DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

Gestión electoral

Universidad Nacional Autónoma de México, IIJ-BJV, 2020
https://revistas.juridicas.unam.mx/index.php/derecho-electoral/issue/archive

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

Procesos electorales y TIC en el ámbito español: ciberseguridad y participación política*

Electoral Processes and ITC's in the Spanish Field: Cybersecurity and Political Participation

Tamara **Álvarez Robles****

Sumario:

* Este trabajo se ha desarrollado en el seno de la Cátedra Almirante Bonifaz de la Universidad de León y del Grupo de Investigación de Derecho Constitucional de la Universidad de León.

** Doctora en derecho constitucional. Profesora contratada, Universidad de Vigo. *talvr@unileon.es//tamara.alvarez.robles@uvigo.es*.

Recibido: 3 de agosto de 2018
Aceptado: 7 de marzo de 2019

Revista Mexicana de Derecho Electoral, núm. 15-16, enero-diciembre de 2019, pp. 159-185, Ciudad de México

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

Resumen:

El trabajo pretende analizar las cuestiones prácticas y teóricas más relevantes ante la posibilidad de llevar a cabo un referéndum constitucional y/o unas elecciones generales mediante el uso de las tecnologías de la información y de la comunicación.

De este modo, en un primer momento, se abordará el concepto de democracia digital, para, seguidamente, atender las cuestiones prácticas que derivan del mismo, a saber: *hackeo*, *doxxing*, *fake news*, etcétera. En tercer lugar, la aproximación al marco normativo de referencia pretenderá la clarificación de la parte teórica a fin de determinar las disfunciones que se podrían producir bajo la influencia de las tecnologías de la información y de la comunicación en los procedimientos participativos señalados.

Abstract:

The paper presented aims to analyze the most relevant practical and theoretical issues faced with the possibility of carrying out a constitutional referendum and / or general elections through the use of information and communication technologies.

Thus, initially, the concept of digital democracy will be addressed, and then the practical issues that derive from it will be examined, in particular: hacking, doxxing, fake news, etc.

Thirdly, the approach to the normative frame of reference will seek to clarify the theoretical considerations in order to determine the dysfunctions that could occur under the influence of information and communication technologies in the aforementioned participatory procedures.

Palabras clave: ciberseguridad, democracia digital, delitos electorales, *hackeo*, *doxxing*, referéndum, sufragio.

Keywords: cybersecurity, digital democracy, electoral crimes, hacking, doxxing, referendum, suffrage.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

I. Aproximación a la democracia digital

Para introducir el tema me gustaría comenzar con la siguiente reflexión:

La democracia en el siglo XXI hemos de plantearla en una época de reflexividad,[1] como causa-efecto de la globalización,[2] produciéndose en un estado de crisis,[3] "crisis democrática". En otras palabras, nos encontramos en el camino a la postmodernidad,[4] ello supone el cuestionamiento no sólo del Estado, en el sentido más amplio del concepto, sino también de las instituciones democráticas que lo conforman, siendo uno de los factores a considerar en esta etapa de revisión, reflexión e incluso transformación, el factor tecnológico y el desarrollo en el nuevo entorno cibernético.

El reflejo de la crisis democrática, su transformación, asemejaría aquella participación directa ciudadana, pareciendo que la democracia indirecta se sitúa en las horas más críticas, cuestionada por la ciudadanía, acusada por las corruptelas políticas, asediada por la globalización[5] y la hiperconexión. La necesidad del pueblo de sentirse actor principal de su comunidad,[6] de su región, de su país, hace que nos preguntemos si el modelo de democracia representativa, indirecta, a participativa, directa,

---

[1] Beck, Ulrich *et al.*, *Modernización reflexiva: política, tradición y estética en el orden social moderno*, Madrid, Alianza Editorial, 1997, pp. 13-73; Beck, Ulrich, *The Cosmopolitan Manifesto,* New Stateman, 20 de marzo de 1998, pp. 28-30, Beck, Ulrich, *Un nuevo mundo feliz: la precariedad del trabajo en la era de la globalización,* Barcelona, Paidós, 2000, pp. 26-32.

[2] Seijas, Ma. Esther, "Hacia un Estado democrático global: crisis y Constituciones", *Themis*, *Revista de Derecho* 67, 2015.

[3] Las "crisis" a las que atendemos suponen un cuestionamiento de axiomas de la modernidad, pudiendo ser de representación política, participación, normativas, etcétera. Buscan la confirmación, negación o reformulación de las instituciones de la modernidad, en una época de transición hacia la postmodernidad. Si bien planteamos la necesidad de repensar las mismas en dos escenarios, que interactúan y se afectan: el tradicional, analógico/offline, y el nuevo, digital/online/cibernético.

[4] Giddens, Anthony, *Un mundo desbocado. Los efectos de la globalización en nuestras vidas,* Madrid, Taurus, 2000, pp. 87-95, Giddens, Anthony, *Consecuencias de la modernidad,* Madrid, Alianza Editorial, 2002, pp. 25 y 26

[5] Beck, Ulrich, *¿Qué es la globalización? Falacias del globalismo, respuestas a la globalización*, Barcelona, Paidós, 1998; Held, David *et al.*, *Global Transformation: Politics, Economics and Culture,* Stanford, Stanford University Press, 1999; Giddens, Anthony, *Un mundo desbocado..., cit.,* Madrid, Taurus, 2000.

[6] Comunidad que no se circunscribe, en esta etapa, bajo el principio de territorialidad sino que se transnacionaliza e incluso se digitaliza, y que se conforma y disuelve en el marco de los intereses que persigue.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

se está produciendo paulatinamente en la actualidad apoyada no sólo por la inquietud ciudadana, sino también por otro factor que se introduce en este diálogo: las tecnologías de la información y la comunicación, TIC.[7]

Si fijamos nuestra atención en el diálogo democracia-participación,[8] podemos observar cómo el constitucionalismo de las últimas décadas comienza a interesarse por el análisis profundo de este nuevo espacio y de las consecuencias o afecciones de las tecnologías de la comunicación y la información, al propio sistema constitucional.[9]

En este orden de ideas, en la necesidad de repensar[10] el concepto de democracia, hay quienes defienden[11] el uso de las TIC para mejorar nuestra calidad democrática,[12] y no sólo por ser éstas más rápidas en el acceso a la participación y en el escrutinio de los resultados, menos costoso, porque puede suponer la accesibilidad a las personas con discapacidad.

Las tecnologías de la información y comunicación, especialmente Internet, se están empleando para establecer, mejorar o ampliar los canales de participación política, de comunicación y de información a los ciudadanos, por lo tanto afectando a la calidad democrática.[13] En esta época, caracterizada, entre otras, por la crisis democrática y de representación,

> en el contexto actual de disminución de la participación en muchas democracias occidentales y decepción generalizada hacia la política, los responsables de las políticas han estado buscando estrategias innovadoras para volver a involucrar a

---

[7] Castells, Manuel, en Himanen, Pekka, *The Hacker Ethic and the Spirit of the Information Age,* Nueva York, Random House, 2001, pp. 155-178.

[8] Criado de Diego, Marcos, *Participar. La ciudadanía activa en las relaciones Estado sociedad,* Madrid, Dykinson, 2014.

[9] Previamente se han realizado análisis parciales, de cuestiones puntuales desde una miopía constitucional y no desde la dualidad constitucional-tecnológica. Sin embargo, en los últimos años viene siendo habitual la presencia de especialistas, no juristas ni constitucionalistas, en las investigaciones que al respecto se desarrollan aportando esa transversalidad y diálogo requeridos.

[10] Este es el caso de autores como Beck, Held, Giddens o Steger.

[11] En este sentido se pronuncia Trechsel, Alexander H., "Potential and Challenges of e-voting in the European Union". El citado estudio analiza la implantación del "e-voting"o "Internet voting" en las futuras elecciones al Parlamento Europeo; de este modo postula la factibilidad de su pronta instalación, disponible en: *http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf*.

[12] Tudela, José *et al.* (coords.), *Calidad democrática y organización territorial*, Madrid, Marcial Pons, 2018.

