ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

19/2017 24 de febrero 2017

*Mayumi Yasunaga Kumano**

Las nuevas tecnologías de votación: ¿una puerta abierta a la injerencia externa?

Las nuevas tecnologías de votación: ¿una puerta abierta a la injerencia externa?

Resumen:

Con la introducción de las Tecnologías de la Información y la Comunicación en el tejido estatal se pretende potenciar toda una gama de servicios públicos ofrecidos por el Estado y facilitar la gestión de los asuntos públicos. La aplicación de estas tecnologías a los procesos electorales puede tener como consecuencia la potenciación de la democracia; no obstante, también la aplicación de estas tecnologías abre la puerta a la posibilidad de llevar a cabo ataques contra los procesos democráticos con el fin último de minar la confianza de los ciudadanos en sus representantes y en su Estado y con ello desestabilizar los sistemas democráticos.

Abstract:

The goal of the introduction of the Information and Communication Technologies in the state's fabric is to strengthen a whole set of public services provided by the State and to facilitate the management of the public affairs. The application of these technologies to electoral processes can have as a consequence the promotion of democracy; however, the use of these technologies can open the door to attacks against those democratic processes with the ultimate goal of undermining the citizen's confidence in their representatives and their State and, thus, to destabilize the democratic systems.

Palabras clave: Nuevas tecnologías de votación, voto electrónico, ciberataques, OSCE, Consejo de Europa.

Keywords: New voting technologies, electronic voting, cyberattacks, OSCE, Council of Europe.

Introducción

Una de las bases sobre las que se asienta la democracia occidental es la existencia de procesos electorales que tienen una serie de características:

- Son libres.

- Son regulares.

- Son justos y transparentes.

Gracias a estos rasgos, los ciudadanos están capacitados para elegir entre los diversos candidatos que les presentan unas estructuras políticas (partidos). Todos estos rasgos están bien asentados en la amplia mayoría de Estados occidentales.

Con el fin de hacer estos procesos electorales lo más abiertos, eficientes, transparentes y accesibles a la población y gracias a una serie de tecnologías, los Estados están implantando sistemas de voto electrónico y se plantean poner en funcionamiento sistemas de voto en línea.

No obstante, en los últimos meses se ha venido planteando una serie de hipótesis y acusaciones que, de confirmarse, supondrían una amenaza letal para una democracia: la posibilidad de que un Estado influya, manipule o siembre dudas sobre la legitimidad de un resultado electoral en un Estado democrático, atacando las bases sobre las que se asienta toda democracia.

En este artículo voy a analizar la progresiva utilización de las TIC (Tecnologías de la Información y la Comunicación) en las estructuras estatales con unos fines muy claros: mejorar la eficacia y la eficiencia del Estado a la hora de prestar sus servicios, entre otros.

A continuación tomaremos el ámbito electoral como marco central del artículo para ver la progresiva implantación del voto electrónico y sus ventajas e inconvenientes como método de voto y contabilización, su transparencia y la seguridad en los comicios.

Respecto a este último elemento, el de la seguridad, veremos las dudas que han generado la implantación y la posibilidad de que se produzca una intromisión en los procesos mediante *hackeo* que afecte a las infraestructuras, los partidos políticos o a la propia maquinaria y sistemas que gestionan los mecanismos de voto electrónico.

Una vez vistas las posibles brechas de seguridad que ofrece el voto electrónico a distintos actores, me centraré en el caso más reciente y quizás más relevante en lo que se refiere a una posible manipulación electoral: las elecciones presidenciales de 2016 que han llevado a la Casa Blanca a Donald J. Trump. El artículo finalizará con los temores de una serie de Estados, especialmente la República Federal de Alemania, de que otro Estado pretenda influir en el resultado de las elecciones que tendrán lugar en 2017.

La penetración de las TIC en el tejido estatal

Las TIC (Tecnologías de la Información y la Comunicación) están moldeando el futuro de las sociedades modernas. La acción de estas tecnologías no solo está afectando a la propia economía destruyendo puestos de trabajo, alterando los trabajos que siguen siendo desarrollados por mano de obra humana o creando nuevos trabajos que hasta hace poco no existían.

