CNS 3/2010

Dictamen en relación con la consulta formulada sobre los sistemas de voto electrónico

Se solicita a la Agencia Catalana de Protección de Datos un dictamen sobre el voto electrónico, especialmente sobre la seguridad y el mantenimiento del secreto de voto, y sobre la viabilidad, las ventajas, los inconvenientes y las garantías, en particular respecto a la seguridad y el secreto, que podría implicar la incorporación del voto electrónico, el voto remoto por Internet y la urna electrónica.

Así pues, el presente dictamen se emite desde el punto de vista de la protección de los datos de carácter personal y no se extiende a todas las implicaciones que para la protección de datos puede tener la celebración de un proceso electoral, sino, simplemente, en relación con el voto electrónico en cualquiera de sus modalidades.

Analizada la consulta y visto el informe de la Asesoría Jurídica, se emite el siguiente dictamen:

I

(...)

II

Lo primero que debe abordarse en el presente dictamen es la aplicabilidad de la normativa de protección de datos, puesto que en función de cuál sea la normativa aplicable pueden resultar exigibles a partir de la legislación vigente determinadas garantías en cuanto al tratamiento de datos personales con ocasión de la incorporación de mecanismos de voto electrónico.

De acuerdo con el artículo 2.3.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), los ficheros regulados por la legislación electoral se rigen por su normativa específica y por lo que, en su caso, prevé expresamente la misma LOPD para esos ficheros.

Por tanto, la LOPD y su normativa de desarrollo sólo resultan de aplicación en aquellas previsiones expresamente contempladas en la propia LOPD. Y lo cierto es que en la LOPD la única referencia expresa a la materia electoral, salvo la ya mencionada contenida en el artículo 2.3.a), es una referencia colateral incluida en la disposición adicional segunda para habilitar que la Administración general del Estado y las Administraciones de las comunidades autónomas puedan solicitar al Instituto Nacional de Estadística una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en el padrón municipal de habitantes y en el censo electoral correspondientes a los territorios donde ejercen sus competencias.

Ahora bien, que no resulte de aplicación la LOPD ni su normativa de desarrollo no implica que no deba respetarse el derecho fundamental a la protección de datos. Por el contrario, encontramos previsiones tanto a nivel constitucional como a nivel estatutario, así como en la normativa electoral general, que requieren que una eventual ley que incorpore el sistema de voto electrónico prevea las garantías necesarias para la protección de dicho derecho. Por otro lado, a escala internacional encontramos también un tratado, el Convenio 108 para la Protección de las Personas en cuanto al Tratamiento Automatizado de Datos de Carácter Personal, suscrito en

Estrasburgo el 28 de enero de 1981 y ratificado por España el 30 de enero de 1994, que vincula igualmente al Estado español y, en consecuencia, también a la Generalitat de Catalunya con respecto al derecho a la protección de datos de carácter personal sin que se prevea ninguna exclusión o reserva en cuanto a la materia electoral.

A nivel constitucional, debe tenerse en cuenta el artículo 18.4 de la CE, el cual establece un mandato al legislador para que limite el uso de la informática para garantizar, entre otros, el derecho a la intimidad de las personas y el pleno ejercicio de sus derechos. En este sentido, es preciso recordar, sin embargo, que la jurisprudencia constitucional ha declarado que el derecho a la protección de datos constituye un derecho fundamental de carácter instrumental, es decir, se trata de un derecho que actúa como un instrumento para la plena efectividad de otros derechos fundamentales, como el derecho a la intimidad (art. 18), pero también otros como sería el caso del derecho de sufragio reconocido en el artículo 23.1 y concretado en el 152 de la CE en cuanto a las asambleas legislativas autonómicas.

Por otro lado, es preciso subrayar que, dada la naturaleza de los procesos electorales, nos encontramos ante información que el Convenio 108 (art. 6) –y también la LOPD (art. 7) a pesar de no ser aplicable en este caso– considera datos que requieren una protección especial, puesto que en la información tratada con ocasión del voto electrónico nos encontraremos no sólo los datos identificativos de las personas ciudadanas incluidas en el censo, sino también otra información más sensible como el hecho de haber ejercido el derecho de voto o no y, en especial, el sentido del voto. Así pues, nos encontramos claramente ante datos que revelan la opinión política de los ciudadanos y que, por tanto, requieren una especial protección.

En cualquier caso, mediante el derecho a la protección de datos se trata, tal como apunta el artículo 18.4 de la CE y como ha reconocido también el Tribunal Constitucional (STC 292/00), no sólo de la protección del derecho a la intimidad de las personas, en la medida en que puede considerarse que la opción política puede formar parte de la intimidad, sino también de la protección de otros derechos fundamentales, en especial el derecho de sufragio o el derecho a la no discriminación. Resulta obvio, en este sentido, que la inexistencia de garantías adecuadas que aseguren el secreto del voto puede actuar como mecanismo disuasorio que acabe afectando a la participación en el proceso electoral e indirectamente a su propia legitimidad, así como que pérdidas de información o tratamientos inadecuados de la información vinculada al proceso electoral pueden dar lugar a prácticas discriminatorias.

En Cataluña cabe destacar además que el Estatuto de Autonomía (EAC) ha incorporado por primera vez a nivel estatutario el derecho a la protección de datos en el artículo 31 respecto a los ficheros que son competencia de la Generalitat (art. 156 del EAC). Previsión que es preciso completar, por un lado, con la del artículo 37.1 del EAC, según el cual las disposiciones dictadas por los poderes públicos de Cataluña deben respetar los derechos reconocidos en los capítulos I, II y III del Título I del Estatuto y que deben interpretarse y aplicarse en el sentido más favorable a su plena efectividad; por otro lado, es preciso completarla con la previsión del artículo 56.1 del EAC, que exige que el sistema electoral en el Parlamento de Cataluña sea mediante sufragio universal, libre, igual, directo y secreto.

