ARTÍCULO

ISSN 1994-5272

La verificabilidad exhaustiva (*end-to-end*) del voto por Internet: una buena solución con algunas dudas legales

Jordi Barrat I Esteve
evol2 / eVoting Legal Lab
http://evol2.wordpress.com
<jordi.barrat@urv.cat>
España

[Resumen] En este artículo se analiza la eficacia de las verificaciones electorales en el sistema tradicional de sufragio en papel y, a partir de ello, se aplica la misma metodología de análisis al voto por Internet poniendo de relieve ciertos retos jurídicos no resueltos. Se examina el sistema de verificación exhaustiva en la emisión del sufragio por Internet aplicado en Noruega y se exponen algunas dudas sobre la aplicación por terceros de los sistemas de verificación, las posibles discrepancias entre dos o más verificaciones y la necesidad de un marco legal sobre la implementación de la verificación exhaustiva.

Palabras clave: Sistema de verificación exhaustiva, voto por Internet, Noruega.

[Title] End-to-end of Internet voting: a good solution with some legal questions

[Abstract] This paper analyzes the effectiveness of electoral verification on the traditional system of paper ballot. From this, it applies the same methodology to analyze the Internet voting and it examines the electoral exhaustive verification system (end-to-end) applied in Norway. Finally, it discusses some open doubts about the actual implementation of exhaustive verification systems by third parties, how to deal with discrepancies between two or more verifications, and the need for a sound legal framework on the implementation of an end-to-end system.

[Keywords]: End-to-end system, Internet voting, Norway.

Barrat I Esteve, Jordi. « La verificabilidad exhaustiva (*end-to-end*) del voto por Internet: una buena solución con algunas dudas legales». En: Elecciones, 2013, enero-diciembre, v. 12, N.° 13, pp. 199-217.

[Recibido] 25/10/13 & [Aceptado] 11/11/13

1. La verificabilidad exhaustiva: palabras mágicas para cualquier proceso electoral

El secreto e integridad del voto, su carácter universal y la libertad del elector son, entre otros, principios básicos del sufragio que cualquier proceso electoral democrático debe cumplir, pero también hay otros elementos procedimentales no por ello menos importantes. En particular, este artículo parte de la necesidad de transparencia y verificabilidad. Las elecciones deben ser directamente controlables por todos los ciudadanos, es decir, el proceso debe ser plenamente verificable, o auditable, y no deben requerirse conocimientos específicos para poder llevar a cabo dichas tareas. Por otra parte, la supervisión debe desarrollase de forma independiente, es decir, no depender de otros grupos de interés o de los datos proporcionados por terceras partes.

La verificabilidad exhaustiva (o *end-to-end* / E2E) consiste precisamente en eso y no se trata de un rasgo únicamente predicable de los novedosos sistemas electorales con componentes informáticos (cfr. Gharadaghy, 2010). Es (o debería ser) un rasgo inherente a cualquier elección con independencia de los mecanismos utilizados para emitir el voto o proceder al escrutinio. Se ofrece a continuación un análisis preliminar de la eficacia de las verificaciones electorales en el caso de sufragio en papel, sea presencial o remoto, y tal aproximación nos permitirá después aplicar esta misma metodología al voto por Internet. El texto no aborda el caso de las urnas electrónicas, es decir, el voto electrónico presencial y no remoto, ya que la verificabilidad de estos supuestos puede solventarse mediante terceras vías (cfr. la propuesta soba en Benaloh, 2011).

La verificabilidad exhaustiva abarca al menos dos tipos de variables: una individual y otra universal. La primera permite a cada elector comprobar que su voto ha sido correctamente procesado desde el principio hasta el final del procedimiento electoral, es decir, cada papeleta debe ser emitida de acuerdo con la intención real del elector (*cast as intended*), debe ser almacenada y gestionada tal y como ha sido emitida (*stored as cast*) y finalmente también debe ser contabilizada tal y como fue emitida (*tallied as cast*). Por otro lado, una verificación universal permite que cada votante, a través seguramente de una coalición de electores, pueda comprobar la exactitud de los resultados globales, es decir, el sistema proporciona suficientes pruebas objetivas para demostrar que cada boleta ha sido almacenada, gestionada y contabilizada tal y como fue

emitida. También debe permitir garantizar que no se han añadido boletas suplementarias, que nadie ha podido quebrar el secreto del sufragio y que, en términos generales, se han respetado los principios básicos de cualquier elección democrática. La verificación universal no incluye la primera etapa, es decir, la garantía de que el sufragio se ha emitido de acuerdo con la verdadera intención del elector, porque tal paso solo puede ser comprobado por cada uno de los votantes y no de modo universal.

El sistema tradicional en papel cumple con ambos requisitos y vale la pena explicar cómo se logra ya que, al abordar las cuestiones de voto electrónico, algunas propuestas parten de malentendidos significativos sobre lo que normalmente sucede dentro de un centro de votación tradicional. La ausencia de metodologías homologadas en el ámbito internacional contribuye también a esta confusión potencial.

