voto será tomado en cuenta.

La modernización de los procesos electorales no sólo significa la adquisición de tecnología, sino ésta se debe de acompañar con un proceso eficiente del ejercicio de sufragar respetando las características que definen a la democracia por lo cual lo convierte en legítimo. Lo anterior implica afinar el funcionamiento de las instituciones y posteriormente evaluar cuáles son las herramientas a través de las cuales se puede efectuar un compromiso con la calidad. El propósito principal para incluir a los medios tecnológicos modernos en el sistema de votación, es entregar un medio que sea más difícil de quebrantar para reducir las posibilidades de que se cometa un delito electoral, de ahí su legitimación.

IV. Código fuente

Uno de los debates inevitables en la implementación de un sistema de votación electrónico, es la auditoría del código de funcionamiento del software que se utiliza en la jornada electoral.

El código fuente de un programa informático o software es un conjunto de líneas de texto que son las instrucciones que debe seguir la computadora para ejecutar dicho programa. Por tanto, en el código fuente se describe el funcionamiento completo del sistema informático.[31]

Se dice que un código fuente es abierto o libre cuando el programador que lo diseña establece permisos para que el sistema esté disponible para que cualquiera pueda estudiarlo, modificarlo o reutilizarlo. En contraposición, el software propietario o cerrado es aquel que no cuenta con ninguno de estos permisos y se restringe sólo al grupo de ingenieros más allegados al desarrollo del sistema.

Como Stewart Fist hace notar,[32] esto constituye una espada de dos filos: el hacer que el código sea abierto, invita a toda la comunidad de informá-

30 Mercuri, Rebecca, "Inside Risks: Voting Automation (Early and Often?)", *Communications of the ACM*, vol. 43, núm. 11, p. 173.

31 Código Fuente, *Wikipedia, la enciclopedia libre*. *http://es.wikipedia.org/wiki/Código_fuente*

32 Fist, Stewart, "Mixed Reviews for E-Voting Systems", *Telecom Asia*, 1o. de marzo de 2004, *http://www.highbeam.com/doc/1G1-115034847.html*.

ticos, hackers, auditores, y universidades a probar la seguridad del sistema. Mientras más gente trabaje en garantizar su seguridad, más confiable llegará a ser el software. Sin embargo, queda abierta la posibilidad de que una falla permanezca sin detectar y, dado que el código fue hecho público, su vulnerabilidad es evidente. Por otro lado, manteniendo el código restringido se corre el riesgo de que durante el corto tiempo que sea puesto en línea alguien no autorizado pueda acceder a él explotando alguna debilidad en el sistema, partiendo de la premisa de que sólo un grupo reducido de personas tuvo tiempo para detectar si el sistema era a prueba de fallos o no. Todo esto, además de suponer que no hay ningún código existente que sea a prueba de fallos. Scott Bradner opina que el mejor sistema para operar con una urna electrónica es bajo un código abierto, con un sistema operativo especialmente diseñado o para eliminar el código innecesario y debilidades de seguridad inherentes.[33] Jason Kitcat[34] propone una solución parcial. Su propuesta consta de mantener un sistema de código cerrado, utilizando a un grupo selecto de especialistas que evalúen la seguridad del sistema, ya que, según él, los sistemas públicos son más débiles que los privados. Sin embargo, este grupo de expertos debería estar constituido por aquellos que sean los más capacitados.

¿Cuánta información bancaria se transmite a través de Internet diariamente?, ¿millones de datos?, ¿trillones? Aún asumiendo el riesgo de que existe el robo electrónico de dinero, millones de usuarios alrededor del mundo siguen utilizando los servicios de Internet para manejar su dinero, aun cuando trasladar dinero a través del Internet significa exponerlo a millones de usuarios de todo el mundo. El argumento clave es que los especialistas en seguridad han hecho un muy buen trabajo protegiendo a los usuarios contra el fraude y el robo de identidad.[35] Los bancos lo hacen, las gestoras de tarjetas de crédito lo hacen. Definitivamente los sistemas electorales también lo pueden hacer.

Entonces, si seguimos los argumentos expuestos, podemos decir con confianza que la implementación de los sistemas de recopilación de votos que no posean la vulnerabilidad inherente de Internet, reducirían los costos de su implementación, de la infraestructura necesaria, la capacidad huma-

33 Bradner, Scott, "Lessons from the E-Voting Mess", *NetworkWorld,* 10 de mayo de 2004, *http://www.networkworld.com/columnists/2004/0510bradner.html.*

34 Kitcat, Jason, "Source Availability and E-Voting: an Advocate Recants", *Communications of the ACM*, vol. 47, núm. 19, 2004, pp. 65-67.