[13] Tejadura, Javier (ed.), *Diez propuestas para mejorar la calidad de la democracia en España,* Madrid, Biblioteca Nueva, 2014.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

> los ciudadanos y promover un proceso democrático participativo. El voto por Internet es una innovación particularmente atractiva en este sentido, en el sentido de que combina la tecnología con el núcleo de la participación democrática...[14]
>
> ...es un instrumento que podría ayudar en la extensión y mejora de los canales de comunicación y participación de éstos y, en este sentido, podría contribuir, de alguna manera, a paliar la crisis de legitimidad que padecen nuestros actores e instituciones políticas.[15]

Pareciera que frente a la crisis democrática se ha dado con la solución, las TIC, esto es, la democracia digital,[16] pues facilitarían no sólo el acceso a la información, sino también la participación en asuntos públicos,[17] que se exponen en la red, en el ciberespacio, en aplicaciones (*software*), para que éstos muestren su parecer, pudiéndose aumentar esa calidad democrática que se requiere y/o se exige. Así, podrían someterse a la ciudadanía desde una consulta sobre alguna política pública a llevar a cabo, unos presupuestos participativos[18] hasta un referéndum o unas elecciones. Las TIC permitirían ir pasando por los escalones de la escalera de Arnstein:[19] información, consulta, asociación, etcétera, adaptada al nuevo contexto político y tecnológico, permitiendo de ese modo el acercamiento de la política, de la toma de decisiones, a la ciudadanía.

Pero si ello es tan sencillo, si la democracia digital es la solución a la crisis democrática existente, ¿cuál es la razón por la que no se utiliza habitual o frecuentemente en España? Sabemos que en algunos Estados americanos y europeos utilizan las TIC en sus procesos electorales y/o en

---

[14] Trechsel, Alexander H. *et al.*, "Potential and Challenges of e-voting in the European Union", 2016. Traducción propia, disponible en: *http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf.*

[15] Borge, Rosa, "La participación electrónica: estado de la cuestión y aproximación a su clasificación". *Revista D'Internet, Deret i Política*, 1/2005, p. 2. Disponible en: *https://idp.uoc.edu/articles/abstract/10.7238/idp.v0i1.367/*.

[16] Digital democracy virtual democracy, cyberdemocracy, e-democracy: son algunos de los términos utilizados para conectar la democracia y los ciudadanos a través de las TIC, y que se enfrentaría a la práctica 100% analógica.

[17] En el caso español, su encaje constitucional supondría ese mayor cumplimiento de los artículos 9.1 y 2, 23.1 o 92 CE relacionados con la participación ciudadana en los asuntos públicos.

[18] Ganuza, Ernesto y Francés, Francisco, *El círculo virtuoso de la democracia: los presupuestos participativos a debate,* Madrid, Centro de Investigaciones Sociológicas, 2012.

[19] Arnstein, Sherry R., "A Ladder of Citizen Participation", *Journal of the American Planning Association,* 35, 4, 1969, pp. 216-224. Disponible en: *http://www.participatorymethods.org/sites/participatorymethods.org/files/Arnstein%20ladder%201969.pdf.*

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

referéndums; empero, en España existe una cierta reticencia a usar este método. Quizá como consecuencia de ese "estigma" negativo o visión de cautela del artículo 18.4 CE que habla de la limitación del uso de la informática (para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos) siendo significativa esa limitación que no regulación.

Cierto es que para cuestiones menores se comienza a usar la web 3.0, facilitando así no sólo la puesta a disposición de información,[20] sino la interactuación con los ciudadanos.[21] Igualmente, somos conocedores de proyectos que estudian la posibilidad futura y enclaves donde se van ensayando[22]

[20] Ello también es consecuencia del impulso europeo de la transparencia.

[21] Cotino esquematiza esa participación ciudadana electrónica en el marco constitucional español en las siguientes esferas: la administración, artículo 105 C.E.; la administración de justicia, artículo 125 C.E.; procesos de formación de voluntad estatal; la vida económica, artículos 129 y 131.2 C.E.; la vida social, artículos 51.2 y 129.1 C.E.; y la vida cultural, artículo 48 C.E., en Cotino, Lorenzo (coord.), *Democracia, participación y voto a través de las nuevas tecnologías,* Granada, Comares, 2007, pp. 8 y 9.

[22] En España se han realizado diversas experiencias piloto. Comunidades autónomas:

País Vasco: En 1998, pionero en la regulación del voto electrónico para las Elecciones al Parlamento Vasco. Desarrolló su sistema de voto electrónico, Demotek.

Cataluña: En 1995, desarrolla una experiencia en dos colegios electorales en las elecciones al Parlamento de Cataluña con tarjetas de banda magnética. En 2003, en las elecciones al Parlamento de Cataluña se realizó una prueba piloto de voto electrónico remoto para los electores catalanes residentes en el extranjero (Argentina, Bélgica, Estados Unidos, México y Chile). También experimentó en estas elecciones con dos sistemas diferentes de voto electrónico presencial en cinco municipios: uno el sistema Demotek y otro de una empresa privada mediante pantalla táctil. En 2010, el ayuntamiento de Barcelona realizó una consulta ciudadana en la que utilizó votación electrónica a través de Internet o telefonía móvil.

Galicia: en 1997, en las elecciones al Parlamento de Galicia se probaron en dos mesas electorales dos sistemas: francés y japonés, con pantalla táctil. En 2005, en las elecciones al Parlamento de Galicia tuvieron lugar dos pruebas de voto electrónico con pantalla táctil.

Comunidad valenciana: en las elecciones autonómicas de 1999, se desarrolló en Villena una experiencia del voto con el sistema de votación electrónica francés CIVIS, que utiliza banda magnética, en la totalidad de las 39 mesas electorales.

Andalucía: en 2004 efectuó en el municipio de Jun una prueba de voto electrónico a través de Internet.

Estado español: En las elecciones generales de 2004 se realizó la primera prueba de voto electrónico remoto en tres mesas. En 2005, con ocasión del referéndum de la Constitución Europea, se realizó un ensayo de voto electrónico remoto por Internet, días previos a las elecciones en un municipio de cada una de las provincias. En las elecciones a diputados y senadores de 2008, en las Europeas de 2009, y en las municipales de 2011 (también en las autonómicas de Cataluña de 2010), se experimentó en diversas poblacio-

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

tímidamente[23] este tipo de tecnologías[24] en relación con los procesos participativos. Una cuestión diferente parece que es la posibilidad de utilizar estas tecnologías en procesos más serios, como son los referéndums constitucionales o las elecciones generales, en un futuro próximo.

En tal sentido, podríamos advertir que la Unión Europea, en su estrategia 2020, viene mostrando su interés por el estudio de las TIC ante las elecciones al Parlamento Europeo, y es quizá a través de ese interés que los Estados miembros, que o bien no se han iniciado, o bien lo hay hecho tímidamente, puedan incorporar estas tecnologías a sus procesos electorales y/o refrendarios, una vez comprobada la fiabilidad, seguridad, en clave europea. Si bien es cierto que se observan dos corrientes o posiciones a nivel europeo en cuanto a la democracia digital: por un lado el interés de la Unión Europea, concretamente en lo referido al Parlamento, a fin de acercarse al ciudadano europeo, y de ese modo conseguir la tan ansiada "identidad europea" mediante el uso de esas TIC y, por otro, ese paso atrás de los Estados miembros que habiendo implantado estas tecnologías vuelven a su revisión, e incluso a su eliminación parcial, por estimar su inseguridad o un riesgo mayor que su beneficio ante una vulneración. Como consecuencia, se podría advertir que la implementación de las TIC en los procesos electorales y/o refrendarios a nivel de Estado miembro devendría del impulso y de la armonización europea, puesto que el Estado no pareciera encontrarse en este momento dispuesto a un compromiso firme, sino al contrario.

En todo caso, dar contestación a la pregunta planteada, y cuya principal disculpa les adelanto, presupone la seguridad,[25] la ciberseguridad,

---

nes a instancias del Ministerio del Interior el sistema de la mesa administrada electrónicamente, disponible en: *http://www.euskadi.eus/botoelek/otros_paises/ve_mundo_est_c.htm#francia*.

[23] Ejemplo de la regulación electoral vasca. Ley 15, de Elecciones al Parlamento Vasco, del 19 de junio de 1998, disponible en: *https://www.euskadi.eus/y22-bopv/es/bopv2/datos/1998/07/9803142a.pdf*. Cataluña y su intento actual de tramitación de la ley de voto electrónico para el "referéndum de octubre de 2017".

[24] En el ámbito español podríamos resaltar el impulso de la administración electrónica y el interés en el ámbito local de estas tecnologías, que favorecen la participación ciudadana.