Siendo como es el caso que nos encontramos ante ficheros que deben ser considerados responsabilidad de la Administración electoral de Cataluña –ya sea adoptando la forma de la Sindicatura Electoral de Cataluña propuesta en el informe que se adjunta a la consulta, o con otra forma o denominación– resulta exigible la

protección de dicho derecho por parte de la futura ley que regule el voto electrónico en Cataluña.

Por otro lado, la propia legislación electoral general, aunque no prevé ningún sistema de votación electrónica (salvo la incorporación de los medios electrónicos para consultar el censo, cuestión a la que nos referiremos más adelante), contiene algunas previsiones aplicables a las elecciones a las asambleas legislativas de las comunidades autónomas en virtud de lo que establece la disposición adicional primera de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG), destinadas a la protección de los datos de carácter personal y, en especial, del carácter secreto del voto. En este sentido, resultan aplicables los principios de transparencia, objetividad e igualdad establecidos en el artículo 8, así como la prohibición de obligar o coaccionar a que se revele el sentido del voto (art. 5), la prohibición de que notarios presentes en los colegios electorales puedan dar fe de actos que se opongan al secreto de la votación (91.3) o el delito de descubrimiento del secreto de voto (146.1.c).

Por último, y para completar el marco legal aplicable, es preciso hacer referencia también a diferentes instrumentos de cariz internacional que reconocen el carácter secreto del derecho a voto, como la Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948, (art. 21.3) o el Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966, (art. 25.b).

También en el ámbito internacional es preciso referirse al Código de Buenas Prácticas en Materia Electoral de la Comisión Europea para la Democracia por el Derecho (Comisión de Venecia), en el seno del Consejo de Europa, como instrumento que recoge diferentes previsiones para asegurar el carácter igual, libre y secreto del derecho de sufragio.

Asimismo, debe tenerse en cuenta de forma específica, pese a no tener carácter vinculante, la Recomendación (2004) 11 del Consejo de Europa a los Estados miembros relativa a estándares legales, operacionales y técnicos para el voto electrónico (*e-voting*), adoptada por el Comité de Ministros de 30 de septiembre de 2004. De acuerdo con dicha recomendación, se definen los sistemas electrónicos de votación como toda elección o referéndum que implique el recurso a medios electrónicos al menos en el momento de registrar el sufragio, y se establecen determinados principios que deben tenerse en cuenta en la regulación legal en relación, entre otros, con el carácter secreto del sufragio, así como garantías procedimentales:

> A) Principios vinculados al carácter secreto del sufragio (principios del 16 al 19):
>
> - El voto electrónico se organizará de modo que pueda excluirse en cualquier fase del proceso de votación y, en particular, en la autenticación del elector, todo aquello que ponga en peligro el secreto del voto.
>
> - El sistema de voto electrónico debe garantizar que los votos introducidos en la urna y los votos contados son, y se mantienen, anónimos, y que no es posible reconstruir un vínculo entre el voto y el votante.
>
> - El sistema de voto electrónico debe estar diseñado de modo que el número de votos esperado en cada urna electrónica no permita relacionar el resultado con votantes individuales.

- Deben tomarse las medidas necesarias para asegurar que la información necesaria durante el proceso electrónico no puede ser utilizada para quebrantar el secreto de voto.

B) Garantías de transparencia (apartados del 20 al 23):

- Los estados miembros tomarán medidas para asegurar que los votantes entiendan y tengan confianza en el uso del sistema de voto electrónico.

- La información sobre el funcionamiento de un sistema de voto electrónico debe estar públicamente disponible.

- Los votantes deben tener la oportunidad de practicar cualquier nuevo método de voto electrónico antes, y separadamente, del momento de emitir un voto electrónico.

- Algunos observadores, con el alcance previsto por la ley, deben poder estar presentes para observar y hacer comentarios acerca de las elecciones con voto electrónico, incluyendo la obtención de los resultados.

C) Garantías de verificabilidad y responsabilidad del sistema (principios del 24 al 27):

- Los componentes del sistema de voto electrónico se revelarán como mínimo a las autoridades electorales competentes, con el fin de comprobación y certificación.

- Antes de que se introduzca cualquier sistema de voto electrónico, y a intervalos apropiados posteriormente, y en particular después de que se introduzcan cambios en el sistema, un ente independiente, designado por las autoridades electorales, debe verificar que el sistema de voto electrónico esté funcionando correctamente y que se hayan adoptado todas las medidas de seguridad necesarias.

- Debe haber la posibilidad de un segundo escrutinio. Los otros elementos del sistema de voto electrónico que puedan influir en la corrección de los resultados deben ser verificables.

- El sistema de voto electrónico no debe impedir la repetición parcial o completa de una elección o un referéndum.

D) Garantías de fiabilidad y seguridad del sistema (principios del 28 al 35):

- Las autoridades del Estado miembro deben asegurar la fiabilidad y la seguridad del sistema de voto electrónico.

- Deben adoptarse todas las medidas posibles para evitar la posibilidad de fraude o intervención desautorizada que afecten al sistema durante todo el proceso de votación.

- El sistema de voto electrónico debe incluir medidas para conservar la disponibilidad de sus servicios durante el proceso de voto. En particular, debe ser resistente a un funcionamiento defectuoso, averías o ataques de denegación de servicio.

- Antes de cualquier elección con voto electrónico, la autoridad electoral competente debe comprobar que el sistema de voto electrónico es genuino y opera correctamente.

- Sólo las personas designadas por la autoridad electoral deben tener acceso a la infraestructura central, los servidores y los datos de la elección. Habrá reglas claras establecidas al respecto. Las actividades técnicas críticas serán realizadas por equipos de como mínimo dos personas. La composición de los equipos se cambiará regularmente. Tales actividades se llevarán a cabo fuera de períodos de elección, cuanto más alejados mejor.

- Mientras una urna electrónica esté abierta, cualquier intervención autorizada que afecte al sistema será realizada por equipos de como mínimo dos personas, será objeto de un informe y estará controlada por representantes de la autoridad electoral competente y observadores de las elecciones.