35 Miller, Harris, "E-Voting Does Work", *eWEEK*, 13 de septiembre de 2004, *http://www. eweek.com/c/a/Government-IT/EVoting-Does-Work/.*

na requerida, y más importante, los riesgos inherentes al manejo electrónico de las elecciones. Este trabajo recalca la necesidad de:

- Fortalecer la democracia electoral a través de la mejora, depuración y certificación de los procesos involucrados en materia electoral.
- Una reforma electoral integral que cubra las debilidades de manejar ya sea un código abierto o uno restringido.
- Un sistema óptimo que encuentre un equilibrio de los beneficios de la tecnología digital en combinación con los procedimientos ya existentes.

Defensores de los derechos civiles y expertos en computación en Norteamérica están promoviendo que todos aquellos que planeen implementar o estén implementando sistemas de registro directo, conocidos como DRE's *(Direct Recording Electronic Voting Machines)* para sus sistemas de votación electrónica, implementen precauciones de seguridad inmediatas, incluyendo el contratar auditores de seguridad externos e independientes para que accedan al código fuente del sistema y lo evalúen.[36]

Uno de los ámbitos a auditar en el código es la seguridad. Los desarrolladores de sistemas realmente no tienen la percepción absoluta de las posibles fallas de seguridad que un sistema pueda tener, y durante el proceso de desarrollo deben de obligatoriamente asumir que una falla se puede presentar en el peor momento posible, y aún así, esto no tiene garantizada la seguridad de un sistema en absoluto.[37] Ésta es una de las razones por las cuales las auditorías tanto internas como externas son necesarias para incrementar la seguridad de un sistema, simplemente por el número de mentes enfocadas en encontrar debilidades en un sistema, se reduce la posibilidad de que una debilidad permanezca sin ser detectada.

La seguridad de los sistemas electrónicos de votación es la preocupación principal tanto de los opositores al movimiento del *e-voting* como de aquellos que lo apoyan. Aunque no se ha encontrado un método infalible para regular los sistemas electorales imperfectos, los rastros de papel son lo mejor que se tiene para asegurar auditorías; aún tomando en cuenta la debilidad que tiene de ser susceptible al fraude electoral, es importante no perder de vista que la boleta de papel limita la posibilidad de la inserción de votos falsos, mientras que con la urna electrónica esta posibilidad se incrementa indes-

36 Carlson, Chris, "E-Voting Safeguards Urged", *eWEEK*, 5 de julio de 2004.
37 Moynihan, Donald P., *op. cit.*, pp. 515-528.

criptiblemente.[38] Una elección tradicional requiere de un sistema complejo de gestores para desviar los resultados de una elección de boletas de papel, mientras que un pequeño grupo de ingenieros puede lograr el mismo resultado con un sistema de urnas electrónicas. Además se debe tomar en cuenta que hoy en día las elecciones tienden a ser mucho más cerradas, debido a las guerras mercadológicas libradas en las campañas electorales y a la mejor preparación de los candidatos. Esto ocasiona que una elección se pueda voltear al modificar unos cuantos cientos de votos en un puñado de distritos clave, lo cual a su vez requeriría solamente de un gran equipo de análisis y de un pequeño grupo de ingenieros especializados para asegurar una victoria electoral.[39]

La relación entre las instituciones electorales y los auditores externos debe estar debidamente regulada y legislada, para mantener protocolos de seguridad tanto en el funcionamiento de los sistemas, como en los procesos de gestión electoral. Los auditores no deben de estar relacionados en absoluto con aquellos que desarrollen los sistemas o los equipos de votación electrónica, ni con el instituto encargado de gestión administrativa; estos auditores deben de tener acceso a la totalidad del código fuente que se va a implementar en los sistemas por un tiempo determinado, y bajo la vigilancia de la empresa que desarrolló el sistema, la institución electoral y los partidos políticos.[40]