[25] Y así queda reflejado por los pronunciamientos de la Junta Electoral Central, siendo uno de los últimos el acuerdo de la Junta Electoral Central, sesión JEC: 16/11/2016, núm. 261/2016, expediente: 109/160. Objeto: Informe de la Junta Electoral Central sobre la regulación del voto de los electores españoles que residen o se hallan en el extranjero (texto refundido), disponible en: *http://www.juntaelectoralcentral.es/cs/jec/doctrina/acu*

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

en un primer momento,[26] hemos de conectarla también con cuestiones normativas.

Podemos advertir, de ese modo, que la democracia digital presenta dos ámbitos de estudio,[27] que se afectan: uno, relativo a la propia institución democrática, y que sería preeminentemente teórico y, un segundo ámbito, que lo configuraría la práctica de estas tecnologías de la información y de la comunicación. En este sentido

> Los temas teóricos se centran en los conceptos de democracia en general, ideas y definiciones para la democratización electrónica, el papel de Internet, las TIC y CMC[28] en el sistema político, las influencias de las culturas políticas existentes, las comparaciones de América y Europa en el desarrollo de democracia, transformaciones estructurales de las esferas públicas y nuevos conceptos de opinión pública. Los problemas de práctica (aplicaciones) se refieren a políticas para construir aplicaciones, políticas en el diseño de interacción, políticas de contenido, la relación de CMC con otros medios existentes como canales de comunicación, la brecha entre la comunicación rica y la comunicación pobre, las cualidades de los debates políticos virtuales y medios para gestionar la interacción social para mantener el acceso y la participación democráticos. [29]

erdos?packedargs=anyosesion=2016&idacuerdoinstruccion=43123&idsesion=889&template=Doctrina%252FJEC_Detalle.

[26] Empero, no sería la única razón, pues somos conocedores de la influencia que el concepto "brecha digital" tiene a este respecto, más aún cuando la población española es una de las más envejecidas. En este orden de cosas, podemos apuntar que no sólo atendemos a la capacidad de conexión, sino al uso correcto, consciente, de las tecnologías de la información y de la comunicación. Igualmente, debemos relacionarlo con la población que tiene tal habilidad y su intención de voto.

[27] En otras palabras, "las acciones normativas relativas al marco de normas que configuran el sistema electoral y que serían susceptibles de reformas; y las acciones inquisitivas relacionadas con la doctrina y los estudios de un lado y con la experimentación las pruebas y los ensayos de otro", Gálvez, Luis A., "El futuro del voto electrónico en España", en Barrat, Jordi (coord.), *El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado,* Madrid, Iustel, 2016, pp. 219-260.

[28] CMC: Computer-Mediated Communication.

[29] Hacker, Kenneth L. y Van Dijk, Jan, *Digital Democracy. Issues of Theory and Practice*, Londres, Sage Publications, 2006, p. 4. Traducción propia.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

1. La problemática práctica en los procesos participativos: la seguridad

Con relación a la práctica —entendida como los medios o mecanismos de participación, la tecnología utilizada— debemos preguntarnos si la utilización de los mismos constituye una mejora en la calidad democrática y si su implementación supone una mayor eficacia y eficiencia; esto es, si el beneficio obtenido en su incorporación es mayor al posible riesgo que se advierte. Y ello, puesto que

> la determinación de los instrumentos materiales de votación, es decir, de todos aquellos medios que ha de utilizar el elector a la hora de elaborar y expresar su opción política, es una de las decisiones más relevantes que ha de tomar el legislador a la hora de regular la organización de las elecciones, por la incidencia que pueda ocasionar en la regularidad del proceso electoral y, por tanto, en su misma credibilidad.[30]

En consecuencia, la seguridad o vulnerabilidad de los procesos participativos refrendarios en relación con las TIC, es objeto de análisis debiendo conectarlo con los principios constitucionales relacionados con el sufragio.

A este respecto, Gálvez plantea la posibilidad del voto electrónico en su visión positiva, facilitar el ejercicio del derecho de sufragio principalmente, pero también en su visión negativa, sus limitaciones,

> la principal es que el voto por internet plantea graves problemas para la integridad de la mayoría de los principios del sufragio. Así, es difícil garantizar que el voto lo emite realmente el elector y no otra persona por él; que lo hace en un ambiente de plena libertad, sin coacción de ningún tipo; y que el sentido de su voto va a permanecer en secreto, sin poder ser espiado o desvelado por nadie. Hay que tener en cuenta, además, otros problemas. Entre otros, cabe citar la pérdida del control de la votación por parte de los electores (miembros de mesas electorales) y los militantes de los partidos (interventores) en beneficio de los profesionales de la informática; el menoscabo del rito de las elecciones, que tanta importancia

[30] Gálvez, Luis A., "Aproximación al voto electrónico presencial: estado de la cuestión y recomendaciones para su implantación", *Teoría y realidad constitucional*, (23), 2009, pp. 257-270. Disponible en: *http://e-spacio.uned.es/fez/eserv/bibliuned:TeoriayRealidadConstitucional-2009-23-50090/PDF.*

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

> tiene como factor de integración de la comunidad; y las dudas sobre la seguridad de las comunicaciones electrónicas.[31]

Estas advertencias de Gálvez son extrapolables a la celebración de un referéndum en el cual se implementen las TIC.

Empero, esta postura o visión negativa del análisis legal en el impacto de la votación por Internet sobre los principios constitucionales de la ley electoral: sufragio universal, igual, libre, secreto y directo, encuentra contestación por Garrone[32] en el "Estudio para la implantación del voto por Internet o electrónico en unas elecciones al Parlamento Europeo",

> el voto por Internet no representa ninguna amenaza para los principios del sufragio directo. El principio del sufragio universal, según el cual todos tienen derecho al voto, sólo podría verse perjudicado por la introducción de la votación por Internet como única modalidad de votación, ya que las personas que no tienen acceso a Internet podrían verse impedidas de votar.

Al respecto de la

> noción un votante un voto, subyacente al sufragio igualitario, no puede asegurarse de igual modo que con los medios tradicionales de votación, que requieren la identificación de los votantes "sobre el terreno", pero esta advertencia también es común a la votación por correo. El sufragio libre no se ve amenazado significativamente por el voto en Internet, a excepción del voto familiar, limitación común para el voto por correo. Por último, garantizar el voto secreto depende en gran medida del diseño y la calidad del sistema; las operaciones de verificación, de quién votó y de quién cuenta el voto, deberían ser independientes y la plataforma debería aspirar a los estándares máximos de privacidad y seguridad.

---

[31] *Idem.*

[32] Garrone, "Fundamental and Political Rights in Electronic Elections", en Trechsel, A. H. y Méndez, F. (eds.), *The European Union and e-voting: Addressing the European Parliament's Internet Voting Challenge*, Nueva York, Routledge, 2005, en Trechsel, Alexander H. *et al.*, "Potential and Challenges of e-voting in the European Union", 2016. Traducción propia. Disponible en: *http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556948/IPOL_STU%282016%29556948_EN.pdf.*

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

La confrontación que trasciende en el ámbito constitucional respecto del análisis de los principios del sufragio[33] tienden a la comparación de los sistemas remotos, o presenciales de votación en sus diferentes modalidades, respecto de los sistemas tradicionales de votación, interesando en este aspecto el voto por correo por ser éste el que revisa tales principios. Si bien nos detendremos en estas cuestiones en un momento posterior, pues ahora nos ocupa el análisis de la práctica.

Apuntábamos anteriormente, que una de las principales excusas o motivos por los cuales no se han implementado las TIC en los procesos electorales generales y/o en los referéndums constitucionales en España, supone atender a la ciberseguridad.

Las dudas planteadas por varios autores sobre la posibilidad de utilizar sistemas presenciales o remotos electrónicos, en sus diferentes modalidades, y la importancia de la confianza que han de generar en la ciudadanía, pasaría por dar contestación a estas dos preguntas: ¿se puede *hackear* un proceso refrendario y/o unas elecciones? ¿se puede influir en los mismos a través del uso de las TIC? Así, varios son los momentos que podemos considerar ante la posibilidad de llevar a cabo un proceso participativo o consultivo mediante el uso de las TIC, de máquinas electrónicas de participación, de votación remota.[34] Por lo tanto, pretendemos realizar, en este momento, una esquematización de aquellas vulnerabilidades que podrían condicionar ese proceso participativo que nos ocupa, desde una perspectiva amplia, y no sólo del propio proceso.