Está afectando, además, a la forma en que nos relacionamos con el resto de la sociedad y también a la forma en que nos relacionamos con nuestros gobiernos. En este sentido, la creación del *e-government* (e-gobierno) supone la introducción de sistemas para gestionar impuestos, licencias, demandas o prescripciones médicas desde nuestros hogares.

Al igual que los ciudadanos y las empresas, los gobiernos han comenzado su particular transición a la esfera digital trasladando parte de sus servicios al mundo virtual e interactuando en la red con los distintos actores sociales.

Durante la década de los 90 se popularizó en EE. UU. el término *e-government*, con el cual se pretendía dar una importancia cada vez mayor a los proyectos tecnológicos que tenían un impacto sobre el modo en que el ciudadano recibía los servicios del Estado.

Mediante las iniciativas conocidas como e-gobierno el Estado pretende ampliar el alcance de los servicios prestados, conseguir una mayor eficiencia en la gestión, acercarse a los ciudadanos e incluirlos en los procesos estatales, aumentar los niveles de transparencia en la administración de los asuntos públicos, etc.

De entre todos los procesos estatales los procesos electorales son los más importantes. No en vano, en ellos los ciudadanos eligen a aquellos que les van a

representar durante un cierto tiempo y en los que se confía los distintos aparatos burocráticos con el fin de aplicar unas políticas determinadas.

Con cada vez mayor frecuencia, en estos procesos electorales intervienen las TIC, que pueden jugar un papel importante durante todo el ciclo electoral. Como veremos más adelante, la introducción del voto electrónico y del voto en línea tienen una serie de atractivos y de inconvenientes. Como se ha visto en las elecciones en EE. UU., los procesos electorales son un objetivo principal de los distintos actores que operan en el ciberespacio. Mediante una serie de acciones un actor puede alterar de manera importante el resultado de unas elecciones, bien sea mediante una acción directa, bien sea a través de la deslegitimación o, simplemente, sembrando dudas sobre la legalidad de los procesos y por ello del resultado electoral. Con ello se puede minar la confianza de los ciudadanos en sus representantes y así dañar la base principal de toda democracia.

¿En qué consiste el voto electrónico?

El voto electrónico forma parte de lo que hoy en día se conoce como nuevas tecnologías de votación (*New Voting Technologies*). Además del voto electrónico, dentro de este grupo se encuentran el escaneo de papeletas o el voto por Internet. Según la OSCE, las nuevas tecnologías de votación se pueden definir como el uso o aplicación de las Tecnologías de la Información y la Comunicación para la emisión del voto, su recuento y posterior tabulación[1].

El Instituto IDEA, por su parte, define el voto electrónico como aquellos «sistemas en que el registro, la emisión o el conteo de los votos en elecciones para cargos políticos y referendos involucra el uso de tecnologías de la información y las comunicaciones (TIC)»[2].

Dentro de la categoría de voto electrónico el Instituto IDEA hace una clasificación en 4 grandes grupos según las técnicas y métodos utilizados por estos sistemas:

- Registro Electrónico Directo (RED).

[1] OSCE. The use of New Voting Technologies: Comparative experiences in the implementation of electronic voting. 2013. Disponible en: https://www.oas.org/es/sap/deco/seminarios/peru/pre/Robert_Krimmer.pdf

[2] Institute IDEA. Una introducción al voto electrónico: Consideraciones esenciales. Estocolmo. 2011.

- Reconocimiento óptico de marcas.

- Impresoras de papeletas electrónicas.

- Sistemas de votación en línea (votación por Internet).