- El sistema de voto electrónico mantendrá la disponibilidad y la integridad de los votos. También mantendrá la confidencialidad de los votos y los mantendrá impermeabilizados hasta el proceso de recuento. Si se almacenan o se comunican fuera de ambientes controlados, los votos se encriptarán.

- Los votos y la información de los votantes permanecerán impermeabilizados mientras los datos estén de una forma en la que puedan ser asociados. La información de autenticación estará separada de la decisión del votante en una fase predefinida en la elección por voto electrónico.

Además, la recomendación prevé también dos apartados dedicados respectivamente a las normas operacionales (forma de uso y mantenimiento del *software* y del material utilizado en el voto electrónico) y normas técnicas (referidas al desarrollo y el funcionamiento del *software* y el material para que permitan la seguridad técnica, la accesibilidad y la interoperabilidad de los sistemas de voto).

Por otro lado, también pueden ser de interés otros documentos como, por ejemplo, los Estándares para los Sistemas de Voto Electrónico, aprobados por la Comisión Electoral Federal de los Estados Unidos de América el 30 de abril de 2002.

III

En la consulta formulada se pide a esta Agencia que elabore un informe sobre el voto electrónico, sobre su viabilidad, sus ventajas, sus inconvenientes y sus garantías, especialmente sobre la seguridad y el mantenimiento del secreto del voto.

En cuanto a la viabilidad del sistema de voto electrónico en las elecciones autonómicas, obviamente esta posibilidad está condicionada a la regulación de esta modalidad de voto mediante la ley electoral de Cataluña, puesto que la LOREG no prevé este sistema de votación. Así lo hizo el País Vasco, que, de hecho, es la única comunidad autónoma del Estado español que prevé mecanismos de voto electrónico en la elección de cámaras legislativas, mediante la Ley 5/1990, de 15 de julio, Electoral del País Vasco (a partir de la reforma operada por la Ley 15/1998, de 19 de junio), que pese a llevar ya más de diez años en vigencia aún no ha sido aplicada en ningún proceso electoral del Parlamento Vasco, puesto que la disposición adicional primera de la Ley 15/98 condiciona la aplicabilidad de sus previsiones sobre el voto electrónico a que el Parlamento Vasco declare, a propuesta del gobierno, la aplicabilidad del sistema, determinando las circunscripciones electorales, las secciones o los municipios donde deba aplicarse, la compatibilidad o no con el voto por papeleta y, en su caso, la progresiva implantación del sistema.

Por otro lado, aunque se han llevado a cabo diferentes pruebas tanto en elecciones autonómicas (por ejemplo, las elecciones al Parlamento de Cataluña de los años 1995 y 2003, o al Parlamento de Galicia del año 1997) como en elecciones estatales (por ejemplo, las elecciones generales de 2004 o las elecciones europeas de 2009), han sido siempre pruebas que, a pesar de estar autorizadas por la Junta Electoral Central, no tenían valor oficial, sino que se han utilizado de forma paralela al sistema tradicional. En cambio, sí que se han llevado a cabo experiencias en otros países, por ejemplo en los Estados Unidos, en países sudamericanos (Brasil, Venezuela) o en países europeos (Bélgica o Francia, en este último caso sólo para los residentes en el extranjero).

En cualquier caso, otros países han previsto estos sistemas en sus legislaciones y existen numerosos proyectos en marcha sobre esta materia tanto en el ámbito de Cataluña, como el Observatorio Voto Electrónico (http://www.votobit.org/), de la Unión Europea (www.eucybervote.org) o de Estados Unidos (estudio sobre el voto electrónico por Internet de la Fundación Nacional de Ciencia Norteamericana, www.interpolicy.org).

Desde el punto de vista de la protección de datos, en principio no se plantean obstáculos que permitan concluir la inviabilidad de forma absoluta de la aplicación de sistemas de voto electrónico, especialmente porque, como veremos, bajo esta denominación se engloban diferentes sistemas de voto con niveles de impacto en la privacidad que pueden ser muy diversos. Sin embargo, resulta evidente que la aplicación de mecanismos de voto electrónico implica la aparición de nuevos riesgos que pueden acabar afectando a algunos de los elementos esenciales del proceso electoral.

En especial, pueden surgir riesgos para el carácter secreto del voto, pero también respecto al carácter libre del derecho de sufragio o el carácter igual. En este sentido, la falta de garantías adecuadas en lo que concierne al secreto del voto puede ser claramente un elemento disuasorio en cuanto a la participación, con las consecuencias que este hecho puede tener en la formación de la voluntad democrática, puesto que acabará afectando a la libertad de acudir a votar o de expresar el voto en un determinado sentido.

Por otro lado, el carácter de igual, que también debe predicarse del derecho de sufragio, puede verse afectado por una falta de garantías que o bien impidan la participación de determinados ciudadanos, por errores en el sistema electrónico de identificación que provoquen duplicidades de voto, o bien permitan suplantaciones de identidad.

La función que cumple el procedimiento electoral como instrumento de legitimación del poder legislativo requiere que se revista de todas las garantías que permitan la más amplia consecución de esta finalidad legitimadora. La incorporación de las tecnologías al proceso de elección política debe ser acogida con cautela e implantada con las debidas garantías para evitar que un instrumento auxiliar (los medios electrónicos) introduzca elementos y condicionantes que puedan subvertir el orden de valores inherentes al derecho de sufragio. Por tanto, sea cual sea el sistema utilizado, el sufragio debe seguir siendo universal, libre, igual, directo y secreto.