El argumento en contra (promovido por aquellos que desarrollan los sistemas) de utilizar auditorías externas para evaluar la seguridad de los códigos es que abriría una brecha en la seguridad de la gestión, pues un auditor podría intentar copiar el código y hacérselo llegar a las personas equivocadas. Este argumento es válido, pero no hay que olvidar que las empresas que desarrollan los sistemas están manejando un negocio, y el material sujeto a *copyright* debe ser protegido de observación innecesaria, por las mismas brechas de seguridad, pero con la intención de proteger una inversión y no con la intención última de servir a la ciudadanía. Estamos hablando de confiarle la democracia de la ciudadanía a una empresa que tiene el mejor interés en esconder posibles fallas que su sistema pueda tener para poder obtener la mayor ganancia de sus clientes, y al mismo tiempo proteger su inversión para que nadie pueda obtener ganancia de su trabajo; la postura de código

[38] Rothke, Ben, "E-Voting: It's Security, Stupid", *eWEEK*, 23 de agosto de 2004, *http://www.eweek.com/c/a/Government-IT/EVoting-Its-Security-Stupid/*

[39] Kearns, David, "Paper Trail Won't Cure E-Voting Ills", *NetworkWorld,* 6 de septiembre de *2004, http://www.networkworld.com/columnists/2004/090604kearns.html*

[40] Carlson, Chris, *op. cit*.

cerrado implica entonces dar la confianza a un proveedor privado cuyo interés principal no es la ciudadanía ni la democracia electoral.[41]

Una perspectiva importante del voto electrónico es el dinero. Los funcionarios electorales, al hacer una adquisición de equipo de esta naturaleza, deben buscar reducir el gasto presupuestal; mientras que los empresarios que producen estas tecnologías su objetivo es incrementar sus utilidades.[42] Ésta es una de las razones por las cuales vale la pena tomar en serio la propuesta de producir internamente las herramientas y la gestión de los procesos involucrados en los actos electorales. Esto incluye tanto al personal que interviene en los procesos hasta las herramientas utilizadas (boletas de papel o urnas electrónicas), en el procesamiento de votos efectivos y emisión de resultados finales. Si las instituciones electorales son capaces de manufacturar, preparar y gestionar sus propios procesos sin necesidad del *outsourcing*, entonces sólo requerirán de auditorías internas, externas y de las vigilancias de otras instituciones autónomas, como de la misma ciudadanía para garantizar:

- La autonomía de las instituciones electorales: con todo el dinero involucrado en la gestión de elecciones, es muy conveniente tener asegurado el nicho que una compañía tenga dentro del sistema; es por esta razón que el cliente se vería obligado a acudir a un solo proveedor para la actualización, mantenimiento y renovación de sistemas; todo esto se elimina si el proveedor de la tecnología es el gestor electoral mismo.
- La eficiencia de los productos emitidos (en este caso las elecciones).
- La transparencia y rendición de cuentas de los procesos a través de los cuales se obtienen estos productos: ante la obligación de transparentar los procesos, los desarrolladores del código están motivados a realizar un trabajo mucho más limpio dado que saben que su trabajo será hecho público, además de que el crédito obtenido por esta labor será mucho mayor; sin olvidar que si aparecen defectos en el producto, un incontable número de colaboradores voluntarios están disponibles para detectarlos y solucionarlos.[43]

Una posible solución sería constituir una serie de cuerpos independientes, formados por expertos en la materia (tanto de computación como en

[41] Kitcat, Jason, *op. cit.*, pp. 65-67.

[42] Mcnamara, Paul, "Readers Vote Nay", *NetworkWorld*, 23 de agosto de 2004, *http://www.networkworld.com/columnists/2004/082304buzz.html.*

[43] Kitcat, Jason, *op. cit.*, pp. 65-67.

material electoral) para garantizar una auditoría confiable y constante, a los sistemas que se planean utilizar.[44] Sin embargo, la constitución de tales cuerpos siempre estará a merced de aquellos que se encarguen de la organización de los mismos, ya sea si pertenece a la gestión electoral o si está desvinculado de la misma y pertenece al sector privado.

Existe una comunidad entera de científicos e ingenieros de disciplinas relacionadas con la tecnología digital que estarían más que contentos de ayudar a identificar, encontrar, depurar y eliminar los errores, las modificaciones malintencionadas, y las vulnerabilidades existentes de las máquinas electrónicas del voto. Sin embargo, la mayoría de la tecnología de *e-voting* es gestionada por software que yace bajo el paraguas de los derechos de autor, por lo cual los propietarios de tales derechos no están dispuestos a permitir que sea examinado por personal que no labore para ellos; en consecuencia, la verificación independiente de que el código funciona correctamente y de que nadie ha introducido un código alterado, no existe hasta el momento.