Una vez asumido que cualquier ciudadano tiene derecho a presentarse a un colegio electoral determinado y, salvo casos de orden, violencia o intimidación, permanecer allí durante el desarrollo de las diversas etapas de los procedimientos electorales,[1] cualquier elector sería capaz de verificar que las urnas no contienen ninguna boleta al comienzo de la votación, que están selladas, que el sello no se ha violado, a no ser en los casos previstos expresamente por la ley, que tanto su voto como todas las otras boletas se han insertado correctamente en la urna y no han sido eliminadas, que nadie insertó papeletas complementarias en la urna y, finalmente, que todas se tabulan adecuadamente al final de la jornada. En definitiva, la combinación de unos pocos dispositivos muy sencillos y tradicionales (urna, papeleta y sellos) proporciona un marco sólido para llevar a cabo la verificabilidad tanto individual como universal.

Sea como sea, una correcta interpretación de lo que ocurre tradicionalmente en los centros de votación requiere algunos matices suplementarios, sobre todo para garantizar su correcta traslación a la verificabilidad en los supuestos de voto por Internet. En primer lugar, no puede obviarse que la verificación indivi-

[1] Nótese que algunos países (ej.: Austria, cfr. Volkamer, 2012) no admiten que el elector permanezca en el centro de votación tras emitir su sufragio y, en estos casos, no habría una verificabilidad individual completa y directa. Así pues, la legislación de cada país puede reducir e incluso anular lo señalado sobre la verificabilidad individual, pero, desde una perspectiva teórica, la votación tradicional en papel permite potencialmente garantizar la verificación individual.

dual se lleva a cabo gracias a una deducción lógica, directa y personal (i). Una vez que un votante inserta su papeleta en la urna, ya no será capaz de identificar cuál de las boletas del interior es la que ha sido anteriormente utilizada por él mismo, pero, en cambio, sí se puede garantizar que ningún voto es posteriormente sustraído mediante la presencia continuada del elector en el centro de votación, parece obvio que la boleta en cuestión será incluida en el recuento final, aunque nadie, ni tan solo el propio votante afectado, podrá vincular una concreta papeleta con un votante determinado. El secreto del voto prohíbe la trazabilidad del sufragio, pero ello no impide que se logre la verificabilidad individual.

Tal verificabilidad solo puede llevarse a cabo a partir de estas deducciones, pero se trata en todo caso de deducciones lógicas, directas y basadas en la comprobación personal de hechos vividos y no históricos. No son suposiciones y tal distinción será crucial para comprender los desafíos que plantea el voto por Internet. Como se expondrá más adelante, el voto por Internet solo puede calificarse de verificable cuando los votantes asumen que lo realizado por terceros, como por ejemplo expertos en informática, merece suficiente confianza. No se trata, por lo tanto, de una deducción lograda por los propios votantes, como la analizada en las elecciones en papel, sino de una confianza delegada en terceros. En definitiva, es una suposición y no una deducción.

En segundo lugar, las verificaciones universales (ii) no pueden ser llevadas a cabo por una sola persona. Habida cuenta que las elecciones tradicionales en papel se sustentan en una estructura descentralizada, que también funge como medida de seguridad contra la manipulación, un ciudadano solo puede verificar totalmente un único colegio electoral. Sin embargo, una coalición de votantes, a través de una eventual alianza de observadores nacionales, podría cubrir todas las mesas electorales y entonces la verificabilidad exhaustiva sería factible mediante la agregación de los resultados de cada una de las mesas. La alianza podría proporcionar, por ejemplo, sus propios resultados y tales datos podrían ser contrastados con los ofrecidos por la administración electoral.

Si nos referimos de nuevo a la diferencia entre deducciones y suposiciones, vale la pena señalar que las mencionadas coaliciones de votantes se basan en suposiciones indirectas ya que cada participante tendría que confiar en los demás. No habría, por lo tanto, una deducción directa y personal.

En tercer lugar, el porcentaje de uso real (iii) de las verificaciones exhaustivas dentro de un marco electoral tradicional no debe cuestionar su utilidad. Incluso en casos de empleo residual, lo cual es una característica común en las democracias occidentales, no hay razón alguna para no mantener ambos tipos de verificaciones electorales. Siempre debe existir la posibilidad teórica de llevarlas a cabo y, ante ciertos escenarios, como elecciones con resultados ajustados y/o con problemas políticos, la ciudadanía puede aprovechar la utilidad de tales facultades y comprobar por sí misma la corrección del proceso electoral. Lo que parece lejano desde una perspectiva occidental, se hace imprescindible en otros marcos en que las autoridades electorales deben enfrentar problemas de credibilidad. Y, si escenarios similares se produjeran en democracias maduras, hipótesis que nunca debe descartarse, siempre podría reactivarse la capacidad de verificar individual y universalmente las elecciones, ya que el sistema habría seguido ofreciendo esta opción.