Estos sistemas de votación han tenido una aceptación considerable a lo largo y ancho del mundo. Más de una decena de países han optado por este método de votación, ya sea en elecciones municipales, regionales o estatales. Canadá, Estonia, Brasil, Bélgica, Estados Unidos, Reino Unido, India y hasta 2007 los Países Bajos han utilizado alguna de las nuevas tecnologías de votación para gestionar sus procesos electorales. Otros países ya han realizado pruebas piloto para la introducción del voto electrónico o han permitido votar a parte de su población en el extranjero (como los soldados desplegados en misiones en el exterior) a través de estos sistemas.

Llevar a cabo la implementación de las nuevas tecnologías de votación no es una tarea fácil. La difícil decisión que tienen que tomar los responsables públicos a la hora de decidir la introducción del voto electrónico viene marcada por una serie de ventajas e inconvenientes que se analizará en el epígrafe siguiente. Sin ninguna duda, el voto electrónico puede suponer un avance nada desdeñable para el desarrollo de los procesos democráticos, no obstante, los inconvenientes que puede provocar una mala implementación, un mal funcionamiento o incluso la disrupción completa del proceso electoral suponen un peso considerable a la hora de decidir no adoptar ningún nuevo método y seguir apostando por los votos en papel.

Ventajas e inconvenientes de la adopción de un sistema de voto electrónico

Las técnicas anteriormente mencionadas vienen acompañadas por un conjunto de factores que se deben tener en cuenta, conocer y calibrar de forma concienzuda antes de decidir su implementación en cualquier escala de la estructura estatal.

Como veremos, la adopción de los distintos sistemas de voto electrónico supone por una parte la posibilidad de mejorar la gestión y el desarrollo de todo el proceso electoral, pero también supone asumir una serie de inconvenientes muchos de los cuales pueden suponer un grave problema en aspectos esenciales de la democracia como puedan ser el secreto del voto, el seguimiento de los resultados o la contabilización de los mismos entre otros.

Entre las ventajas que, según el Instituto IDEA, ofrece el voto electrónico encontramos[3]:

- La rapidez del sistema a la hora de contar los votos emitidos y, gracias a ello, la obtención más acelerada de los resultados de los comicios.

- La eliminación del error humano a la hora del conteo de los votos, debido a la mayor precisión de las máquinas.

- Una mayor comodidad para los ciudadanos que podría conllevar una mayor participación en las elecciones, dando mayor legitimidad a los procesos electorales.

- Evita las conductas fraudulentas en las mesas electorales y en el conteo de los votos.

- Da una mayor accesibilidad a las personas con alguna discapacidad, con problemas de movilidad o con dificultades para ejercer su derecho al voto.

- Ahorros en la gestión de los procesos electorales al eliminar papeletas, reducir el número de personas necesarias en las mesas o resolver problemas logísticos asociados al voto por correo.

Se puede apreciar en esta lista cómo las nuevas tecnologías de votación pueden suponer una mejora en la eficiencia del Estado a la hora de gestionar los procesos electorales, reduciendo los costes, acelerando los resultados, mejorando el acceso de los ciudadanos y facilitando su participación generalizada.

Si las ventajas pueden resultar atractivas, los inconvenientes pueden suponer problemas y dudas de difícil solución.

Los argumentos contrarios a la aplicación de las nuevas tecnologías de votación están asociados a la necesidad de formación de la población, la inversión inicial, las necesidades de suministro y los riesgos asociados a la transparencia, anonimidad, riesgo en la seguridad de los sistemas y falta de confianza de los ciudadanos.

El Instituto IDEA menciona, entre otros, los siguientes argumentos en contra de las nuevas tecnologías de votación:

- Falta de transparencia.

- Falta de homogeneidad y de garantía en la certificación de los sistemas.

[3] Ibídem

- Posibilidad de destrucción del secreto del voto.

- Posible manipulación por ataques informáticos.

- Necesidad de un suministro constante de energía.

- Necesidad de realizar campañas de educación de la población.

- Falta de confianza en los resultados.

Aunque todas estas facetas negativas son compartidas por las nuevas tecnologías de votación, varias de ellas se potencian cuando se quiere ir más allá y permitir la votación en las elecciones a través de Internet, la votación en línea.