Una posible solución a este problema es la adquisición de los derechos de autor por el software utilizado por los sistemas junto con los aparatos. Es decir, una adquisición total del servicio, desde las máquinas, los manuales de construcción y mantenimiento, hasta los derechos de autor sobre la máquina, sus componentes (en caso de estar disponibles), y el software utilizado para que la máquina funcione. De esta manera se mantiene la independencia de la institución de gestión electoral, y da oportunidad al productor de obtener una ganancia.

Este argumento nos lleva de regreso al código abierto, dado que si no hay derechos de autor, entonces no hay problema de hacerlo público, tanto a un grupo limitado de especialistas, como a toda la ciudadanía en general. Es muy fácil encontrar errores en los sistemas de manejo de votos gracias a determinados indicadores obvios:[45]

- El número de votos que recibe un candidato.
- Si un candidato no recibe ningún voto.
- La proporción de votos emitidos, participación ciudadana y el padrón electoral.
- El voto residual.

Sin embargo, hay maneras de desviar votos mucho más sutiles y más difíciles de detectar, como cambiar votos de un candidato a otro sólo a intervalos establecidos (como uno de cada cincuenta).

44 Carlson, Chris, *op. cit*.

45 Moynihan, Donald P., *op. cit.*, pp. 515-528.

Aún así, el argumento más devastador a favor del voto electrónico es que hoy en día, cuando el *e-voting* es prevalente en países a lo largo y ancho del espectro económico, cultural y religioso, y la lucha por la obtención de elecciones limpias y transparentes está regida por la contienda entre los partidos políticos, no se ha encontrado una sola instancia verificable de manipulación mal intencionada en cualquier tipo de máquina de votación electrónica.[46]

V. Hardware

Los equipos electrónicos de votación directa (DRE's por sus siglas en inglés) son los sistemas más avanzados del voto electrónico.[47] Cuando los votantes llegan a la casilla electoral, se les entrega una tarjeta de memoria para insertarla en la máquina, que deben deslizar con un código de uso único, o verificar la identidad del elector a través de un medio biométrico o su identificación oficial, para posteriormente elegir a un candidato mediante una pantalla sensible al tacto o de un sistema de botones paralelos. Estos votos son intencionalmente tabulados por la máquina y contabilizados en una estación central.[48]

Los DRE's son sistemas más complejos, principalmente el resultado de un subsistema altamente complejo (el software usado para contar los votos), incluso los sistemas de computación más sencillos tienen cientos de miles de líneas de código, y la complejidad del software exige complejidad en el hardware; como resultado, el hardware para el *e-voting* es más complejo que las máquinas de votación utilizadas anteriormente, lo cual incrementa más los riesgos potenciales.[49] Al parecer, el paso a seguir para los procedimientos estadounidenses, con base en lo que ellos han aprendido a través de su experiencia con el voto electrónico, es adquirir DRE's que utilicen sistemas denominados Voter Verified Paper Audit Trail (VVPAT).[50] Hacer que los registros sean de naturaleza permanente (esto es, que no estén basados sólo en la memoria de la computadora) provee un medio por el cual un recuento

46 Miller, Harris, *op. cit*.

47 Fischer, Eric A. y Coleman, Kevin J., "The Direct Recording Electronic Voting Machine (DRE) Controversy: FAQs and Misperceptions", *CRS Report for Congress*, 2005, pp. 1-20, *http://digital.library.unt.edu/ark:/67531/metacrs8245/m1/1/high_res_d/RL33190_2005Dec14.pdf*.

48 Moynihan, Donald P., *op. cit.*, pp. 515-528.

49 *Idem.*

50 "Voter Verified Paper Audit Trail", *Wikipedia, the Free Encyclopedia. http://en.wikipedia. org/wiki/Voter_Verified_Paper_Audit_Trail*

preciso puede ser llevado a cabo; el asegurar la confiabilidad, la seguridad, y la verificabilidad de las elecciones públicas son factores fundamentales si es que se pretende asegurar una democracia estable, pues la conveniencia y la rapidez del conteo de los votos no son sustitutos para los resultados precisos y la confianza que la ciudadanía tiene en sus procesos e instituciones electorales.[51]