El voto por correo (iv) no cumple con estos criterios ya que no admite ni una verificación individual ni una universal, al menos si la entendemos de forma completa y exhaustiva, pero se trata de un canal de votación admitido en algunos países y validado por organismos internacionales (cfr., sobre la Comisión de Venecia, Sánchez Navarro 2009).

El voto por correo constituye un ejemplo de voto a distancia en el que siempre hay una etapa excluida de la supervisión del votante, concretamente la fase en la que una boleta se transfiere a la mesa electoral correspondiente. Habida cuenta que el elector no contará con una supervisión directa, personal y completa de su boleta durante todo el proceso, la verificabilidad individual deviene inviable, al menos si debe abarcar la segunda y tercera etapas del proceso, es decir, la comprobación de que el sufragio se almacena/gestiona tal y como fue emitido y que también es contabilizado de la misma forma. La primera verificación, es decir, la que garantiza que la boleta se emite de acuerdo con la intención del elector, sigue siendo posible con medios postales.

En cuanto a la verificabilidad universal, el voto por correo necesita también un enfoque diferente. A pesar de que no puede proporcionar una verificación exhaustiva, ya que la transferencia de la boleta hacia cada centro de votación será siempre una etapa débil, la verificabilidad universal resulta todavía factible si se inicia cuando el voto por correo es recibido por el colegio electoral. Una vez que

la papeleta se procesa ya en el entorno supervisado de un centro de votación, no hay diferencia entre la gestión de los votos emitidos por medios postales y la del resto. Todos ellos serán sometidos a los mismos procedimientos que, como se explicó anteriormente, son susceptibles de una verificación universal.

La correcta comprensión de cómo funcionan las verificaciones mencionadas con el voto por correo resulta crucial para abordar adecuadamente los retos inherentes al voto por Internet ya que también constituye un sistema de votación a distancia. Legítimamente podría afirmarse que lo admitido en un marco basado en papel, como el del sufragio postal sin verificabilidad individual ni exhaustiva completas, también debe ser aceptado dentro de un entorno virtual. Dado que los problemas son los mismos, sería injusto exigir una verificabilidad exhaustiva solo para este tipo de canal electrónico de votación a distancia y no para los demás. Si se admite este razonamiento, basado en un enfoque comparativo entre dos modalidades de emisión del sufragio, el voto por Internet debería incluir al menos la misma verificabilidad universal parcial que ya existe en el voto por correo, es decir, al menos desde el momento en que la boleta virtual es recibida por el servidor. Además, algunas soluciones de voto por Internet tratan de mejorar dichos esquemas ensayando distintas formas de verificación individual como, por ejemplo, los códigos de retorno utilizados en Noruega.

Por último, pero no menos importante, las verificaciones tradicionales pueden llevarse a cabo sin conocimientos técnicos específicos (v), incluso por personas analfabetas. Como ha recordado el Tribunal Constitucional alemán, las urnas electrónicas y, de forma análoga, también el voto por Internet, solo pueden ser aceptadas si cualquier elector, de forma personal e independiente, puede llevar a cabo una supervisión significativa de los procedimientos electorales (cfr. BVerfGE 2 BvC 3/07, 3 de marzo de 2009). Esta característica es particularmente importante cuando se necesita una alianza de observadores ya que, aun basándose en cierto tipo de confianza mutua, los socios pueden seleccionarse de forma tradicional, teniendo en cuenta su disponibilidad, su lugar de residencia u otros factores similares. La red no se limitará a un grupo de personas ya preseleccionados gracias a su experiencia técnica.

2. El caso noruego: un ejemplo avanzado de verificabilidad exhaustiva (E2E)[2]

En septiembre de 2011, Noruega comenzó a utilizar el voto por Internet aprovechando la convocatoria de las elecciones municipales y comarcales. Se trató de una iniciativa piloto que solo abarcó diez municipios, pero el gobierno ha mantenido y mejorado el proyecto repitiendo la experiencia en las recientes elecciones generales de septiembre de 2013. En comparación con otras soluciones de voto por Internet, como las de Estonia, Suiza o Francia, el sistema noruego incluye cambios importantes a nuestros efectos como, por ejemplo, los llamados códigos de retorno (i) o generosas licencias de *software* que permiten llevar a cabo inspecciones por terceros (ii). Se trata seguramente del único caso en el que se ha pretendido ofrecer una verificación E2E de un sistema de voto por Internet.

Antes de las elecciones cada votante recibe una tarjeta electoral (i) en donde hallará una lista de los candidatos y un código aleatorio relacionado con cada uno de ellos. El código de un determinado candidato también será diferente para cada elector. Cuando el ciudadano emite su voto, el sistema le envía un mensaje de texto que reconoce la correcta recepción del sufragio en el *Vote Collector Server* (VCS) e incluye la selección realizada por el elector en un formato codificado. El elector puede verificar si dicho código es el ya impreso en su tarjeta de votación para el candidato que él mismo había elegido previamente. Por otra parte, el mensaje de texto se envía a un número de teléfono celular previamente proporcionado por el ciudadano, es decir, el votante emite su sufragio mediante un dispositivo, pero recibe el mensaje a través de otro canal.