Por eso, desde el punto de vista de la protección del dato relativo a la opción política de las personas que participan en el proceso electoral –dato que, como hemos visto, merece la consideración de dato especialmente protegido de acuerdo con la normativa de protección de datos–, aunque la LOPD no resulte de aplicación en sentido estricto, es preciso adoptar las medidas de seguridad adecuadas para evitar su alteración, pérdida, tratamiento o acceso no autorizado (art. 9 LOPD). Al respecto, el artículo 81 del Reglamento de Desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, regula la aplicación de los niveles de seguridad a los tratamientos de datos de carácter personal y, concretamente, la letra a) del artículo 81.3 prevé que se apliquen las medidas de seguridad de nivel alto a los ficheros o los tratamientos que revelen datos de ideología.

Ahora bien, la aplicación de esas medidas puede no ser suficiente en vista de los riesgos generados por este peculiar proceso y su importancia para la legitimidad de las propias instituciones públicas.

Sin entrar en los detalles de las medidas de protección concretas que deberían aplicarse, ya que eso dependerá de los sistemas y los dispositivos de votación electrónica que se utilicen, sí que puede avanzarse que deberá darse respuesta efectiva a lo que se desprende de lo contenido en el principio de seguridad. Es decir, con independencia de las medidas concretas que se apliquen, éstas deberán evitar la alteración, la pérdida y el tratamiento o el acceso no autorizado de los datos personales relacionadas con el proceso de votación electrónica.

En los procesos de votación concurren dos conceptos a priori antagónicos, cuya sincronización resulta especialmente compleja en el caso de los procesos donde intervienen tecnologías, como el hecho de que, por un lado, cada persona que participa emitiendo su voto debe estar perfectamente identificada, a fin de evitar suplantaciones o duplicidad de votos, y, por el otro, debe garantizarse el secreto del voto emitido, es decir, identificación y anonimato deben quedar salvaguardados en el conjunto del proceso de votación. Obviamente todo ello teniendo en cuenta las necesarias garantías que deben acompañar el proceso de escrutinio final y de libre emisión del voto.

En definitiva, desde la óptica de la normativa de protección de datos de carácter personal habrá que implantar todas las medidas de seguridad previstas en el título VIII del Reglamento ya mencionado, tanto las de carácter automatizado como las no automatizadas, puesto que, como ya se ha apuntado, los sistemas de votación electrónica resultarán complejos y no estarán exclusivamente automatizados en todas las fases del ciclo de votación electrónica.

Para analizarlo, a continuación expondremos las ventajas y los inconvenientes de los sistemas de votación electrónica, siempre desde la perspectiva de la protección de datos, tal como se solicita en la consulta.

IV

Lo primero que debe aclararse, para analizar las ventajas y los inconvenientes de los sistemas electrónicos de votación, es que, pese a que suela utilizarse una misma denominación, *voto electrónico*, para referirse a los diferentes sistemas posibles, existen profundas diferencias entre unos sistemas y otros, que aconsejan distinguir, como mínimo, entre los sistemas de voto electrónico presencial y los sistemas de voto electrónico remoto.

En los primeros, es decir, los sistemas presenciales, se incluirían tanto los sistemas que se limitan a facilitar la lectura electrónica de las papeletas como los que permiten introducir la opción de voto directamente a través de un terminal ubicado en los colegios electorales (sistemas de Registro Electrónico Directo, RED), así como aquellos en los que el terminal facilita el voto incorporado en un soporte electrónico que es introducido en la urna electrónica.

Por otra parte, los sistemas de voto remoto, siguiendo la definición de la Recomendación 2004 (11) del Consejo de Europa, son aquellos sistemas en los que el sufragio se registra a través de un dispositivo no controlado por la autoridad electoral. Así pues, el elemento clave no es la lejanía del lugar donde se ejerce el voto (el voto en una embajada no sería un voto remoto), sino la ausencia de control presencial por parte de la autoridad electoral en el momento de expresarse el voto.

De acuerdo con eso, algunos sistemas, como la emisión del voto electrónico desde un lugar lejano respecto al espacio donde se realiza la votación, pero que se realice a través de terminales facilitados y controlados por la autoridad electoral (por ejemplo, en los consulados o en otros espacios habilitados por la Administración electoral), no tendrían, de acuerdo con esta recomendación, la consideración de voto remoto, aunque el hecho de que la información se transmita a través de la red conlleva, como veremos, algunos riesgos que exigen tratarlos en determinadas cuestiones como un sistema de voto remoto. Por otro lado, en el informe adjunto a la solicitud de dictamen de la Agencia, se describen dos mecanismos de voto electrónico, uno de carácter presencial, mediante la utilización de urnas electrónicas, y otro de carácter no presencial o a distancia, basado en el uso de redes públicas de telecomunicaciones. Concretamente se hace referencia al "voto remoto por Internet". Por eso, aunque de acuerdo con aquella recomendación este supuesto no tendría la consideración de voto remoto, nosotros lo incluiremos en esta categoría a efectos de dar respuesta a la pregunta planteada, ya que en cualquier caso se trata de sistemas que utilizan Internet en el proceso de emisión del voto.

La distinción es importante porque los riesgos generados para la protección de datos en unos sistemas y otros presentan profundas diferencias que aconsejan tratarlos por separado. Por tanto, dedicaremos los siguientes epígrafes al análisis de cada uno de estos sistemas, presencial y remoto, distinguiendo dentro de cada uno las diversas fases del proceso electoral.

V

Sin embargo, antes de entrar en el análisis de las ventajas y los inconvenientes distinguiendo entre los sistemas de voto electrónico presencial y remoto, es preciso hacer algunas consideraciones generales que, aunque no se refieran propiamente al acto de votación y escrutinio, sí que forman parte del proceso electoral, plantean algunas cuestiones de interés desde el punto de vista de la protección de datos y puede convenir tenerlas en cuenta también con vistas a una futura ley electoral catalana.

La incorporación de los medios electrónicos para la formación del padrón goza ya de una consolidada experiencia en nuestro país desde que la modificación del artículo 17 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, efectuada en 1996 mediante la Ley 4/1996, de 10 de enero, estableció que el padrón municipal debía ser llevado por los ayuntamientos con medios informáticos y que debía preverse reglamentariamente la transmisión telemática de los datos del padrón a la oficina del censo para la elaboración del censo electoral.