Gilbert,[35] en su artículo "Votos en riesgo: seis maneras de hackear elecciones", apunta varias de las posibilidades de alterar los resultados de unas elecciones en el enclave estadounidense, alguna de las cuales podríamos aplicar a la casuística española ante un referéndum: *hackear* las máquinas de votación, listas electorales corruptas, *hackear* la agencia Associated Press, un ataque "DDoS" a gran escala, *hackear* la infraestructura crítica

[33] Gálvez Muñoz, Luis A. y Ruiz González, José Gabriel, "El voto electrónico y el test de calidad; o de cuatro bodas complicadas y un posible funeral", *UNED. Revista de Derecho Político,* núm. 81, mayo-agosto de 2011, pp. 253-274.

[34] Pareciera que la Unión Europea se hubiera decantado por la votación remota, a la luz del mencionado estudio, a saber: Trechsel, Alexander H. *et al.*, "Potential and Challenges of e-voting in the European Union", *cit.*

[35] Gilbert, David, *Votos en riesgo: seis maneras de* hackear *las elecciones*, 2016. Disponible en: *https://news-old-origin.vice.com/es/article/votos-riesgo-seis-maneras-hackear-elecciones*.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

del país y divulgar información errónea. Mientras De Diego Ramos[36] se centra en varias de ellas: el *doxxing* y las filtraciones, la propaganda y difusión de noticias falsas, los sistemas electorales y la defensa y seguridad nacional.

Analicemos alguna de estas opciones plausibles en el caso español:

A. Prácticas indirectas a través de difusión de información, filtraciones y *doxxing*

Una de las primeras posibilidades que pueden alterar el resultado de unas elecciones generales o de un referéndum constitucional, tiene relación con la información puesta a disposición de los ciudadanos, pues a través de la misma se intentaría influir[37] en la opinión de éstos a fin de conseguir su voto. Ese condicionamiento de la opinión pública se encuentra conectado con las prácticas informáticas a través de varias técnicas: *mailing*, *hackeo de webs*, *social network*, *uso de bots*, *fake news*, *trols*, *doxxing*. La existencia de cibervoluntarios que se dedican a crear opinión pública junto con la actividad de los profesionales ofertan, como vemos, una infinidad de posibilidades a llevar a cabo.

Las redes sociales, por su usabilidad y capacidad de alcanzar a una multitud de sujetos, se han convertido en las herramientas más importantes para la difusión de información, si bien esa ventaja advertida supone también su mayor vulnerabilidad, al ser un medio de difusión de información incorrecta, mal intencionada, de desinformación".[38] Las

[36] Diego Ramos, Gonzalo de, "El «doxxing» o el nuevo peligro que amenaza a las democracias", 2017, disponible en: *https://www.elconfidencial.com/alma-corazon-vida/2017-02-28/politica-ciberseguridad-democracia-elecciones-noticias-falsas-filtraciones_1340272/*.

[37] En palabras recogidas en el Informe del Consejo de Estado elaborado por la Comisión de Estudios del Consejo de Estado, en sesión celebrada el 24 de febrero de 2009 sobre las propuestas de modificación del régimen electoral general de 2009: "este llamado aspecto teleológico de la norma que regula las campañas institucionales ha sido muy debatido. En su tenor actual —derivado, a su vez, de reforma legislativa de la primigenia versión de la LOREG— cabe localizar un elemento negativo determinante (en ningún caso puede influir en la orientación del voto) y una enumeración positiva de contenidos de naturaleza estrictamente informativa".

[38] Pablo Pardo Plantea en su artículo la relación entre información, prestadores de servicios, y responsabilidad de los mismos: "la responsabilidad de plataformas como Facebook, Twitter y Google pasa por ajustar su credibilidad y remarcar cuando una información proviene de una fuente de confianza. Una posibilidad es que, cuando se comparta un contenido en uno de estos sitios web, se informe —o se recuerde— el daño que la

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

fake news,[39] en el plano legal, están dando lugar a un debate encarnizado mediante la confrontación de principios constitucionales de libertad de expresión,[40] derecho a la información y seguridad.[41] Esas redes sociales,[42] que son utilizadas por las diferentes tendencias que participan de un proceso electoral o referendario, pueden ser utilizadas con ese fin malintencionado y condicionar así el voto, a través de la creencia de una información falsa o incorrecta o de la creación de opinión pública, si bien somos conocedores del surgimiento de la tendencia *fact-checking*[43] que pone a prueba esas informaciones falsas o manipuladas.

Los medios de comunicación[44] también juegan un papel importante en la difusión de esta información,[45] a veces manipulada.[46] El "cuarto poder" ha sido objeto de escándalos por favorecer a alguno de los candidatos o a algunas de las posturas, así como también pueden ser objeto de amenazas

---

desinformación puede llegar a causar en quien la termina recibiendo. También podrían diseñar algoritmos que releguen el *clickbait* a la parte más baja del *timeline*. Son cambios difíciles porque afectan a su eficacia comercial, de modo que quizá precisen de un empuje legislativo". *Cómo Internet se convirtió en una amenaza para la democracia*, disponible en: *https://www.facebook.com/elmundo/posts/10155093319231867*.

[39] Palmer, Ellis, *Spain Catalonia: Did Russian 'fake news' stir things up?*, disponible en: *http://www.bbc.com/news/world-europe-41981539*.

[40] En este sentido, la regulación alemana de las redes sociales "Act to Enforcement of the Law in Social Networks". Disponible en: *https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2*.

[41] Véase el Proyecto de Ley francés conocido como "la fiabilidad de la confianza de la información".

[42] El ejemplo más reciente se puede circunscribir a la campaña del Brexit y el uso de perfiles de la red social Facebook, disponible en: *https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions* y en: *https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump*.

[43] El *fact-checking* suele identificarse con ese periodismo, que contrasta o comprueba la veracidad de las informaciones diseminadas por Internet, redes sociales. Si bien en su forma ampliada podríamos llegar a aquellos grupos civiles organizados que remiten estas informaciones veraces o desmienten las *fakes news*.

[44] "UK phone hacking scandal: The News of the World didn't go far enough", 2009. Disponible en: *https://wikileaks.org/wiki/UK_phone_hacking_scandal:_The_News_of_the_World_didn%27t_go_far_enough*.

[45] Un ejemplo, de esta posibilidad de influir en los procesos democráticos por los medios de comunicación, serían las noticias sobre Matteo Renzi, la abundante propaganda mediática con el Brexit, las opiniones sobre Le Pen y Macron o las noticias sobre las elecciones presidenciales de USA.

[46] Disponible en: *http://www.huffingtonpost.es/2017/09/17/posverdad-y-redes-sociales-una-amenaza-para-la-democracia_a_23063245/*.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

informáticas o susceptibles de ser *hackeados*. Pensemos qué sucedería si se difunden resultados falsos a través de los medios de comunicación; el cuestionamiento de ese referéndum sería inevitable, al igual que la desconfianza ciudadana ante una rectificación de la información previamente difundida por las agencias de noticias.

Hemos de reparar igualmente en la posibilidad de que se produzca *doxxing*[47] o investigación, recopilación y difusión de información, generalmente de carácter privado, sobre una persona específica o un partido o grupo político, con el objetivo de perjudicarla. Esta información suele difundirse en el momento en que se obtiene un mayor rédito político, campaña electoral,[48] previamente a las fechas señaladas para un referéndum, con el propósito de minorar los votos de su opción defendida. Incluso su uso se haría más efectivo en casos en los cuales la población se encuentre más polarizada o fracturada, como en un referéndum, puesto que "la utilización de la misma por parte de algún candidato le otorga una relevancia que multiplica su impacto en la opinión pública".[49] Ante esta eventualidad, en la fase tanto de recopilación como de difusión, se plantea la ciberseguridad de las personas potencialmente expuestas,[50] pues en ocasiones no aplican ni las mínimas pautas de seguridad que se

[47] Recopilación de documentación, información, etcétera, sobre una persona, un grupo de personas, organización, disponible en Internet, generalmente para su posterior tratamiento y difusión.

[48] Respecto a la campaña electoral, García Mahamut advierte de que "La realidad se muestra tozuda y habrá que prepararse para afrontar la existencia de bases de datos por parte de los partidos que capturarán información sobre los votantes de una variedad de fuentes importantes. Ello se pondrá a disposición de campañas personalizadas y dirigidas a concretos segmentos del electorado. Lo que abre una perspectiva no demasiado alentadora: ¿dónde queremos poner los límites?", en García Mahamut, Rosario, "Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español", *Teoría y Realidad Constitucional*, Madrid, UNED, núm. 35, 2015, pp. 309-338, disponible en: *http://revistas.uned.es/index.php/TRC/article/viewFile/14921/13256*.