Dado que los códigos de retorno incluyen el contenido del sufragio, es decir, la opción ideológica del elector, emerge una lógica preocupación sobre el secreto del voto y la libertad del ciudadano, pero, sin negar la trascendencia de este debate, lo cierto es que, a nuestros efectos, estos códigos son un buen sistema de verificación individual parcial. Los ciudadanos cuentan con pruebas sólidas de que sus votos han sido emitidos de acuerdo con sus intenciones y almacenados tal como han sido emitidos, pero no existen pruebas vinculadas al resto de fases, es decir, los procedimientos posteriores de gestión y el escrutinio.

[2] Las consideraciones de este artículo abarcan únicamente la experiencia llevada a cabo por Noruega en septiembre de 2011.

Por lo tanto, los códigos de retorno solo garantizan una verificación individual limitada a las dos primeras etapas, pero, si se compara con el voto por correo, la solución noruega mejora el nivel de verificabilidad porque abarca tanto la fase inicial, también cubierta en el caso postal, como parcialmente la posterior, es decir, la recepción del sufragio para su custodia hasta el recuento, etapa que no está incluida en las verificaciones permitidas por el voto por correo.

Con respecto a las verificaciones universales, las licencias de *software* (ii) teóricamente deben admitir supervisiones del proceso globales[3] y de carácter independiente, es decir, ajenas al control de la autoridad electoral o de las empresas contratadas para la gestión. Sin perjuicio de los supuestos técnicos necesarios para aceptar la viabilidad de dicha verificación (cfr. Spycher, 2011), existen por lo menos dos etapas problemáticas relativas a la generación inicial de los códigos de retorno (a) y las etapas finales (b), es decir, la descarga de la base de datos con los sufragios, su filtrado, mezcla y escrutinio.

Habida cuenta que los códigos de retorno (a) vinculan el contenido de una boleta con un ciudadano determinado, su admisión implica un gran riesgo para el secreto del voto. Además de su uso para una eventual coacción una vez recibidos por el ciudadano tras la votación (cfr. Barrat 2012), hay otro peligro que consiste en la vinculación ilegal de datos por parte de los diferentes servidores que participan en este proceso. Si el sistema es capaz de remitir un código determinado a cada elector con su opción política, parece lógico presuponer que ese sistema ha sido capaz de desvelar el contenido de un sufragio determinado y vincularlo con un ciudadano en concreto. Este fraude permitiría, por lo tanto, revelar el contenido del voto a terceros incluso si el votante no muestra el recibo a nadie y la única manera de resolverlo consiste en combinar ingeniería criptográfica con procedimientos de gestión selectivos que incluyan, por ejemplo, una rigurosa separación de funciones, pero todo ello no puede ser supervisado ya mediante las mencionadas licencias de *software*, es decir, queda fuera de los límites de una verificabilidad exhaustiva basada únicamente en medios informáticos/matemáticos (cfr. para otros casos similares, Jones, 2009).

[3] Calificar los comicios noruegos de verificables de forma exhaustiva no es de hecho un planteamiento pacífico (véase, por ejemplo, el debate entre Josh Benaloh y Jordi Puiggalí derivado de la presentación, en un seminario nist, de Benaloh, 2013).

Algo similar ocurre durante las últimas etapas del procedimiento de votación (b). Los votos deben ser descargados desde el VCS en tres equipos aislados que llevarán a cabo el filtrado (*cleansing*), la mezcla (*mixing*) y, por último, el escrutinio. Por lo tanto, los datos serán transferidos desde un dispositivo a otro, incluso desde el VCS a las computadoras que han permanecido aisladas, y nuevamente el rigor de cada una de estas transferencias se basa tanto en el uso adecuado de herramientas informáticas como en medidas de gestión apropiadas. Es cierto que, en este caso, pueden idearse mecanismos técnicos que garanticen la inviolabilidad de las bases de datos (*zero-knowledge proofs*), pero se trata de estrategias que van más allá de la mera autorización contemplada en las licencias de uso. Se trata más bien de medidas de gestión que, utilizando soluciones informáticas, permiten una verificación independiente.

Como conclusión, el sistema noruego puede proporcionar herramientas de verificación exhaustiva siempre que se asuma que los medios informáticos/matemáticos deben complementarse con medidas tradicionales de control.

Una vez expuesto un supuesto particularmente avanzado de sistema de votación con verificabilidad exhaustiva, es hora de retomar un enfoque estrictamente jurídico. Aunque las herramientas de verificación exhaustiva pretenden resolver uno de los problemas inherentes a cualquier sistema de votación por Internet, consistente en el mantenimiento del derecho del votante a inspeccionar y verificar el sistema en su conjunto, surgen algunas dudas jurídicas en relación con su aplicación práctica (véase Buchmann, 2009).