Pero, más allá de eso, desde el punto de vista de la protección de datos resulta relevante la posibilidad de incorporar los medios electrónicos como sistema de consulta de las listas electorales. La incorporación, a partir de la Ley Orgánica 1/2003, de 10 de marzo, para la Garantía de la Democracia de los Ayuntamientos y la Seguridad de los Concejales, de la posibilidad de que la consulta de las listas pueda realizarse a través de medios informáticos, previa identificación del interesado, salvo que el ayuntamiento no cuente con medios informáticos para hacerlo, ha supuesto una medida que debe ser valorada positivamente desde el punto de vista de la protección de datos, puesto que evita accesos indebidos a datos del resto de los electores, a pesar de que una plena garantía del derecho requeriría que este medio se extendiese de forma obligatoria a todos los casos, de modo que se suprimiría la posibilidad de la exposición de las listas, especialmente a partir de la exigencia de incorporación de los medios electrónicos prevista en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP). Dicha posibilidad ha sido

desarrollada por el Real Decreto 1799/2003, de 26 de diciembre, y ha sido objeto también de la Instrucción de 20 de enero de 2004 de la Junta Electoral Central. De dicho real decreto debe destacarse que, aunque prevea los sistemas de identificación de los votantes cuando efectúan la consulta ante el ayuntamiento u oficina consular (DNI, pasaporte o permiso de conducir, y la tarjeta de residencia para los extranjeros), no recoge la forma de identificación por medios electrónicos, por lo que habrá que atenerse a lo establecido en el artículo 13 de la LAECSP. En cualquier caso, para evitar discriminaciones derivadas de la falta de acceso a los medios informáticos necesarios para efectuar la consulta, sería necesario no sólo prever la posibilidad de hacer esta consulta por Internet, con las garantías necesarias de identificación, sino también establecer puntos de atención presencial donde se pongan a disposición de los ciudadanos los medios electrónicos necesarios para realizar estas consultas (art. 8.2.a de la LAECSP).

En segundo lugar, otra cuestión que debe analizarse en este apartado sería la relativa a la Administración electoral, tanto desde el punto de vista de su composición como de sus funciones. Respecto a esta cuestión, debe tenerse en cuenta que la regulación de las juntas electorales contenida en la LOREG, de acuerdo con la disposición adicional primera de la misma ley orgánica, resulta aplicable también a los procesos electivos a las asambleas de las comunidades autónomas. Tal como ha manifestado el Tribunal Constitucional, no pueden alterarse "aspectos relevantes que alteren su posición institucional", pero en cambio "las comunidades autónomas pueden regular, respecto a sus propias elecciones parlamentarias, aspectos específicos de las Juntas actuantes en su territorio" (STC 154/88).

En cuanto a la composición, hay que tener en cuenta que tradicionalmente han formado parte de las juntas electorales personas con un marcado perfil jurídico o de los ámbitos de la sociología o las ciencias políticas (art. 9.1, 10.1 y 11.1 de la LOREG), mientras que la incorporación de los medios tecnológicos requeriría también la incorporación en estos órganos de miembros con un perfil claramente tecnológico o, como mínimo, la dotación a la Administración electoral de medios personales que permitan atender de forma adecuada las nuevas funciones que en el ámbito tecnológico le deben corresponder.

En cuanto a las funciones, el Estatuto de Autonomía de Cataluña establece que la Administración electoral es independiente y garantiza la transparencia y la objetividad del proceso electoral. Coincide en eso con la LOREG, que en su artículo 8 establece que las juntas electorales garantizan la transparencia y la objetividad, así como el principio de igualdad. Pero, más allá de eso, en la regulación de las funciones de las juntas (art. 19, 20 y otros) no se prevé expresamente, por ejemplo, la intervención de la junta electoral en la supervisión y el control de los sistemas electrónicos de votación, a diferencia de lo que ocurre, por ejemplo, con las papeletas y los sobres en la votación manual (art. 70.1). Convendría, por tanto, regular las funciones de la Administración electoral teniendo en cuenta las exigencias derivadas de los sistemas electrónicos de votación.

En cualquier caso, dicha verificación u homologación a priori de los sistemas electrónicos que pretendan utilizarse debería permitir un análisis completo tanto de los equipos como del *software*, abarcando la posibilidad de acceder al código fuente y a los programas utilizados, cuestión esta última que ha resultado problemática en algunas experiencias realizadas hasta el momento, dada la incidencia de cuestiones relativas a la propiedad intelectual. En este sentido, la ley brasileña de voto electrónico (Ley n.º 9504, de 30 de septiembre de 1997), que después ha sido seguida por leyes de otros países de Sudamérica, aparte de prever este control por parte de la Administración electoral, prevé también la participación en dicho control de

representantes acreditados de los partidos políticos (art. 66). También en este sentido, la recomendación relativa a la seguridad de los sistemas de voto electrónico elaborada por la Comission National d'Informatique et Libertés, autoridad francesa de protección de datos, recomienda tanto el carácter accesible del código fuente como el establecimiento de mecanismos para evitar la alteración o la modificación del sistema con posterioridad a su control.

En tercer lugar, junto con estas cuestiones relativas a la Administración electoral, es preciso llamar la atención sobre los riesgos que pueden generarse en el proceso electoral como consecuencia del encargo de determinadas funciones a empresas privadas por parte de la Administración electoral. Nos estamos refiriendo a las empresas que facilitan el *hardware* necesario para llevar a cabo el proceso, así como a las que desarrollan las aplicaciones informáticas que serán utilizadas o las que deben intervenir en las incidencias que se produzcan en el día de la votación. En este sentido, es frecuente que puedan aparecer impedimentos vinculados a la protección de la propiedad intelectual que puedan acabar afectando a la transparencia del sistema, por lo que es preciso establecer las medidas apropiadas que permitan su verificación completa, accediendo, en su caso, al código fuente utilizado. Del mismo modo, tal como establece la citada recomendación del Consejo de Europa respecto a las intervenciones que deban llevarse a cabo durante el funcionamiento del mecanismo electoral, es preciso establecer garantías para asegurar que sean realizadas sólo por personal autorizado, así como que se cumplan otras garantías adicionales, como la necesidad de que se cambie este personal periódicamente o la conveniencia de que intervengan en equipos de más de una persona. Por otro lado, siempre que fuera posible, dichas operaciones de mantenimiento no deberían llevarse a cabo durante el tiempo en que se desarrollara la elección.