[49] Torres Soriano, Manuel R., "Hackeando la democracia: operaciones de influencia en el ciberespacio". Documento de opinión 66/2017, Instituto Español de Estudios Estratégicos, disponible en: *http://www.ieee.es/temas/ciberseguridad/2017/dieeeo66-2017.html*.

[50] En este sentido: Burguera Ameave, Leyre y Cobacho López, Ángel, "El derecho al olvido de los políticos en las campañas electorales", en Corredoira, Alfonso L. y Cotino Hueso, L. (dirs.), *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales*, Madrid, Centro de Estudios Políticos y Constitucionales, 2013, pp. 501-520.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

les presupone a los usuarios normales, y ello facilita en exceso el acceso a la información de carácter privado, personal, e incluso institucional.

Este tipo de prácticas se concentran por tanto en una fase previa a la propia fecha de la celebración de las elecciones o del referéndum, y su principal interés es la creación de opinión pública a través de la cual se interfiere en el resultado de los mismos.

B. Prácticas directas a través de técnicas de hackeo a webs, sistemas de votación e infraestructuras críticas

A través de estas técnicas lo que se pretendería es la injerencia directa en algunos de los sistemas que tendrán un claro protagonismo o incidencia en el procedimiento.

Hackear webs o ataques "DDoS": en este caso lo que se pretendería sería inhabilitar las *webs* de las partes enfrentadas para impedir el acceso a la información, la comunicación, o bien conseguir información de carácter privado y/o personal, como puedan ser las listas de las personas afiliadas a un partido político o grupo de interés, modos de financiación de las campañas. También podrían verse afectadas por esta práctica otro tipo de *webs* que desarrollan un papel importante en un proceso electoral o refrendario, redes sociales, medios de comunicación, imprentas. El *hackeo* de estas *webs* puede ser ilícito o lícito, como ocurre con el mal denominado "referéndum catalán del uno de octubre" y las medidas adoptadas por el Juzgado de Barcelona número 13, tendentes a limitar el acceso a las *webs* del mismo. La licitud vendría desarrollada por las fuerzas y cuerpos de seguridad del Estado en aras a proteger un interés general y derechos fundamentales, en absoluta connivencia con el derecho constitucional.

Hackear los sistemas de votación: la variedad de tecnologías puestas a nuestra disposición hace que podamos hablar de la posibilidad de realizar unas elecciones generales o un referéndum constitucional TIC. Empero, la preocupación ante la posibilidad de alterar los resultados de una votación que utilice este tipo de tecnologías supone la principal excusa para su no implementación, como apuntamos anteriormente. Si bien es cierto que algunas de estas máquinas no se conectan a la red, a Internet, no es menos cierto que el *hackeo* puede darse en la propia fase de fabricación del *software* o en fases posteriores de escrutinio.[51]

Esta posibilidad, que comenzó a preocupar en Estados Unidos a partir de la emisión del documental "Hacking Democracy", en 2006, y que dio

[51] A modo de ejemplo la amenaza de Anonimus a las elecciones del 21-D de Cataluña.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

lugar a innumerables artículos, ha sido advertida por David Dills, quien afirma que si bien no cree que haya habido ningún problema en relación con el procedimiento electoral estadounidense, tampoco puede demostrar que no lo hubo. E igualmente advierte que "para cada procedimiento de seguridad que una compañía pueda implementar para derrotar esos esfuerzos, los piratas informáticos producirán más métodos sofisticados para evitarlos".[52] Mientras que Harris advierte de la posibilidad de intereses ocultos en las compañías que fabrican estas máquinas de votación: "las máquinas almacenan sus datos de una manera que no es fácilmente" auditable, "y que están hechos por compañías que tienden a ser reservadas acerca de sus procesos e inversores".[53] Michaels apuesta por la auditoría como una posible solución a la vulnerabilidad de las máquinas

> La verificación manual de los votos contados por las máquinas es esencial. El recuento por el que Jill Stein recaudó millones revela una crisis en la rendición de cuentas y la transparencia de las elecciones estadounidenses. Sólo los ojos humanos y el recuento manual de los votos pueden estar seguros de exponer los errores de la máquina o la piratería.[54]

Aunque estas ideas responden a la realidad estadounidense.

A estas voces se unen las del especialista en *hacking* Antonio Ramos:[55] "No hay que olvidar que el *software* puede ser manipulado tanto desde fuera como desde dentro, es decir, desde quien fabrica el sistema". Empero, también existen posturas de defensa de estas tecnologías que se enmarcan dentro no sólo de la rapidez y sencillez del procedimiento electoral sino también de la seguridad de las tecnologías utilizadas, como es el caso de Ignacio del Corral:[56]

---

[52] David Dills es ingeniero informático de la Universidad de Stanford; *cfr*. Manjoo, Farhad, *Hacking Democracy*, 2003, traducción propia, disponible en: *http://www.salon.com/2003/02/20/voting_machines_3/*.

[53] Harris es un publicista y escritor literario, cuyas investigaciones sobre el mundo secreto de las empresas de equipos de votación han llevado a algunos a llamarla *Erin Brockovich* de las elecciones, en Manjoo, F., 2003, *Hacking Democracy*, traducción propia, disponible en: *http://www.salon.com/2003/02/20/voting_machines_3/*.

[54] *Cfr*. Figueredo, Mike, *10 Years After HBO's Hacking Democracy, Electoral Vulnerabilities Still Exist,* 2016, traducción propia, disponible en: *http://www.huffingtonpost.com/entry/584f8d14e4b0016e5043070b?timestamp=1481683802425*.

[55] *Cfr*. Diego Ramos, Gonzalo de, "El «doxxing» o el nuevo peligro que amenaza a las democracias", *cit.*

[56] *Idem.*

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

> Las máquinas electorales son más seguras que las papeletas. Todo es vulnerable, la papeleta también, todo tiene su grado. Se puede poner un nivel de seguridad muy alto, si bien nunca será del 100%, pero cuantos más cortafuegos haya, más difícil va a ser interferir en las votaciones. Yo creo que es más seguro e infinitamente más rápido. Manipular el sistema de elecciones de un país europeo no está al alcance de cualquiera.

Con todo ello podemos advertir la posibilidad real de *hackear* estas máquinas en orden a conseguir un resultado alterado en la votación, si bien una auditoría que recuente manualmente las papeletas o los votos podría asegurar la veracidad de los datos ofrecidos por las máquinas, pese a que ello implicaría dos cosas: la primera, la existencia de un trazo en papel/comprobante de la votación, y la segunda, el recuento posterior y tardío de los resultados a fin de determinar la veracidad de los mismos o la ulterior corrección; ello se conoce como "método Mercuri".[57] Sin ese trazo de papel, la auditoría[58] posterior parecería seguir contando con las mismas dudas o inquietudes que el procedimiento en sí, dado que hablaríamos de *software*, de líneas de código indescifrables a ojos de personas no expertas en programación. Esa no fiscalización del proceso electoral supondría que el constitucional alemán[59] se pronunciara en 2009 en contra del sistema de urna electrónica utilizada, por vulnerar el principio de publicidad en la fase de escrutinio.

No hemos reparado aún en la posibilidad de que la votación[60] se pueda llevar a cabo desde nuestras casas con un simple clic desde nuestros dispositivos en una *web*; ello abriría infinidad de posibilidades de vulnerabilidades, desde la falta de seguridad en nuestros propios dispositivos infectados por *malwares*, *hackeados* o la propia *web* donde se produce la votación, hasta el robo de identidades.

---

[57] Más información, disponible en: *http://webdelprofesor.ula.ve/economia/sananes/ForoProfesoral/20060520%5BForoprofesoral%5D%20Fwd%20Declaraci%F3n%20de%20experta%20sobre%20Voto%20Electr%F3nico.htm.*

[58] En este caso lo que se podría valorar es el coste-beneficio ante el uso de estas tecnologías y la necesidad de la auditoría posterior con presencia de trazo de papel.

[59] Sentencia 2 BVC 3/07 - 2 BVC 4/07, disponible en: *http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-019.html.*

[60] En este sentido: González de la Garza, Luis M., *Voto electrónico por Internet, construcción y riesgos para la democracia,* Madrid, Edisofer, 2008.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

Últimamente se apuesta por la tecnología *blockchain*[61] como una posibilidad futura de participación, que posibilitaría el conocimiento de los datos reales en todo momento y dificultaría la manipulación de los mismos, pues atendemos a una base de datos de lectura. Empero, ello parecería que entra en conflicto con la normativa electoral, en tanto que al disponerse de los datos reales de votación cabría la posibilidad de advertir de la tendencia que va en ventaja e influir en el referéndum, hablaríamos de un escrutinio[62] general instantáneo, que se opondría al artículo 95.1 de la Ley Orgánica de Régimen Electoral: "terminada la votación, comienza, acto seguido, el escrutinio".