3. Algunas dudas legales sobre los sistemas de verificación exhaustiva (*end-to-end*)

Esta sección abordará tres cuestiones que a menudo permanecen sin resolver, incluso cuando una plataforma de voto por Internet incluye una buena herramienta de verificación exhaustiva. En primer lugar, resulta obvio que estos procedimientos asumen que los votantes deben delegar su poder de verificación a un grupo de expertos en informática. En segundo lugar, si atendemos a la práctica electoral real, cabe preguntarse qué pasaría si nadie asume la tarea de llevar a cabo la mencionada verificación exhaustiva y, si por suerte hay varios expertos independientes finalmente implicados en ella, también cabe preguntarse qué sucedería si cada uno llega a conclusiones diferentes. Finalmente, la normativa no suele incluir ciertos detalles necesarios en estos casos.

3.1 La verificación exhaustiva por terceros

Cualquier sistema de verificación exhaustiva implica confiar en terceras partes y, por lo tanto, los ciudadanos asumen una pérdida de poder en el ámbito electoral. Confiar en expertos, cuyas conclusiones se basan en lógicas matemáticas, es de alguna manera diferente a depositar nuestra esperanza en el quehacer de organismos electorales u otros actores interesados, pero la realidad no debe ocultarse ya que la delegación de facultades sigue existiendo y es en sí misma negativa, sea cual sea el delegatario. Desde el punto de vista de un ciudadano medio sin conocimientos específicos ni experiencia en criptografía, es decir, en realidad la práctica totalidad de la ciudadanía, cualquier verificación exhaustiva significa que tal ciudadano no será capaz de inspeccionar los procedimientos electorales por sí mismo y que se verá obligado a confiar en las conclusiones proporcionadas por terceros.

Teniendo en cuenta las ventajas de estos nuevos canales de votación, así como otros factores sociales e institucionales, como la conciencia cívica global o la credibilidad de los administradores electorales, podría llegar a aceptarse esta nueva situación como un compromiso razonable, pero es preciso analizar también un escenario peor en el que voto por Internet solo sería aceptado si mantiene al menos las mismas garantías que ya existen en las formas tradicionales de emisión del sufragio.

Como ya se ha visto, estos canales de votación basados en papel pueden también incluir algún tipo de delegación de competencias e incluso una pérdida completa de supervisión directa. El voto por correo, por ejemplo, solo puede aceptarse asumiendo que ni la supervisión individual ni la universal serán capaces de cubrir al menos una de las etapas críticas del proceso, el traslado de las papeletas hacia un entorno supervisado. De hecho el voto por correo reduce el ámbito de la verificación individual únicamente a la primera fase de votación, es decir, aquélla en la que se garantiza que el voto emitido coincide con la verdadera voluntad del elector (*cast as intended*). Por otra parte, la verificación universal siempre se basa en una iniciativa colectiva que implica algún tipo de confianza mutua y reparto de poder.

Teniendo en cuenta todas estas características, cabe preguntarse si, en el caso del voto por Internet, la verificación exhaustiva ofrece idéntico nivel de

garantías y la respuesta es en cierto modo paradójica. Si centramos nuestra atención en la verificación individual, algunas soluciones de verificación exhaustiva, como los códigos de retorno de Noruega, permiten incluso mejorar el sistema actual en papel, ya que consiguen implantar nuevas medidas de supervisión y así ensanchar el ámbito susceptible de ser controlado directamente por un elector. Si el voto por correo solo permitía una supervisión individual limitada a la hora de emitir el sufragio, los códigos de retorno generan pruebas suficiente de que las boletas han sido al menos recibidas por el servidor tal cual fueron emitidas. La verificación individual desborda pues el mero *cast as intended* y alcanza al menos el *stored as cast*, aunque ya no ofrece garantías de que la gestión posterior al almacenamiento inicial preserve la integridad de la boleta.

En cuanto a la verificación universal, mientras que los sistemas tradicionales necesitan una delegación de poder a través de un enfoque colectivo, los métodos exhaustivos pueden lograr el mismo objetivo con un equipo muy reducido de expertos, incluso con un solo verificador independiente. Sin embargo, el sistema no será verificable por los ciudadanos comunes y por lo tanto ya no proporciona el mismo nivel de garantías que existe en la actualidad. Los ciudadanos perderían poder, pero el razonamiento no debe necesariamente detenerse ante tal constatación negativa. La conclusión final puede ser diferente.