Para asegurar la precisión e imparcialidad de los procesos electorales, la *Association for Computing Machinery* (ACM) recomienda que todos los sistemas de votación (especialmente aquellos que estén basados en sistemas electrónicos de computación) se vean desarrollados, evaluados y auditados a través de una ingeniería cuidadosa, sistemas de seguridad extremadamente finos y rigurosos, y procesos de prueba que dictaminen si son aptos hasta el extremo en su diseño y su operación; además, los sistemas de votación deben de permitir que cada elector se asegure de que alguna forma de evidencia física (por ejemplo, un pedazo de papel) compruebe que su intención haya sido traducida en un voto efectivo de una manera precisa, de tal manera que esta evidencia sirva como un sistema de auditoría secundario que sea producido y almacenado por el mismo sistema.[52] Lo más importante de instaurar un sistema nuevo de votación es garantizar:

1) El anonimato del voto.
2) La traducción precisa de la intención del elector en un voto efectivo.
3) La imposibilidad de la manipulación malintencionada de los resultados.

Obviamente se tienen como referencia los resultados, con defectos y virtudes, obtenidos con la boleta de papel; es a través de esta referencia como se debe de evaluar si los DRE's exceden las expectativas que se tienen para el método tradicional. De acuerdo con diversos análisis realizados sobre este tema,[53] antes de seleccionar y aplicar un medio electrónico para emitir el voto se deben analizar cinco factores:

51 Grove, Jeff, "ACM Statement on Voting Systems", *Communications of the ACM*, vol. 47, núm. 10, 2004, pp. 69 y 70.

52 *Idem.*

53 Hite, Randolph C., "Electronic Voting Offers Opportunities and Presents Challenges", *United States Government Accountability Office*, 2004, pp. 1-47, *http://www.gao.gov/new.items/ d04766t.pdf.*

Categoría	*Justificación*
Seguridad	Este tema implica todas las medidas de seguridad que serán utilizadas antes, durante y después de la elección. Esto incluye la capacitación de funcionarios electorales y mecanismos para prevenir el robo de identidad de los votantes, así como la inviolabilidad de los votos emitidos y la legitimidad de los conteos. Por ejemplo, en el caso del voto electrónico, la encriptación de los datos de cada casilla al término de la jornada electoral.
Precisión	Esta categoría se refiere a la exactitud con la cual se efectúan y cuentan los votos. De hecho, implica una capacitación tanto del elector como del funcionario electoral, para la utilización efectiva de las nuevas herramientas tecnológicas. De tal forma, la precisión se refiere a la correcta instalación y uso de los mecanismos de votación por parte de los votantes y de los funcionarios electorales.
Facilidad de uso	Es el diseño de la interfaz entre el medio electrónico y el usuario. Para que el número de votos nulos o erróneos sea menor, el diseño debe ser accesible y sencillo en su uso por parte del votante y de los funcionarios electorales. También debe incluir mecanismos que permitan emitir el sufragio a votantes discapacitados. Sin embargo, esto puede llegar a incrementar el costo considerablemente.
Eficiencia	Este indicador se refiere a la velocidad y veracidad con la que un equipo recibe y cuenta los votos. De igual forma, se refiere al número de votantes que pueden utilizarlo a lo largo de la jornada electoral. Evidentemente, es necesario realizar un análisis costo-beneficio del equipo que se vaya a adquirir. La opción óptima será aquella que tenga la mayor capacidad al menor costo.
Costo	Existen tres aspectos que deben ser considerados previamente a la adquisición del equipo electrónico: la inversión inicial, el costo de mantenimiento y la vida útil. Una reexaminación de estos aspectos junto con el rubro de eficiencia permitiría escoger la mejor opción.

No importa lo novedosa, útil, poderosa, costosa y vanguardista que puede ser una herramienta. Al final del día, si no se cuenta con seres humanos que posean y hagan suyo todo el material producido por la ciencia política, operando a través de una institución que se comprometa con la optimización de sus resultados, la calidad de los instrumentos con los que se opera es una variable que simplemente no entra en juego para los resultados que se

emiten. Es primordial tener instituciones de calidad, diseñadas para llevar a cabo sus funciones con la meta de entregar resultados que aspiren a la perfección. Desafortunadamente la importancia del diseño institucional a menudo es ignorada o menospreciada por los actores políticos, tanto aquellos que disputan una contienda, así como aquellos que pretenden negociar un acuerdo, al grado de que han sido necesarias algunas regresiones institucionales y constitucionales para poder conseguir que la democracia sobreviva.[54]

Jason Kitcat lanzó al mercado el primer sistema de voto electrónico de código abierto, llamado GNU.FREE, y después de tres años de esfuerzo, dejó de producirlo. Kitcat argumenta que no importa que tan disponible sea el código, ni que tan ingenioso sea su diseño, no hay defensa en contra de la mala implementación o los cambios maliciosos dentro y fuera del sistema.[55]

VI. Conclusiones

Las nuevas tecnologías han mejorado la capacidad de generar información, misma que está siendo utilizada por el Estado para mejorar los servicios que está comprometido a ofrecer a la ciudadanía, logrando con ello incrementar la interacción entre las autoridades gubernamentales y la población, haciéndola más eficiente.