En cuarto lugar, otra posibilidad, mientras exista el sistema de votación presencial, sería la de incorporar la solicitud de voto por correo a través de medios electrónicos. En este caso habrá que establecer las garantías adecuadas en cuanto a la identificación y la autenticación de las personas que lo soliciten, así como para asegurar la confidencialidad de los envíos que se realicen.

Pero, sin lugar a dudas, el aspecto sobre el que se debe llamar más la atención en esta fase preparatoria es la importancia de facilitar información adecuada y suficiente a los futuros votantes sobre el sistema de votación electrónico. Veremos más adelante que la existencia de riesgos adicionales creados por la utilización de medios electrónicos requiere adoptar medidas para preservar los principios que debe reunir el derecho de sufragio, esto es, su carácter universal libre, igual y secreto. Este aspecto es esencial para la legitimidad del proceso de votación. Ahora bien, la adopción de esas medidas no es suficiente para garantizar la consecución de dichos principios, puesto que el desconocimiento o la desconfianza de los futuros votantes en los nuevos sistemas implantados pueden acabar afectando a los rasgos esenciales que debe cumplir el proceso de votación. A pesar de haber adoptado las medidas de seguridad necesarias, es preciso generar confianza entre los ciudadanos en la utilización del sistema para que el sufragio sea realmente universal, libre e igual.

En un proceso de votación tradicional, la presencia humana y el control realizado directamente por el votante en el momento de la introducción del sobre en la urna, así como el control humano realizado directamente en el momento del escrutinio, no sólo por parte de los integrantes de las meses sino también de los interventores y apoderados designados por los partidos políticos, contribuyen a generar en los electores la confianza de que su voto será secreto y el recuento será correcto.

Por eso resulta esencial una adecuada información a los ciudadanos. En este sentido, el artículo 43 del Estatuto de Autonomía de Cataluña establece que los poderes públicos deben procurar que las campañas institucionales que se organicen en ocasión de los procesos electorales tengan como finalidad promover la participación ciudadana y que los electores reciban de los medios de comunicación una información veraz, objetiva, neutral y respetuosa con el pluralismo político. En el mismo sentido se manifiesta también el artículo 50 de la LOREG al prever que los poderes públicos puedan llevar a cabo una campaña institucional dedicada a informar a los ciudadanos de la fecha de la votación, el procedimiento para votar y los requisitos y trámites del voto por correo. Pues bien, en el caso de la utilización de medios tecnológicos, la realización de una campaña para explicar los sistemas de votación, el procedimiento y las medidas de seguridad aplicadas y las otras garantías establecidas no debería ser sólo una opción de los poderes públicos, sino que debería constituir un auténtico mandato. Tal como pone de manifiesto la recomendación del Consejo de Europa mencionada, la transparencia del sistema, entendida como información a los ciudadanos sobre sus características y funcionamiento, resulta un requisito esencial.

Y esta exigencia no sólo se derivaría de lo que acabamos de exponer, sino también desde el punto de vista de la normativa de protección de datos. Así se desprende por ejemplo de los razonamientos del Tribunal Constitucional en relación con el artículo 5 de la LOPD, que regula el derecho de información de las personas respecto al tratamiento de sus datos personales: “sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia”. El derecho a ser informado del destino y el tratamiento que se dará a los datos de carácter personal forma parte del núcleo esencial del derecho fundamental a la protección de datos y adquiere aún más importancia cuando se trata de datos especialmente protegidos como son los referentes a la opción política. Por eso, aunque en materia electoral no resulte aplicable el artículo 5 de la LOPD, resultará igualmente exigible asegurar por los medios adecuados que el ciudadano tiene conocimiento de cómo serán tratados sus datos.

VI

En cuanto a las ventajas de la implantación de un sistema de voto electrónico presencial, suelen citarse la menor carga de trabajo de los miembros de las mesas, la rapidez del escrutinio y la posterior transmisión de los datos, la reducción de la conflictividad en el recuento, la ampliación de las formas de expresión del derecho de sufragio (en el supuesto de que sea un sistema opcional), la introducción de las nuevas tecnologías en este ámbito, que contribuye a la educación del cuerpo electoral en las nuevas tecnologías, e incluso una reducción del voto nulo.

No obstante, estrictamente desde el punto de vista de la protección de datos, es decir, de la protección del derecho fundamental de las personas a que la información sobre su persona, en este caso relacionada con su opción política, sea tratada adecuadamente, no parece que plantee ventajas significativas respecto al sistema tradicional de votación. Tal vez la ventaja más relevante serían las mayores garantías de seguridad que ofrecen los medios electrónicos para una identificación segura de los votantes, pero lo cierto es que hasta el momento ésta tampoco había sido una cuestión especialmente conflictiva en el sistema de voto tradicional.