Si el voto por correo se admite asumiendo que no puede proporcionar una verificabilidad completa tanto individual como universal, el voto por Internet también podría aceptarse si logramos un equilibrio justo entre una nueva forma de supervisión indirecta y las ventajas derivadas del uso de estas novedosas herramientas informáticas. En este sentido, resulta importante retener que la mencionada supervisión indirecta se sustentaría sobre un discurso procedimental, es decir, una vez asumida la idea de que la verificación debe ser delegada a un grupo reducido de expertos, el sistema en su conjunto será suficientemente fiable para un ciudadano medio si el reglamento establece claramente la forma de llevar a cabo las verificaciones exhaustivas. Si somos capaces de convencer a la ciudadanía de que estructuralmente el sistema es susceptible de ser supervisado por cualquier persona, pese a que en la práctica solamente serán expertos informáticos, que el sistema por completo puede ser sometido a este control y que tal tarea no está vinculada a un tipo de *software* en concreto, el ciudadano medio contaría con suficientes pruebas indirectas del desempeño

correcto del sistema siempre y cuando ningún experto en informática encuentre y divulgue alguna vulnerabilidad

Pero, si la única manera de aceptar la confianza indirecta consiste en centrar nuestra atención en el cumplimiento estricto de los meros procedimientos (cfr. Barrat, 2011), cabe preguntarse las consecuencias de no utilizarlos según lo inicialmente previsto: ¿qué pasará, por ejemplo, si ningún experto independiente muestra su interés por llevar a cabo una verificación exhaustiva? ¿Qué pasará si diversas verificaciones exhaustivas alcanzan conclusiones divergentes? Y, finalmente, ¿cómo debemos actuar ante el habitual vacío normativo en este tipo de aspectos?

3.2 ¿Qué sucede si nadie lleva a cabo una verificación exhaustiva?

No hay respuestas fáciles porque no se puede asumir que la pasividad de los técnicos implique que los ciudadanos estén de acuerdo con la labor de la administración electoral. Puede haber muchas razones para no asumir la tarea de verificación exhaustiva de un proceso como, por ejemplo, motivos económicos, limitaciones temporales, ausencia del equipo apropiado de expertos o simplemente una priorización alternativa de los compromisos. Todos ellos son argumentos razonables, pero no suficientes para colmar el vacío generado por la inexistencia de una verificación exhaustiva independiente. Como se advierte en escenarios análogos,

> [...] having an audit trail does not guarantee that anyone will dig through it to see whether there is a problem or to correct the outcome if the outcome is wrong. Strong software independence does not correct anything, but it is an essential ingredient for a system to be self-correcting (Benaloh 2011: 2).

Los ciudadanos comunes, que de hecho ya habían delegado su poder originario de supervisión electoral (véase supra), afrontan ahora un nuevo escenario con problemas redoblados ya que se les pide que crean que no hacer nada, es decir, no llevar cabo ninguna verificación exhaustiva significa que el sistema electoral es suficientemente fiable. Se trata a todas luces de un exceso. El frágil equilibrio alcanzado entre las ventajas de las soluciones de voto por Internet y las nuevas formas de supervisión ciudadana quiebra con facilidad si, más allá de lo teóricamente factible, la praxis muestra que no hay supervisión indepen-

diente en absoluto. El sistema podría aceptarse si el contexto electoral ofrece otros elementos colaterales de confiabilidad, pero lo cierto es que el sistema de voto por Internet en sí mismo habría fracasado en su intento de ofrecer garantías solventes y objetivas de fiabilidad. Por otro lado, el hecho de que, desde un plano teórico, tales verificaciones exhaustivas puedan realizarse de forma indefinida, aspecto inherente a esta metodología por el tipo de pruebas que proporciona, no soluciona el problema planteado ya que el procedimiento electoral se guía por unos marcos temporales estrictos y limitados durante los que deben ofrecerse ya conclusiones definitivas.

Ante la ausencia de expertos independientes, todo el proceso descansaría únicamente en la correcta ejecución de los correspondientes organismos electorales, lo cual es difícil de aceptar desde el punto de vista democrático, porque la desconfianza mutua es de alguna manera el punto de partida de cualquier ordenamiento electoral. Por otra parte, la comparación con el voto por correo ya no es válida. Obviamente siempre puede argumentarse que la transmisión de los votos postales también se apoya únicamente en la probidad de los organismos electorales, pero tal analogía tiene algún punto de fuga. El voto por Internet necesita la mencionada probidad de los servidores públicos electorales, pero también debe poder demostrar que el sistema funciona. Se trata de dos aspectos diferentes y lo segundo solo puede lograrse bien a través de expertos independientes, bien teniendo fe ciega en el desempeño de los organismos electorales.

La experiencia noruega en 2011 nos muestra además que este razonamiento es algo más que una mera hipótesis teórica. Este país se vio obligado a hacer frente precisamente a esta situación ante la ausencia de expertos independientes interesados en realizar una verificación exhaustiva y, finalmente, el gobierno optó por contratar a determinados grupos de expertos para llevar a cabo una verificación como mínimo parcial. Se trataba seguramente de la mejor solución en esas circunstancias, pero cabe preguntarse en qué medida ese control es realmente independiente ya que el gobierno remunera a los expertos por su labor o por lo menos les invita de forma nominativa. Las verificaciones exhaustivas no fueron pensadas para ser implementadas de esta manera y, por lo tanto, corren el riesgo de perder toda su utilidad ya que pueden no generar suficiente credibilidad ciudadana.

3.3. ¿Qué sucede si hay discrepancias entre dos o más verificadores?