Hackear la infraestructura crítica del país: esta opción sería uno de los mayores retos a los cuales se enfrentaría un *hacker*, pues se presupone que la mayor inversión en ciberseguridad se destina a la protección de aquellas infraestructuras críticas, sensibles, del Estado. Pero no podemos cerrar los ojos ante la veracidad[63] de los intentos de *hackeo* que sufrimos a diario, la "ciber guerra"[64] es un hecho, y los intereses que existen detrás de la misma son infinitos.

Esta idea de vulnerabilidad, pese a contar con la tecnología suficiente para desarrollar un proceso participativo digital, es la defendida por la Secretaría de Estado de Seguridad[65] española para descartar la posibilidad del voto electrónico,[66] pese a que se sigan desarrollando proyectos, investigaciones para albergar en un futuro el uso de estas TIC en procesos refrendarios y elecciones.

---

[61] Preukschat, Alexander (coord.), *Blockchain: la revolución industrial de Internet,* Barcelona, Gestión, 2017.

[62] Arnaldo Calcubilla, Enrique y Delgado-Iribarren García-Campero, Manuel, *Código electoral*, Madrid, La Ley, 2007.

[63] Un ejemplo de ello sería el *hackeo* que sufrió Ucrania en su red eléctrica en diciembre de 2015, la brecha de seguridad en el Aeropuerto Internacional de Stewart en Estados Unidos.

[64] Seamos conscientes de los cinco escenarios donde se han de garantizar la seguridad: tierra, mar, aire, espacio y ciber.

[65] "El secretario de Estado de Seguridad, José Antonio Nieto Ballesteros, ha afirmado que el gobierno descarta implantar el voto electrónico debido al aumento de la ciberdelicuencia, a pesar de contar con la tecnología necesaria para hacerlo", *El País*, 1o. de junio de 2017, disponible en: *https://politica.elpais.com/politica/2017/06/01/actualidad/1496339415_076530.html*.

[66] Ampliar información en: *http://www.csd.gob.es/csd/asociaciones/1fedagclub/procesos-electorales-y-voto-electronico/descripcion-del-sistema-de-voto-electronico-proporcionado-por-el-csd/*.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

Imaginemos qué sucedería si se consigue alterar la información de los electores, si se consigue interrumpir la red eléctrica de un país, la red de comunicaciones. Podríamos hablar de cuestiones temporales, aplazar un proceso consultivo, unas elecciones, pero también de un caos en el Estado que lleve mucho tiempo solventar, con los respectivos costes.[67]

A este respecto, el departamento de seguridad norteamericano advierte que "un ataque la infraestructura crítica durante las elecciones, sería visto como un acto de guerra"[68] De este modo, se ha declarado el propio proceso electoral como infraestructura crítica, a fecha de enero de 2017, e irrumpir en las bases de datos de votantes y otros elementos de la infraestructura crítica y electoral atendería a esa caracterización.

En el marco de seguridad español, hemos de señalar que el propio proceso electoral y/o refrendario habría de ser calificado como "infraestructura crítica",[69] para de ese modo asegurar la protección que brinda la normativa[70] específica, sin dejar margen a la interpretación judicial, al igual que hace Estados Unidos.

Frente a estos intereses existentes, de injerencias en procesos electorales o refrendarios,[71] como puedan ser los que incitan a actuar a las APT, como APT28[72], *Dragonfly 2.0* o *Hidden Cobra*, existe la dificultad de determinar quién está detrás de los mismos y cuál es su verdadera motivación. El rastreo de estas prácticas, más aún cuando las desarrollan

[67] "Hemos conectado servicios vitales a sistemas digitales que pueden ser atacados desde Internet. El coste de estos ataques es infinitamente más económico que movilizar material a una frontera. Cuantos más objetos tienes conectados, los riesgos se disparan" Ramos, Antonio en: Diego Ramos, Gonzalo de, *El doxxing o el nuevo peligro que amenaza a las democracias*, 2017, disponible en: *https://www.elconfidencial.com/alma-corazon-vida/2017-02-28/politica-ciberseguridad-democracia-elecciones-noticias-falsas-filtraciones_1340272/*.

[68] Gilbert, David, *Votos en riesgo: seis maneras de hackear las elecciones*, 2016, disponible en: *https://news-old-origin.vice.com/es/article/votos-riesgo-seis-maneras-hackear-elecciones*.

[69] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[70] Derivada de la Ley 8/2011 por la que se establecen medidas para la protección de las infraestructuras críticas.

[71] El ejemplo más actual serían las últimas elecciones a la presidencia de los Estados Unidos de Norteamérica, aún se escuchan ecos de la injerencia rusa y china, del espionaje a la candidata Clinton o la presumible injerencia en las filtraciones de información del candidato Emmanuel Macron los días previos a las presidenciales francesas.

[72] Entre sus objetivos se encuentra España, disponible en: *http://www.globalcybersec.com/reader.php?p=516*.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

verdaderos profesionales, se muestra en ocasiones como una tarea ardua, cuando no imposible, siendo esa vinculación inequívoca entre ataque y atacante la que dan lugar a la responsabilidad penal.[73]

La ciberseguridad en los procesos participativos ha de darse en todos los niveles y en las diferentes etapas: desde los sujetos/partidos que van a ser parte de los grupos que apoyan alguna de las opciones, hasta quienes acuden a votar o se encargan de verificar, auditar, el proceso en sí. Esta seguridad es reclamada previamente a la propia fecha de la votación, durante la misma y en fechas posteriores, a fin de garantizar la veracidad de los datos. Tan es así, que la ciberseguridad que se muestra como uno de los hándicaps a superar o mejorar para que la democracia digital, *digital democracy*, se instaura en el sistema participativo español.

> No hay que olvidar, por otro lado, que la emisión de un voto se configure en torno a un procedimiento electrónico requiere lograr previamente la confianza de los ciudadanos en el mismo. Los electores no deben albergar dudas sobre la seguridad de las llamadas "urnas electrónicas", es decir, deben tener confianza en que nadie pueda interferir el proceso de votación con la intención fraudulenta de eliminar, añadir o modificar votos".[74]

La ciberseguridad se presenta como la inversión necesaria frente al "gobierno del miedo"[75] en el contexto aquí planteado.

2. Teoría

La segunda de las posibilidades que apuntamos, al plantear la democracia digital, junto a la práctica, tenía relación con la teoría. La posibilidad de atender en un futuro a un referéndum constitucional o a unas elecciones generales TIC, no sólo se ve condicionada por cuestiones técnicas, que indudablemente son una de las razones principales de oposición a la instauración, sino que también dependen en gran medida de la normativa aplicable, al suponer una importante revisión del marco normativo y de los principios relacionados con el ámbito electoral. Ese compromiso

[73] Responsabilidad que hemos de unir a la teoría de la ubicuidad derivada del artículo 23.1, CP.

[74] Gálvez, Luis A., "Aproximación al voto electrónico presencial: estado de la cuestión y recomendaciones para su implantación", *Teoría y Realidad Constitucional*, *cit*.

[75] Recordemos que es este gobierno del miedo el que lleva a algunos países a paralizar su impulso en la *e-democracy*, a tenor de las hostilidades vividas a lo largo de los últimos años en el entorno ciber.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

no se trataría de una reforma nimia del proceso, sino que "alteraría de modo determinante la relación votante con el procedimiento electoral y por ello mismo subvierte algunos de los principios tradicionales de toda elección democrática".[76]

La dificultad normativa a la que nos enfrentamos aumenta en cuanto a que hemos de precisar el tipo de tecnología, procedimiento que se habría de incardinar, pues sólo con la definición de tal proceso se podrían mostrar al legislador las posibles modificaciones de las normas. Junto a ello, la influencia, apuntada, en los procesos electorales por las tecnologías de la información y de la comunicación, que están poniendo a prueba los principios y normas electorales, creando nuevos escenarios y conflictos que han de tener respuestas.

Hacemos cómplice al lector del presente trabajo, de la imposibilidad de profundizar en el mismo sobre el conjunto de principios expuestos a revisión. Es, por tanto, objetivo de este apartado el mostrar algunas de las disfunciones o nuevas problemáticas que se advierten en la interlocución tecnología-elecciones/referéndum a fin de su posterior resolución o investigación por quien nos considera.