En cuanto a los inconvenientes del sistema, es obvio que la incorporación de medios electrónicos conlleva nuevos problemas como, por ejemplo, los derivados de errores

en el *software* o el riesgo de una manipulación indebida, ya sea de forma intencionada por parte de las entidades que participan en su elaboración o mantenimiento, o como consecuencia de la actuación de terceras personas. En cualquier caso, los problemas que puedan generarse dependerán de la tecnología elegida, de modo que previsiblemente deberían ser menores en sistemas que se limiten a la lectura electrónica de la papeleta en soporte papel que en aquellos otros que incorporen otros elementos en soporte electrónico. Estos problemas pueden deducirse de los riesgos generados por la implantación de estos nuevos sistemas de votación. Para analizarlo distinguiremos cuatro fases clave en este ciclo:

- Fase de identificación y autenticación de la persona con derecho a voto
- Fase de emisión del voto
- Fase de escrutinio y destrucción de la información
- Fase de verificación o control del voto emitido

1.- Fase de identificación y autenticación

En esta fase se identifica a la persona con derecho a voto con el fin de proporcionarle algún tipo de "credencial" para proceder a la votación electrónica, así como su posterior autenticación, es decir, la acreditación por medios electrónicos de la identidad de una persona. En el caso de la urna electrónica, no tiene por qué aparecer este elemento de identificación previa y asignación de credencial de voto electrónico, ya que el hecho de ser presencial permite aplicar los protocolos de identificación que se aplican en los sistemas de voto tradicional. De hecho, en función del tipo de sistema de voto electrónico presencial del que se trate, la identificación seguirá realizándose con lo que podríamos llamar sistemas tradicionales, puesto que la incorporación de los medios electrónicos se referiría sólo a la emisión del voto y el posterior recuento.

Ahora bien, la incorporación de medios electrónicos en esta fase en una votación presencial podría suponer que se permita la identificación por medios electrónicos a través, por ejemplo, del DNI electrónico. Pero este hecho no debe introducir necesariamente riesgos adicionales respecto a los procesos de identificación tradicional, salvo que el sistema de votación electrónico se lleve a cabo de modo que permitiese vincular un determinado voto (su sentido) con una determinada persona. Una carencia de ese tipo afectaría al carácter secreto del derecho a voto. Pero, en realidad, no sería un problema de la fase de identificación, sino de la fase posterior de emisión del voto.

En cualquier caso, en función de cuál sea la tecnología utilizada, sí que es preciso tener especial cuidado con aquellos procesos que impliquen la atribución de códigos o claves a los futuros votantes para poder ejercer su derecho de voto, porque el carácter secreto no sólo puede verse comprometido en el momento del escrutinio, sino en el momento de la atribución o la comunicación de esos códigos o claves.

2.- Fase de emisión del voto

En el caso de la votación electrónica basada en "urnas electrónicas" deben tenerse en cuenta aspectos relacionados con la protección de los sistemas que almacenan los votos emitidos, de forma que no pueda accederse a ellos (consulta o alteración), ya no sólo desde redes externas de carácter público, sino desde redes internas. Las medidas de seguridad deben evitar que alguien pueda conocer el contenido del voto de una persona concreta y que, mediante procesos de explotación de la información a partir de la exportación de bases de datos o la copia de esta información en otras

ubicaciones, se pueda tener un acceso fuera de los canales habituales de explotación de la información. En este sentido, deben extremarse las medidas de seguridad no sólo en relación con los usuarios de aplicaciones informáticas relacionadas con la explotación de los datos, sino también las vinculadas con el personal técnico o los administradores de sistemas que puedan tener relación con los servidores y las infraestructuras técnicas de soporte al proceso de votación electrónica; en definitiva bajo ninguna circunstancia nadie diferente a la persona que ha emitido el voto puede conocer su contenido. El secreto del voto debe ser salvaguardado en todo momento.

Al margen de eso, las medidas encaminadas a preservar el carácter secreto del derecho de voto que ya estaban aplicándose en el sistema tradicional, como por ejemplo las cabinas o espacios similares, así como la adecuada orientación de las pantallas –en el caso de que se utilicen pantallas táctiles–, pueden seguir siendo plenamente exigibles para los sistemas de votación electrónica presencial.

En cualquier caso, debe eliminarse cualquier posibilidad de vincular un voto con una determinada persona directa o indirectamente (así, por ejemplo, las papeletas electrónicas deben conservarse de forma que no coincida con el orden en el que han sido emitidos los votos).

3.- Fase de escrutinio y destrucción de la información

En esta fase debe garantizarse que la información sobre los votos no sea accesible hasta que finalice el plazo de votación del conjunto del proceso electoral, por lo que la información debe estar convenientemente custodiada hasta que los sistemas de escrutinio puedan empezar a contabilizar los votos recibidos.

En el caso de las urnas electrónicas, hay que custodiar el soporte que ha recibido el voto, de modo que no pueda accederse (consultarse o manipularse) a la información sobre el sentido del voto hasta el final de la votación y, si es posible, con algún mecanismo que requiera la participación de los diferentes miembros de la mesa (por ejemplo, atribuyéndoles a cada uno de ellos una parte de un código). También deberán preverse medidas para el transporte de la información desde esos dispositivos hasta los sistemas de escrutinio o de consolidación de resultados, tanto si el transporte se basa en redes de telecomunicaciones, como en el traslado físico de dispositivos digitales de almacenamiento.

Aunque no tenga un impacto directo en los datos personales como tales, también conviene que, a fin de salvaguardar la no alteración de la información en los procesos de escrutinio, puedan preverse sistemas que permitan reproducir de distintas maneras el proceso de escrutinio (recuento). Este control puede servir para detectar posibles errores en las aplicaciones informáticas. A tal fin algunos autores apuntan la posibilidad de que el elector obtenga un comprobante de su voto, que en algunos sistemas debería introducirse en una urna paralela que permitiría un recuento manual paralelo, en caso de ser necesario (método Mercurio), y en otros actuaría como una especie de resguardo del voto ejercido. De ser así, para evitar que la existencia de esos comprobantes pueda facilitar el uso de medidas de coacción (permitiría al coaccionador verificar la eficacia real de la coacción) que acaben afectando a la libertad y al secreto del voto, es preciso que de esos comprobantes no pueda deducirse el sentido del voto, sin la intervención de la autoridad electoral.