En el ámbito de la actividad política también se han generado cambios en la participación social impulsados por la facilidad de comunicación que otorgan los instrumentos modernos que han logrado, inclusive, que personas sin afiliación partidista se involucren en acciones de carácter electoral.

El uso de la informática se está haciendo más frecuente en las diferentes etapas de los procesos electorales, incluyendo la referente a la elección de candidatos a ocupar puestos de elección popular; de tal manera que la utilización del voto electrónico está alcanzando una aplicación mayor en las democracias modernas. La aceptación de esta nueva práctica está en función de diferentes variables, entre las que se encuentra el conocimiento que la sociedad tenga acerca de las ventajas que este medio alternativo de ejercer el voto tiene sobre el método tradicional.

[54] Reilly, Ben, "Democratic Levers for Conflict Management", en Harris, Peter y Reilly, Ben (comps.), *Democracy and Deep-Rooted Conflict: Options for Negotiators*, Suecia, Instituto Internacional para la Democracia y la Asistencia Electoral, 1998, pp. 140-142, *http://www.idea.int/ publications/democracy_and_deep_rooted_conflict/upload/ddrc_full_en.pdf.*

[55] Kitcat, Jason, *op. cit.*, pp. 65-67.

Otro aspecto que influye en la confiabilidad de la aplicación del voto electrónico es el tipo de código fuente que se utilice entre abierto o secreto. En el primer caso, la comunidad tiene la posibilidad de poner a prueba el sistema, lo que no ocurre cuando se utiliza un código fuente secreto, ya que en este caso solamente lo puede hacer personal muy restringido y debidamente autorizado. Existen ventajas y desventajas en el uso de cada uno de ellos, por lo que es recomendable acudir al apoyo de auditores tanto internos como externos que validen la seguridad de los sistemas.

Lo anterior implica que, la utilización de las tecnologías puede ser útil en el proceso de profundización de la democracia en el sentido que se abren como canales de participación ciudadana. Y en la medida en que se modernicen y se eficienten los procesos para ejercer el voto utilizando las tecnologías de comunicación información y que estos sean considerados como legítimos e incuestionables, habrá procesos electorales con mayor certidumbre para los competidores e instituciones electorales más confiables.

La adopción del voto electrónico ha incrementado el riesgo de que ocurran fallas en los sistemas electorales.[56] Algunos expertos en tecnología de la información han identificado una variedad de riesgos y vulnerabilidades inherentes a los sistemas de votación electrónica, que varían desde el mal diseño, ingeniería inferior a la hora de desarrollar el *software*, medidas protectoras mediocres, hasta pruebas de funcionamiento limitadas e insuficientes.[57] Sin embargo, los beneficios involucrados en el uso de tecnologías de la información para facilitar y acelerar los procesos electorales sobrepasan por mucho los riesgos que existen con el uso de boletas tradicionales. Si el sistema de gestión es lo suficientemente saludable para enfrentar estos riesgos y controlar los procesos adecuadamente para garantizar los resultados con transparencia y eficiencia, entonces las instituciones electorales estarán listas para enfrentar estos riesgos y entregarle a la ciudadanía mejores elecciones de las que le ha venido entregando.

VII. Bibliografía

Álvarez, R. Michael *et al.*, "Studying Elections: Data Quality and Pitfalls in Measuring the Effects of Voting Technologies", *VTP Working Paper*, núm. 21, 2004.

Álvarez, R. Michael y Hall, Thad E., *Electronic Elections: The Perils and Promises of Digital Democracy*, Princeton University Press, 2008.

56 Moynihan, Donald P., *op. cit*, pp. 515-528.

57 Grove, Jeff, *op. cit.*, pp. 69 y 70.

———, *Point, Click & Vote: The Future of Internet Voting*, Washington D. C., Brookings Institution Press, 2004.