Estonia y la sociedad digital

Algunos países ya han avanzado la posibilidad de acercar aún más el proceso electoral a los ciudadanos, dándoles la posibilidad de que estos voten desde sus hogares a través de sus ordenadores e incluso de sus móviles.

Estonia ha hecho de Internet un punto clave de su economía, de su gobernanza y de la gestión de los servicios públicos. El plan e-Estonia ha integrado Internet y las Tecnologías de la Información y de la Comunicación dentro de la estructura del Estado potenciando una serie de servicios y facilitando el acceso de los ciudadanos a un conjunto de sistemas basados en las TIC.

Para el caso que nos concierne, dentro de estos sistemas, el e-*voting* permite a los ciudadanos emitir su voto desde cualquier punto con el único requisito de tener una conexión a Internet. Estonia fue pionero a la hora de implementar el voto en línea. Desde el año 2005, Estonia permitió como uno de los métodos de votación en sus elecciones el voto en línea. Desde ese año, la utilización de este sistema no ha dejado de crecer en los siguientes procesos electorales que han tenido lugar en el país báltico.

No obstante, a pesar de la versatilidad, facilidad y comodidad que supondría el no desplazarse hasta los colegios electorales, varias voces se han alzado contra esta posibilidad por considerarla incluso más peligrosa que los sistemas de voto electrónico antes analizados[4].

[4] World Economic Forum. Why electronic voting would be a complete disaster. 2016. Disponible en:

David Dill profesor de informática en la Universidad de Stanford, es contrario a la introducción del voto en línea en los procesos electorales por la falta de seguridad en el ciclo de la emisión y la supervisión del voto. A su juicio «el abrumador consenso de los expertos técnicos es que el *e-voting* es peligroso y que los votantes deben ser capaces de verificar que sus votos fueron adecuadamente registrados»[5] añadiendo que «el *e-voting* sin papeletas es más peligroso que los sistemas con urnas ya que abre la puerta a errores a gran escala. Un simple virus, o software malicioso instalado por un único individuo, podría distribuirse a miles de máquinas por todo el país, lo que podría cambiar un gran número de votos de forma indetectable».

La seguridad de las TIC se convierte de esta manera en una preocupación constante para los responsables públicos.

Abundando en los posibles fallos, Jason Kitcat señaló que «cuando mis compañeros y yo llevamos a cabo pruebas de monitoreo siempre hemos observado serios defectos en la seguridad y la fiabilidad de los sistemas que se han usado» afirmando que «hemos encontrado problemas cada vez, y los hemos documentado de forma extensa en artículos revisados por expertos»[6].

Las dudas sobre la fiabilidad de los sistemas no son un simple inconveniente más de una lista sino que golpean de lleno uno de los pilares de los procesos electorales y de los sistemas democráticos. A fin de facilitar la introducción de las nuevas tecnologías de votación, el Consejo de Europa publicó una serie de líneas directrices para garantizar la transparencia en las elecciones[7].

El Consejo de Europa agrupó las directrices en una serie de bloques. El bloque de recomendaciones generales se basa, en primer lugar, en haber conseguido un estado previo de confianza generalizada en el sistema electoral; en segundo lugar, asegurar por todos los medios la transparencia en los procesos electorales y, finalmente, haber

---

https://www.weforum.org/agenda/2016/06/why-online-voting-would-be-a-complete-disaster

[5] DILL, David. Electronic Voting: An overview of the problem. Stanford University. Disponible en: usacm.acm.org/images/documents/dill.pdf

[6] The Guardian. Why electronic voting is not secure. 2015. Disponible en: https://www.theguardian.com/technology/2015/mar/30/why-electronic-voting-is-not-secure

[7] Consejo de Europa. Dirección general de democracia y asuntos políticos. Guidelines on transparency of e-enabled elections. Estrasburgo. 2011 Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059bdf6

llevado a cabo una campaña de información sobre las ventajas que se derivan de la adopción del sistema.