A. Principios que rigen para el sufragio universal, libre, igual, directo y secreto

A este respecto, hemos que apuntar el diferente tratamiento de los procesos que nos ocupan, pues mientras las elecciones generales se someten a la Ley Orgánica 5/1985, del 19 de junio, del régimen electoral general, el referéndum tiene una doble regulación, a saber: la Ley Orgánica 2/1980, del 18 de enero, sobre regulación de las distintas modalidades de referéndum, y la Ley Orgánica 5/1985, del 19 de junio, del régimen electoral general, puesto que conforme al artículo 11 de la Ley de referéndum, se somete el procedimiento al régimen electoral general, en lo que sea de aplicación y no se oponga a la misma, guiándose por los principios que rigen para el sufragio universal, libre, igual, directo y secreto[77] en el ámbito que corresponda a la consulta.

---

[76] Barrat, Jordi (coord.), *El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado,* Madrid, Iustel, 2016, p. 14.

[77] Respecto del voto secreto Barrat I. Esteve, Jordi, "Cultura indígena y procesos electorales. A propósito del secreto del voto", en Pigrau Solé, Antoni (ed.), *Pueblos indígenas, diversidad cultural y justicia ambiental. Un estudio de las nuevas Constituciones de Ecuador y Bolivia*, Valencia, Tirant lo Blanch, 2013, pp. 211-228.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

En este último aspecto, los principios de sufragio, nos remitimos a la idea previa de necesidad de precisión de la tecnología a implementar,[78] así como al apartado precedente, si bien, apuntamos algunas de las cuestiones que preocupan en mayor medida al legislador y a las diferentes personas que estudian esta posibilidad.

La crítica que se dirige a la brecha digital[79] en cuanto a la universalidad e igualdad, que podría condicionar el proceso en tanto que no toda la población tiene capacidades tecnológicas y/o conexión a Internet, a la vez puede suponer un mayor cumplimiento para aquellos que teniendo esa capacitación se encuentran en dificultad de ejercer su derecho a voto por no estar de forma presente,[80] o que por circunstancias orográficas tienen ese obstáculo, siendo el voto remoto su opción, o en el caso de discapacidad, la tecnología, puede dar cumplimiento a la adaptación.[81] La universalidad en este sentido ha de ser entendida como el cumplimiento de una doble premisa: "el fácil manejo del sistema a implementar y la no exclusión de aquellos que previamente estaba integrados en el mismo".[82]

A su vez, hemos de relacionar estos principios de universalidad e igualdad con el carácter secreto del voto y con conceptos tales como encriptación, procesos que aseguren el anonimato del mismo y la garantía de un entorno controlado donde se eviten coacciones en la emisión, suplantaciones de identidades. En este último supuesto se estaría, asimismo,

[78] Ello podría comportar, en un primer momento, la modificación de la Ley Orgánica 2/1980, del 18 de enero, sobre regulación de las distintas modalidades de referéndum, pues en su artículo 16.1 se establece que la votación se realizará por medio de papeletas y sobres ajustados a modelo oficial y contendrá impreso el texto de la consulta, a salvedad de que esa tecnología no implique el cambio en la votación, por tener esa trazabilidad de papel.

[79] Brecha digital que hemos de entender en un sentido doble: por un lado la incapacidad o dificultad de acceso a la red y/o a las TIC, y por otro, la complejidad de acceder a la información, de entenderla, procesarla, etcétera.

[80] A este respecto también podemos remitirnos al voto por correspondencia artículos 72 y ss., LOREG.

[81] La adaptación supuso la modificación de la LOREG en 2011 en su precepto 87, apartado segundo, para personas con discapacidad visual, mientras que la discapacidad de forma genérica se contempla en el apartado primero del mismo precepto, que establece la presencia de una persona de confianza para la elección o colocación de la papeleta en el sobre o en la urna.

[82] Esa doble premisa es tenida en cuenta por Presno Linera, Miguel A., en Barrat I. Esteve, Jordi y Fernández Riveira, Rosa Ma. (coords.), *Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías,* Pamplona, Thomson-Reuters, 2011, pp. 35-38.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

asegurando la personalidad del sufragio; esto es, la identificación de quien posee ese derecho al voto. En este orden de cosas, respecto a la libertad del sufragio, la no coacción ni alteración del voto emitido,

> se hará preciso incluir nuevos procedimientos de control a fin de mantener incólume el objeto último de toda elección, es decir, la actuación libre del votante y una transparencia suficiente que permita verificar de forma independiente la corrección tanto del proceso en su conjunto como de los resultados finales.[83]

Ese principio de libertad podría ser el que más preocupe a aquellas personas encargadas de la ciberseguridad, como ya apuntamos al hablar del *hackeo* de los sistemas de votación, pues a través de su cumplimiento aseguramos el procedimiento democrático.

B. Principios relacionados con el periodo electoral: pluralismo, proporcionalidad, neutralidad e igualdad

Del análisis de la citada LOREG, en ambos casos de estudio, se deriva una necesidad de repensar la importancia de las tecnologías de la información y de la comunicación con relación al propio periodo electoral. Es quizá en este momento en el cual el poder y la política se relacionen de tú a tú con su electorado cuando se produce la confrontación de principios constitucionales derivados de este marco normativo, siendo la comunicación pieza angular de esa formación de la opinión pública, que subsecuentemente se trasladará a una opción en forma de voto.

Advertimos, líneas arriba, la importancia que las tecnologías de la información y de la comunicación tienen respecto a la creación de la opinión pública, más aún en la actualidad, donde el poder es poder de la comunicación, "poder y política se deciden en el proceso de construcción de la mente humana a través de la comunicación. En nuestro tipo de sociedad, los medios de comunicación de masas son decisivos en la formación de la opinión pública que condiciona la decisión política".[84] Esa importancia de los medios de comunicación no pasaría desapercibida para el legislador, quien la incorporó a través de una arquitectura de

[83] Barrat, Jordi (coord.), *El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado,* Madrid, Iustel, 2016, p. 14.

[84] Castells, Manuel, "Comunicación, poder y contrapoder en la sociedad red (II)", *Revista TELOS*, núm. 75, abril-junio de 2008, disponible en: *https://telos.fundaciontelefonica.com/telos/articuloautorinvitado.asp@idarticulo=1&rev=75.htm*.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

principios a la normativa electoral, siendo igualmente perfeccionada por la doctrina y la jurisprudencia constitucionales.

De este modo, los principios observados y en ocasiones confrontados serán los relativos al pluralismo político y social, igualdad, proporcionalidad y neutralidad informativa, derivados de los preceptos 60 a 68 de la LOREG, y en relación con los derechos y libertades comunicativas, informativas, que suponen lo relacionado a la campaña electoral y la observancia del principio de "legitimidad democrática".[85]

Estos principios que han venido estudiándose desde la perspectiva de los medios de comunicación tradicionales,[86] radio, prensa y televisión, con relación a la presencia y distribución de espacios temporales, plantean actualmente un nuevo escenario de análisis, el cibernético. Es en este espacio en el cual se potencia la presencia política en los periodos electorales, donde se perciben ciertos comportamientos que podrían incluso ser susceptibles de actitudes contrarias a la norma,[87] esto es, podríamos atender a prácticas calificadas como "delitos electorales" conforme a la LOREG (artículos 139 a 150). Pensemos en el siguiente ejemplo: ¿qué sucedería si un candidato *retweetea* a varios de sus votantes en una jornada de reflexión?, o si en un mitin en el que se prevé una intervención por

[85] A este respecto, la sentencia del Tribunal Constitucional 20/1990, en su FJ 4.a) "STC 6/1981: «El artículo 20 de la Constitución, en sus distintos apartados, garantiza el mantenimiento de una comunicación pública libre, sin la cual quedarían vaciados de contenido real otros derechos que la Constitución consagra, reducidas a formas hueras las instituciones representativas y absolutamente falseado el principio de legitimidad democrática que enuncia el artículo 1.2 de la Constitución, y que es la base de toda nuestra ordenación jurídico-política». En el mismo sentido se pronuncia la STC 159/1986, al afirmar que «para que el ciudadano pueda formar libremente sus opiniones y participar de modo responsable en los asuntos públicos, ha de ser también informado ampliamente de modo que pueda ponderar opiniones diversas e incluso contrapuestas». Y recordando esta sentencia la doctrina expuesta en las que hemos citado anteriormente, insiste en que los derechos reconocidos por el artículo 20, no sólo protegen un interés individual sino que son garantía de la opinión pública libremente formada, «indisolublemente ligada con el pluralismo político»".