Ansolabahere, Stephen *et al.*, "Residual Votes Attributable to Technology", *The Journal of Politics*, vol. 67, núm. 2, 2005.

Baltimore, David y Vest, Charles M., *Voting: What Is, What Could Be*, Caltech-MIT Voting Technology Project, 2001.

Bradner, Scott, "Lessons from the E-Voting Mess", *NetworkWorld,* 10 de mayo de 2004.

Carlson, Chris, "E-Voting Safeguards Urged", *eWEEK*, 5 de julio de 2004.

Donsanto, Craig, "Corruption of the Election Process under U.S. Federal Law", en Álvarez, R. Michael *et al.*, (comps.), *Election fraud. Detecting and deterring electoral manipulation,* Washington D. C., Brookings Institution Press, 2008.

Fischer, Eric A. y Coleman, Kevin J., "The Direct Recording Electronic Voting Machine (DRE) controversy: FAQs and misperceptions", *CRS Report for Congress,* 2005.

Fist, Stewart, "Mixed Reviews for E-Voting Systems", *Telecom Asia*, 1o. de marzo de 2004.

Grove, Jeff, "ACM Statement on Voting Systems", *Communications of the ACM*, vol. 47, núm. 10, 2004.

Hite, Randolph C., "Electronic Voting Offers Opportunities and Presents Challenges", *United States Government Accountability Office*, 2004.

Kearns, David, "Paper Trail Won't Cure E-Voting Ills", *NetworkWorld,* 6 de septiembre de 2004.

Kitcat, Jason, "Source Availability and E-Voting: an Advocate Recants", *Communications of the ACM*, vol. 47, núm. 19, 2004.

Kossick, Robert M., "The Role of Information & Communication Technology in Strengthening Citizen Participation & Shaping Democracy: an Analysis of Mexico's Initial Experience & Pending Challenges", *Information Technology in Developing Countries*, vol. 13, núm. 1, 2003.

Liburd, Soyini D., "An N-Version Electronic Voting System", *VTP Working Paper*, Massachusetts Institute of Technology, núm. 17, 2004.

McNamara, Paul, "Readers Vote Nay", *NetworkWorld*, 23 de agosto de 2004.

Mehta, Seema, "The Rise of the Internet Electorate", *Los Angeles Times*, 18 de abril de 2011.

Mercuri, Rebecca, "Inside Risks: Voting Automation (Early and Often?)", *Communications of the ACM*, vol. 43, núm. 11.

Miller, Harris, "E-Voting Does Work", *eWEEK*, 13 de septiembre de 2004.

Moynihan, Donald P., "Building Secure Elections: E-Voting, Security and Systems Theory", *Public Administration Review*, vol. 64, núm. 5, 2004.

NEGROPONTE, Nicholas, *Being Digital,* Nueva York, Alfred A. Knopf Inc., 1995.

NORRIS, Pipa, *E-Voting as the Magic Ballot? The Impact of the Internet on Electoral Participation and Civic Engagement*, Harvard University, John F. Kennedy School of Government, 2004.

PAPP, Daniel S. *et al.*, "Historical Impacts of Information Technologies: An Overview", en ALBERTS, David S. y PAPP, Daniel S. (comps.), *The Information Age: An Anthology on its Impact and Consequence*, CCRP Publication Series, 1997.

REILLY, Ben, "Democratic Levers for Conflict Management", en HARRIS, Peter y REILLY, Ben (comps.), *Democracy and Deep-Rooted Conflict: Options for Negotiators*, Suecia, Instituto Internacional para la Democracia y la Asistencia Electoral, 1998.

RHEINGOLD, Howard, "Tools for Thought: The History and Future of Mind-expanding Technology", The MIT Press, 2000.

ROTHKE, Ben, "E-Voting: It's Security, Stupid", *eWEEK*, 23 de agosto de 2004.

SELKER, Ted, "Processes Can Improve Electronic Voting: a Case Study of an Election", *VTP Working Paper,* núm. 19, 2004.

SHAMOS, Michael, I., "Paper Versus Electronic Records – An Assessment", *Proceedings of the 14th ACM Conference on Computers, Freedom and Privacy,* Berkeley, 2004.

STEWART, Thomas A., "Welcome to the Revolution", en ALBERTS, David S. y PAPP, Daniel S. (comps.), *The Information Age: An Anthology on its Impact and Consequence*, CCRP Publication Series, 1997.