En primer lugar, debe asumirse que las discrepancias pueden afectar tanto a los resultados como a la propia metodología, es decir, incluyen una cuestión previa sobre si el sistema realmente se sustenta en una verificación exhaustiva o, por el contrario, no cumple con los requisitos establecidos teóricamente para este tipo de supervisiones. Así pues, podría haber al menos los dos siguientes tipos de discrepancias:

- Con independencia de lo afirmado por la administración electoral e incluso por los propios expertos, alguien puede entender que el sistema de control no constituye una verificación exhaustiva porque algunas características o elementos quedan excluidos de la supervisión.

- Una vez practicada una verificación exhaustiva y, comparando sus resultados con los alcanzados por otros análisis similares, se constata que las conclusiones no son unívocas.

Una vez más, no hay respuestas fáciles. Obviamente, en un ágora académica, tales discrepancias desembocarían en un sugerente debate público, probablemente prolongado, en pos de la auténtica verdad científica tras descubrir los defectos de cada propuesta, pero los procedimientos electorales no cuentan con plazos tan generosos. Las elecciones deben ofrecer en un período breve resultados correctos y precisos, con el objetivo de aumentar o, al menos, mantener el nivel actual de confianza de la administración electoral y del sistema político. En definitiva, no tenemos tiempo para descubrir quién está equivocado y una tercera opinión, aunque sea la emitida por forenses durante un litigio, tampoco resolverá el problema.

La supervisión de los sistemas tradicionales basados en papel también podría generar discrepancias, pero pueden ser resueltas directamente por el propio Tribunal porque no requieren otros conocimientos especializados que los jurídicos. Por ejemplo, las boletas no válidas suelen plantear fuertes discusiones, pero los jueces pueden evaluar por sí mismos el problema y adoptar la decisión pertinente. Otros problemas similares también pueden ser dirimidos directamente por los propios jueces. Sin embargo, si un tribunal debe resolver

una discrepancia sobre la verificación exhaustiva en una plataforma de voto por Internet, los jueces no contarán seguramente con suficiente experiencia y su opinión se basará en un tercer informe técnico, cuya solidez no va a poder ser evaluada con propiedad por los propios jueces en comparación con los anteriores informes discrepantes.

Se trataría de un informe forense cuya validez, desde el punto de vista legal, probablemente prima sobre otros textos particulares de cada experto, pero, desde una perspectiva científica, la documentación forense también puede contener errores. Se habría alcanzado, por lo tanto, una solución legal, pero la credibilidad de los sistemas de voto por Internet no puede ser abordada con un enfoque puramente legalista. Se trata de un desafío legal, pero también de un problema cívico que necesita una solución más amplia. La ley siempre puede ser útil, pero basarse únicamente en soluciones legales constituye un error, particularmente cuando la decisión final no tiene argumentos sustanciales de peso. Normalmente los jueces prefieren el informe forense únicamente porque es el forense, pero su contenido real puede no ser tomado en consideración debido al alto nivel de conocimientos técnicos necesarios.

De hecho los jueces afrontan problemas similares en otras áreas tecnológicas (por ejemplo, los litigios con aseguradoras) en las que deben decidir qué opinión técnica es la mejor y en principio el mismo esquema podría aplicarse a la votación por Internet, pero nótese que, en este caso, el debate técnico no es el punto de partida realmente importante. Habíamos alcanzado esta etapa tras aceptar que podíamos confiar en la objetividad de las matemáticas, es decir, que los ciudadanos podrían asumir sin problemas la pérdida de su facultad democrática de supervisión electoral, pero tal delegación de facultades solo es aceptada sobre la base de que las matemáticas iban a proporcionar una conclusión única, sólida, clara y sobre todo aceptada unánimemente por los expertos. Si no es el caso, si debemos acudir a los tribunales para dirimir las divergencias de los propios expertos, no estamos en realidad ante una simple disputa legal entre compañías de seguros, donde cada una aporta sus propios equipos de expertos, sino que debemos afrontar otro tipo de problema consistente en cómo reconstruir la confianza del ciudadano. Y no parece una buena estrategia confiar simplemente en una nueva opinión experta y forense. No se produce ningún salto cualitativo que solvente la falta de univocidad que la verificación

exhaustiva e independiente debía proporcionarnos En definitiva, las matemáticas habrían perdido su misterio y no serían útiles a nuestros efectos.

3.4. Los silencios legales

Tanto las herramientas de verificación exhaustiva como otros mecanismos de supervisión electoral, como los comprobantes en papel, las certificaciones o las auditorías postelectorales, suelen estar previstas en la correspondiente normativa vigente, pero a menudo estos documentos solo prevén su introducción y olvidan aclarar cómo solventar legalmente la presencia de conclusiones divergentes. Las regulaciones de los comprobantes constituye, por ejemplo, un caso emblemático ya que suelen requerir un recibo en papel para cada sufragio e incluso un control aleatorio posterior, pero paradójicamente no suelen determinar ninguna regla que indique qué dato prevalece en caso de discrepancias entre el escrutinio electrónico y el tradicional, es decir, el realizado en papel con los correspondientes testigos de voto.