En el bloque de directrices legales, el Consejo de Europa recomienda analizar previamente los cambios legales que se deben realizar para poder adoptar las nuevas tecnologías de votación, cambiando, de ser necesario, las reglas penales, civiles, constitucionales o de observación electoral.

También pide el Consejo de Europa la máxima transparencia a la hora de dar acceso a todos los documentos e informes relativos a los procesos electorales. Especialmente sensibles son los documentos relativos a los certificados y a los procesos de auditoría del sistema adoptados. Se requiere además la puesta en funcionamiento de un programa de capacitación y entrenamiento para los observadores electorales nacionales e internacionales.

El bloque relativo a los sistemas hace referencia a una serie de factores que deben tenerse en cuenta como son:

- Evitar la sobre dependencia de uno o dos proveedores de la tecnología.

- Permitir la auditoría del código fuente de votación.

- Disponer de un segundo medio de almacenamiento del voto registrado para tener en todo momento una copia de seguridad.

- Si se dispone de esta copia de seguridad, llevar a cabo recuentos al azar para certificar que ambas bases de datos concuerdan.

- Tener a disposición de las autoridades reglas claras sobre las acciones a ejercitar en caso de que las bases de almacenamiento de votos primaria y secundaria no concuerden.

- Tener mecanismos para permitir a los votantes saber si su voto ha sido contabilizado.

Como se puede observar, las líneas directrices del Consejo de Europa hacen de la transparencia y la integridad dos requisitos indispensables para el buen funcionamiento de unas elecciones realizadas a través de las nuevas tecnologías de votación.

No en vano, y como veremos más adelante, la integridad de las elecciones, entendida como la gestión adecuada de todo el proceso electoral basado en los principios de transparencia, profesionalidad, competencia e imparcialidad, es la base de la confianza

ciudadana en el sistema y es la fuente de legitimidad de las autoridades emanadas de las urnas.

La ausencia de esa integridad, transparencia y legitimidad es una receta perfecta para las convulsiones políticas, algo que ningún sistema puede permitirse y menos una democracia.

A pesar de que en muchos ámbitos de la vida cotidiana la tecnología está siendo adoptada sin muchas complicaciones por los ciudadanos, los acontecimientos que han tenido lugar en los últimos meses, especialmente debido a las elecciones presidenciales en EE. UU., han comenzado a alertar a los expertos y a los responsables políticos sobre los riesgos que para una democracia pueda tener el hecho de sufrir un pirateo informático que tenga como consecuencia que un Estado pueda cambiar el destino político de otro Estado con el fin de aupar a un candidato u otro en un determinado proceso electoral.

En el próximo epígrafe analizaremos el informe publicado por las agencias de inteligencia de EE. UU. y presentado al presidente Donald J. Trump respecto a la injerencia rusa en las elecciones de 2016.

La injerencia en las elecciones de EE. UU. en 2016 y en futuros procesos electorales

Si algo ha marcado el ritmo de las elecciones de 2016 en Estados Unidos ha sido la sospecha de interferencias extranjeras durante todo el proceso. Meses antes de las elecciones se inició un debate sobre la seguridad del voto electrónico y su posible incidencia sobre los resultados de las elecciones. Se ha señalado que «los expertos indican que los sistemas electorales disponibles hoy en día no proporcionan la protección adecuada que se necesitaría para evitar que un hacker extranjero —de hecho, un hacker en cualquier parte— pudiera manipular nuestras elecciones. Lo que es peor, los ataques podrían pasar desapercibidos»[8].

Uno de los factores más importantes de la campaña fue la infiltración y robo de documentos de la Convención Nacional Demócrata y la posterior publicación de la

[8] CHIN Jimmy. Foreigners could hack US elections, experts say. 2015. Disponible en: http://whowhatwhy.org/2015/08/31/foreigners-could-hack-us-elections-experts-say/

información a través de *WikiLeaks* en julio del año pasado. Aunque durante los meses previos al 8 de noviembre se demostró cómo las máquinas utilizadas para ejercitar el voto de manera electrónica eran vulnerables o no daban las suficientes garantías de seguridad, ya en 2011 se habían realizado informes sobre las graves vulnerabilidades en las máquinas de votación[9].