[86] Kölling, Mario (coord.), *El sistema electoral español. Un debate de sus logros y deficiencias*, Zaragoza, Fundación Manuel Giménez Abad, 2012.

[87] Este supuesto ha sido advertido en el caso del Brexit o de las elecciones estadounidenses, por haberse, presuntamente, utilizado determinadas empresas informáticas/tecnológicas, para la consecución de un mejor posicionamiento en motores de búsquedas y un mayor impacto de la publicidad/propaganda, a través del uso de perfiles de redes sociales de sus ciudadanos. E igualmente por no haber sometido estas prácticas a la normativa electoral presupuestaria. Esta práctica podría ser observada en nuestro ámbito electoral.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

videoconferencia se *hackea* el mismo, ¿se aplican los delitos electorales? Este tipo de preguntas, en suma adquieren una mayor complejidad en cuanto al debate o confrontación doctrinal de quienes entienden que los conocidos como "delitos electorales" (artículos 139 a 150) no son aplicables en los supuestos de refrendo,[88] frente a quienes defendemos que sí ha de ser aplicable, por no responder a criterios de analogía, sino de interpretación, especificidad y remisión expresa (tipo general elecciones, tipo específico referéndum del artículo 23.1, CE). En otras palabras, quienes defendemos que estos tipos delictivos sí han de aplicarse en el referéndum, lo articulamos a través del artículo 11 de la Ley Orgánica de las distintas modalidades de referéndum, LO 2/1980, en cuyo apartado primero establece que "el procedimiento de referéndum estará sometido al régimen electoral general en lo que le sea de aplicación y no se oponga a la presente Ley"; por tanto, el espíritu del legislador es la remisión expresa a la LOREG; siendo el referéndum regulado en el procedimiento por ésta, atenderíamos, de esta forma, a una "interpretación" o a una "interpretación extensiva", pero no a una "analogía"; en otras palabras,

> la interpretación consiste en la búsqueda del contenido y alcance de un texto legal, en tanto que con la analogía no se interpreta una ley, que en absoluto falta, sino que, por el contrario, se aplica al caso concreto una regla que disciplina un caso semejante. De modo preciso podríamos, pues, decir que en la interpretación extensiva falta la expresión literal, pero no la voluntad de la ley, y en la analogía falta también la voluntad de ésta.[89]

Esa falta de expresión literal en los delitos electorales conforme a la LOREG, la suple la voluntad del artículo 11 de la Ley Orgánica de Referéndum.

Reconociendo que nuestro Tribunal Constitucional no se muestra favorable a esta práctica de interpretación[90] extensiva penal ni la distingue

---

[88] Pérez Alonso, Esteban y Martín Morales, Ricardo, "Referéndums, consultas populares y delitos electorales. ¿Son aplicables los tipos delictivos de la Ley Orgánica del Régimen Electoral General a las consultas populares?", *Revista Electrónica de Ciencia Penal y Criminología*, 19-32, 2017.

[89] García Fernández, Javier, *Antología de la Revista de Derecho Público (1932-1936),* Madrid, Centro de Estudios Políticos y Constitucionales, 2016, p. 572.

[90] "Pese a que la jurisprudencia sigue refiriéndose a ellas conjuntamente afirmando que ambas están prohibidas, la interpretación extensiva contra reo y la analogía i*n malam partem* no deben confundirse: la primera, por ser interpretación, es perfectamente admisible, aunque sea contra reo si, respetando el tenor literal posible, es aconsejada

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

de la analogía; sin embargo, nuestra postura es de respeto al principio de legalidad. Siendo conscientes de la clara proximidad entre ambas instituciones, pero siendo ambas diferentes, en lo ya expresado, lo que tratamos de defender es la interpretación del concepto de elección hasta el referéndum, interpretación extensiva, en tanto que el referéndum es una especificidad de ese proceso electoral; de ahí la remisión del artículo 11 mencionado, que respetaría el principio de legalidad penal, y se cubriría el vacío de punibilidad que se presume existente. En suma, podríamos incluso atender a una interpretación analógica en la remisión de la LO de las distintas modalidades de referéndum a la LOREG, donde se contemplan los delitos electorales que se pueden cometer en el desarrollo del proceso electoral y, por tanto, refrendario.

Si bien esta confrontación doctrinal hace necesario adaptar ese cuadrado normativo —Ley Orgánica reguladora de las distintas modalidades de referéndum, Ley Orgánica Régimen Electoral General, Código Penal—, en aras a responder a las realidades de las tecnologías de la información y de la comunicación, pues ello supondría no dejar margen de interpretación, sino al contrario, la creación de una seguridad jurídica necesaria en el ámbito penal. Es así que nuestra intención es llamar la atención del legislador en este aspecto a fin de prevenir estas posibilidades en un futuro no tan lejano.

---

por una interpretación teleológica del precepto, esto es, atenta al espíritu y finalidad de éste. Tampoco son infrecuentes las posiciones doctrinales contrarias a la interpretación extensiva contra reo, advirtiéndose en ellas una confusión con la analogía. No obstante su licitud, interpretar de forma extensiva contra reo será la excepción: procederá cuando el fin de protección de la norma lo aconseje, pero no debe olvidarse que el derecho penal en su conjunto está informado por el principio de mínima intervención, que apunta precisamente en sentido contrario. Tanto la analogía como la interpretación son actos o actividades de creación del derecho. No sólo, por tanto, la primera, que implica, eso sí, la creación judicial de una norma: la analogía implica por parte del juez, la asunción de competencias legislativas, asunción lícita por delegación legal en el caso del artículo 4.1 del Código Civil pero expresamente prohibida, como hemos visto, por el artículo 4.1 del Código Penal. La interpretación, pese al modelo ideal propio de la Ilustración, no es, nunca fue, un simple silogismo, sino que encierra, siempre, una actividad creativa: a través de ella el juez concluye el programa normativo al que da inicio el legislador. Dado que en un caso el juez crea una norma y en el otro acaba una norma o atribuye significado a la norma creada por el legislador (o Poder Ejecutivo si son normas de rango inferior), ambas actividades son teóricamente diferenciables", Ramón Ribas, Eduardo, "Interpretación extensiva y analogía en el derecho penal", *Revista de Derecho Penal y Criminología*, tercera época, núm. 12, julio de 2014, pp. 111-164.

DOI: http://dx.doi.org/10.22201/iij.24487910e.2019.15-16.15902

II. Reflexión

La realidad de la instauración de tecnologías de la información y de la comunicación en un proceso electoral general y/o refrendario constitucional en España parece encontrar dificultades normativas y técnicas.

Advirtiendo la importancia e influencia de estas tecnologías en los procedimientos electorales tal y como se conforman en la actualidad, a través de técnicas indirectas, de injerencias, e incluso mediante el impulso institucional de las mesas electorales administradas electrónicamente, hemos de repensar los principios constitucionales que son subvertidos.

Asimismo, la necesidad de clarificar el sistema que se pretendería instaurar condicionaría la reforma del propio marco normativo y la práctica derivada del mismo.

Parece, por tanto, lejana la instauración de formas presenciales o remotas de votación electrónica en el ámbito español. Quizá el interés europeo en este tipo de sistemas, para crear la identidad europea y acercar el Parlamento Europeo a sus ciudadanos, derive en posibilidad más plausible de su instauración por los Estados miembros. Si bien es cierto, aquellos que habían implementado tales tecnologías de la información y de la comunicación se encuentran en una fase de revisión y/o de retirada en virtud de la garantía de la seguridad, ciberseguridad, de los procesos electorales y/o refrendarios.

En todo caso, "confianza y seguridad" encierran las claves del futuro del referéndum o de las elecciones generales por medio de tecnologías de la información y la comunicación. La "confianza" generada en la ciudadanía, por un lado, y en las instituciones electorales, por otro, supone uno de los dos pilares del sistema; por ello, será preciso la inversión en educación, a fin de mejorar la comprensión y capacitación de los agentes implicados. Por otro lado, la segunda de las columnas vertebradoras, la "seguridad", que podemos extender a la ciberseguridad, garantizada en todos los niveles del proceso refrendario —*ex-ante* a través de la prevención; durante, la defensa y *ex-post*, análisis y responsabilidad— a fin de conseguir un apoyo en la instauración de las tecnologías en procesos refrendarios, electorales y participativos y, subsecuentemente, en lograr los cambios necesarios en el marco normativo de referencia.