Los mecanismos exhaustivos de verificación pueden hallar problemas similares. Los reglamentos suelen hacer hincapié en que el sistema electoral está abierto a una verificación exhaustiva, pero callan sobre las consecuencias legales (no técnicas) de tales actividades. Parecen estar asumiendo que la propia posibilidad de utilizar herramientas de verificación exhaustiva elimina cualquier problema, es decir, cualquier divergencia sustancial o metodológica, pero ya sabemos que tal presunción no es del todo cierta. La implantación de supervisiones exhaustivas necesita un esfuerzo suplementario desde la óptica legal con el fin de cubrir todos los escenarios problemáticos generados por su aplicación real.

En Noruega, por ejemplo, el reglamento preveía que «the system shall enable independent third parties to verify the integrity of the election by using cryptographic proofs» (art. 27.3 / *Regulations relating to trial electronic voting*),[4] pero no había ninguna otra indicación sobre cómo reaccionar legalmente si no hubiera terceras partes independientes dispuestas a realizar estas pruebas o si las verificaciones arrojaran conclusiones discrepantes. Obviamente las normas electorales generales siguen siendo válidas y las partes

[4] <www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/E-valgsforskriften_endelig_versj_230611_engelsk.pdf>

interesadas pueden presentar una demanda judicial, pero, teniendo en cuenta la especificidad de este ámbito, sería recomendable, y probablemente necesario, que la normativa sobre el voto electrónico también incluyera un tratamiento detallado de las consecuencias jurídicas derivadas de la verificabilidad exhaustiva.

Referencias bibliográficas

Barrat, Jordi, Michel Chevallier et al.

2012 «Internet Voting and Individual Verifiability: The Norwegian Return Codes», *Electronic Voting* 2012, Bregenz: e-Voting.cc

Barrat, Jordi

2011 *Observing E-enabled Elections: How to implement Regional Electoral Standards*, Estocolmo: idea, 2011. <www.idea.int/democracydialog/upload/Observing-e-enabled-elections-how-to-implement-regional-electoral-standards.pdf>

[Última consulta: 12 de octubre de 2013].

Benaloh, Josh

2013 «End-To-End Verifiable Election Technologies», *Symposium on the Future of Voting Systems*, Washington dc: nist.

<csrc.nist.gov/groups/st/voting2013/presentations/benaloh_fov2013.pdf> [Última consulta: 16 de abril de 2013].

Benaloh, Josh, Douglas Jones, Eric Lazarus & Mark Lindeman

2011 «soba: Secrecy-Preserving Observable Ballot-leved Audit», *evt/wote* 11, San Francisco: Usenix/Accurate.

<static.usenix.org/events/evtwote11/tech/final_files/Benaloh.pdf>

[Última consulta: 12 de octubre de 2013].

Buchmann, Johannes & Melanie Volkamer

2009 «Verifiability in Electronic Voting - Open Issues», *End-to-End Voting Systems Workshop*, Washington dc: nist

<csrc.nist.gov/groups/st/e2evoting/documents/papers/volkamer_nist_BuchmannVolkamer.pdf> [Última consulta: 12 de octubre de 2013].

Gharadaghy, Rojan & Melanie Volkamer

2010 «Verifiability In Electronic Voting - Explanations For Non Security Experts», *Electronic Voting* 2010, Bregenz: e-Voting.cc.

Jones, Douglas

2009 «Some Problems with End-to-End Voting», *End-to-End Voting Systems Workshop*, Washington dc: nist. <csrc.nist.gov/groups/st/e2evoting/documents/papers/Jones_E2E_Paper.pdf> [Última consulta: 16 de abril de 2013].

Sánchez Navarro, Angel

2009 «Venice Commission's Opinions and the Issue of Distance Voting: Are Common Standards Possible?», 5th *European Conference of Electoral Management Bodies*, Bruselas: Comisión de Venecia, pp. 47-59.
<www.venice.coe.int/webforms/documents/?pdf=CDL-EL%282009%29017-bil> [Última consulta: 12 de octubre de 2013]

Spycher, Oliver, Melanie Volkamer & Reto Koenig

2011 «Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting», *The Norwegian E-vote 2011 Conference*, Oslo: Ministry of Local Government amd Regional Development.

Volkamer, Melanie

2012 «Deducing technical requirements from legal regulations», SecVote2012, Daghstul Seminar. <secvote.*uni.lu/slides/mvolkamer-deducing-reqs.pdf*> [Última consulta: 16 de abril de 2013].

[Sobre el autor]

Jordi Barrat i Esteve

Español. Licenciado en Derecho por la Universidad de Navarra y PhD en Derecho Constitucional por la Universidad de León. Desde 2010, es profesor titular de la Universidad Rovira i Virgili. Asimismo ha sido profesor en la Universitat d'Alacant y de la Universitat Oberta de Cataluyna. Ha publicado resultados de sus investigaciones sobre voto electrónico en diversas revistas académicas en España y Alemania.