En septiembre, el Departamento de Seguridad Interior (*Department of Homeland Security*) alertó de que más de 20 Estados habían sufrido algún tipo de intento de infiltración. El mismo Departamento ofreció a todos los Estados un análisis de seguridad adicional al nacional[10].

El pasado 6 de enero de 2017 el Director de Inteligencia Nacional hizo público una parte del informe titulado *Valorando las actividades e intenciones rusas en las recientes elecciones en Estados Unidos*: *El proceso analítico y atribución del ciber incidente*[11]. En el informe, que no se publicó en su totalidad por razones de seguridad, 3 agencias estadounidenses, la CIA, la NSA y el FBI valoraron la campaña mediática y las herramientas informáticas que Rusia empleó «con el objetivo de minar la fe pública en el proceso democrático en los Estados Unidos, denigrar a la secretaria Clinton y dañar su elegibilidad y su potencial presidencia». Añadiendo que «Putin y el Gobierno ruso desarrollaron una clara preferencia por el presidente Trump».

Según el informe, se sabe que varios actores vinculados al Gobierno ruso estuvieron probando listas de electores y de información sobre los votantes de ciertos Estados y que se intentaron infiltrar en sistemas y máquinas de votación. De hecho, se apunta que, desde principios de 2014, «la inteligencia rusa ha investigado los procesos electorales de Estados Unidos, su tecnología y su equipamiento». No obstante, a pesar de que «la inteligencia rusa obtuvo y mantuvo acceso a múltiples juntas electorales a nivel local y estatal, el Departamento de Seguridad Interior considera que los tipos de sistemas que los actores rusos tenían como objetivo o comprometieron, no estaban dedicados al recuento de votos». Ello implicaría que, a pesar de los intentos, la

[9] FRIEDMAN Brad. Diebold machines can be hacked by remote control. 2011. Disponible en: https://www.salon.com/2011/09/27/votinghack/

[10] GELLER Eric, SAMUELSOHN Darren. More than 20 states have faced major election hacking attempts, DHS says. 2016. Disponible en: http://www.politico.com/story/2016/09/states-major-election-hacking-228978

[11] Office of the Director of National Intelligence. Assessing Russian activities and intentions in recent US elections. 2016. Disponible en: https://www.dni.gov/files/documents/ICA_2017_01.pdf

campaña rusa no pudo manipular el voto de forma directa, aunque sí que pudo lastrar la campaña de la candidata demócrata.

Por otra parte, si el objetivo ruso era sembrar dudas sobre los procesos democráticos en EE. UU., no hay duda de que hasta cierto punto lo han conseguido y que las maniobras rusas parecen haber dañado la imagen de los dos candidatos: desde las protestas contra Hillary Clinton por parte de los seguidores de Bernie Sanders tras las revelaciones de *WikiLeaks* y el consiguiente daño en su imagen que hubiera tenido Clinton de haber ganado, hasta las protestas contra Trump después de las elecciones. Según una encuesta del *Washington Post*, un 18 % de los ciudadanos no consideraba como presidente legítimo a Donald Trump, cifra que se elevaba hasta el 33 % entre los votantes de Clinton[12].

Como ya se señaló antes, la integridad en los procesos electorales da a los que pierden los comicios la seguridad de que han sido derrotados de manera legal y justa. Aunque las actividades rusas no tuvieran un impacto directo en el resultado de las elecciones, la mera posibilidad de sembrar la duda sobre la legitimidad de los resultados electorales puede convertirse en un elemento tremendamente nocivo para una democracia.

Desafortunadamente, en el informe del Director Nacional de Inteligencia se advierte que «Moscú va a aplicar las lecciones aprendidas en la campaña ordenada por Putin y dirigida contra las elecciones presidenciales de Estados Unidos para realizar campañas de manipulación en el futuro, incluso contra aliados de Estados Unidos y sus procesos electorales»[13].

2017 va a ser un año cargado de elecciones importantes, especialmente en Europa, y los acontecimientos de Estados Unidos no han hecho sino encender todas las alarmas ante un posible intento de manipular o influir en las elecciones que tendrán lugar en países como Holanda, Francia[14] o Alemania.

---

[12] CLEMENT Scott. The Washington Post. One-third of Clinton supporters say Trump election is not legitimate, poll finds. 2016. Disponible en: https://www.washingtonpost.com/news/the-fix/wp/2016/11/13/one-third-of-clinton-supporters-say-trump-election-is-not-legitimate-poll-finds/

[13] Office of the Director of National Intelligence. Assessing Russian activities and intentions in recent US elections. 2016. Disponible en: https://www.dni.gov/files/documents/ICA_2017_01.pdf

[14] GONZÁLEZ Enric. Francia afirma que "no está a salvo" de ciberataques rusos contra sus elecciones. 2016. Disponible en: http://www.elmundo.es/internacional/2017/01/09/58729cd046163fc8028b461a.html

En estos dos últimos países ya se ha dado la voz de alarma por las posibles interferencias con los procesos electorales que tendrán lugar en abril de este año y en otoño respectivamente. El presidente del *Bundesnachrichtendienst* (Servicio de Información Federal) señaló que «tenemos pruebas de que están teniendo lugar ciberataques que no tienen otro propósito que el de crear incertidumbre política», añadiendo que «los atacantes están interesados en deslegitimar el proceso democrático como tal, independientemente de a quién acabe beneficiando. Tenemos indicios que los ataques proceden de la región rusa»[15].

Conclusiones

Las Tecnologías de la Información y la Comunicación van a ser un pilar fundamental para la gobernanza de un Estado moderno. La introducción de estas tecnologías en todos los ámbitos de la gestión del Estado (sea en materia de transporte, medio ambiental, fiscal, servicios médicos, educación, etc...) va a multiplicar la capacidad de las autoridades para administrar los servicios públicos.

No obstante, la introducción de estas tecnologías en campos como el voto y los procesos electorales tienen que ser cuidadosamente planificadas y ejecutadas, especialmente el aspecto de la seguridad, puesto que los fallos en este ámbito tienen un carácter extremadamente nocivo para cualquier democracia.

La seguridad de las nuevas tecnologías de votación y de los procesos electorales es un asunto de seguridad nacional para todos aquellos Estados que disponen o que están pensando implementar dichas tecnologías en sus elecciones.

La injerencia de un Estado en los procesos democráticos de otro Estado no es nueva, lo que es nuevo es el abanico de posibilidades que la tecnología ofrece a los atacantes para intentar socavar los fundamentos democráticos de sus enemigos (desde la manipulación de las máquinas, robo de información de partidos políticos pasando por los chantajes a políticos por información robada hasta tumbar páginas de partidos políticos). Todos estos riesgos se han amplificado con el ciberespacio y la interconectividad de la sociedad.

[15] CONNOLLY Kate. German spy chief says Russian hackers could disrupt elections. 2016. Disponible en: https://www.theguardian.com/world/2016/nov/29/german-spy-chief-russian-hackers-could-disrupt-elections-bruno-kahl-cyber-attacks

Como hemos visto, las nuevas tecnologías de votación ofrecen ventajas a la hora de gestionar los procesos electorales, sin embargo, siempre y cuando no se pueda garantizar la máxima seguridad, las papeletas deben ser la prioridad. Preguntado sobre si el papel era el patrón oro, David Dill respondió «Sí. El papel tiene unas propiedades fundamentales como tecnología que lo convierten en la tecnología a usar para votar. Tienen unas marcas más o menos indelebles sobre él. Tienes objetos físicos que puedes controlar. Y todo el mundo lo entiende»[16].

i

*Mayumi Yasunaga Kumano**
Abogada

[16] World Economic Forum. Why electronic voting would be a complete disaster. 2016. Disponible en: https://www.weforum.org/agenda/2016/06/why-online-voting-would-be-a-complete-disaster