Los riesgos que surgen en esta fase están relacionados con el almacenamiento y la explotación de la información, es decir, debe determinarse, una vez cerrado oficialmente el proceso de votación y finalizado el escrutinio, en qué situación queda la información hasta el agotamiento de los plazos de recurso contencioso electoral. Debe

concretarse si debe quedar bloqueada y de qué manera, así como los mecanismos de destrucción segura de la información y las condiciones de recuperación si fuera el caso.

Por tanto, las medidas de seguridad tendrán que ver con el control de acceso e integridad de la información, y de gestión de los soportes donde se encuentre almacenada, y con los mecanismos de borrado seguro de la información.

4.- Fase de control o verificación

Habitualmente los sistemas de votación electrónica incorporan mecanismos que permiten a la persona que emitió el voto verificar a posteriori si su voto ha sido correctamente recogido y contabilizado; por supuesto eso requiere no sólo mecanismos técnicos, sino también organizativos que garanticen esta parte del ciclo de votación.

Aparte de los riesgos que ya hemos señalado en la fase anterior, también existe la posibilidad de que con estos sistemas de verificación o control a posteriori alguien pueda acceder al sentido del voto de personas identificadas o identificables, ya sea por suplantación de credenciales o por sustracción de la información de los servidores que almacenan la información.

Desde la perspectiva de la protección de datos, nos situaríamos en el contexto de la obligación que tiene el responsable del tratamiento de salvaguardar la información que tiene almacenada y los soportes que la contienen (sistemas de copias de seguridad, por ejemplo), así como de garantizar que sólo pueda acceder a dicha información la persona a la que corresponde el voto emitido.

VII

En el caso del voto electrónico remoto, a las ventajas que ya se han expuesto en el epígrafe anterior respecto al voto electrónico presencial suele añadirse el hecho de que incrementa las posibilidades de participación, puesto que facilita el derecho de voto, por un lado, de aquellas personas que no pueden o tienen dificultades para acceder a los colegios electorales (por ejemplo, personas residentes en el extranjero o personas con discapacidades o enfermedades) y, por el otro, de aquellos colectivos que por su familiaridad con el uso de las nuevas tecnologías, especialmente las personas jóvenes, pueden sentirse más atraídos por este canal. Por otro lado, también se alega una reducción de gastos a medio plazo, que parece previsible en el sistema de voto remoto (siempre, claro está, dependiendo de la estabilidad del sistema y de la posibilidad de uso en diferentes tipos de elecciones) y que, en cambio, no parece que pueda predicarse en el caso del voto electrónico presencial, e incluso se dan argumentos vinculados a la sostenibilidad ambiental.

Pero, al margen de la mayor o menor exactitud de esas supuestas ventajas, especialmente en lo relativo al supuesto aumento de la participación (de hecho, no parece que las experiencias piloto que se han realizado –con el condicionante, claro está, de ser pruebas sin valor vinculante– permitan llegar a esta conclusión), lo cierto es que desde el punto de vista de la protección de datos tampoco se observa ninguna ventaja significativa para la protección de los datos de carácter personal, más allá de lo que ya hemos expuesto en el epígrafe anterior respecto a la autenticación de los electores.

En cuanto a los inconvenientes, aparte de los derivados de la eliminación de los aspectos rituales asociados tradicionalmente a la emisión del voto, desde el punto de vista de la protección de datos, más allá de los errores en el *software* o su manipulación, aspectos en los cuales se dan por reproducidas las consideraciones formuladas respecto a los sistemas de voto electrónico presencial, adquieren especial relevancia los problemas derivados de la utilización de la red de Internet como canal de transmisión del voto. Como en el caso anterior, los analizaremos a partir de la detección de los riesgos generados en cada una de las fases del proceso de votación:

1.- Fase de identificación y autenticación

Esta fase es de especial relevancia cuando se trata de un sistema de votación "remota" o no presencial. Esta fase se identifica en el informe de expertos como el registro previo que permite el voto por Internet, así como la posterior autenticación del votante.

Los peligros que pueden darse en esta fase pueden surgir en relación con la articulación de mecanismos y procedimientos que no sean suficientemente seguros a la hora de identificar a las personas con derecho a voto y de proporcionarles la credencial que les debe permitir votar por Internet o remotamente.

Algunas de las consecuencias de una mala definición de este protocolo podrían ser:

• Proporcionar una credencial de voto a alguien que no tiene derecho a votar

• Proporcionar una credencial de voto de una persona a otra diferente

• Proporcionar más de una credencial de voto a una misma persona

En este sentido, el envío de credenciales que permitan el ejercicio del derecho a voto, que en principio deberían ser anónimas, debe asegurar que la persona que realmente recibe la credencial es quien se supone que es, así como establecer algún mecanismo complementario que permita asegurar la autenticación en el momento de la votación.

Desde la perspectiva de la protección de datos de carácter personal, según cuál sea el sistema que se diseñe, podemos encontrarnos ante una vulneración del principio de calidad si, por ejemplo, puede existir verificación posterior del voto por parte del votante con una credencial comprometida produciéndose un acceso o tratamiento no autorizado.

En esta fase también resulta de especial relevancia la robustez de la credencial que permite votar electrónicamente, de modo que no debe poder reproducirse ni debe ser conocida por terceras personas, ya que también podríamos encontrarnos con situaciones de acceso o tratamientos no autorizados.

Hay modelos de gestión como el de las entidades de certificación, que emiten certificados digitales que permiten tanto la autenticación en sistemas informáticos como la generación de firmas electrónicas, que tienen procesos de registro orientados a garantizar que el certificado digital y las claves criptográficas relacionadas le son proporcionadas a la persona correcta –habitualmente utilizan una estructura de gestión basada en entidades de registro– y que realizan las tareas de identificación de las personas y de entrega segura de los certificados digitales y claves.

En Cataluña tenemos experiencia con este modelo de entrega de credenciales electrónicos a través de las actividades del Consorcio Administración Abierta de Cataluña y específicamente de la Agencia Catalana de Certificación (Catcert).

En cualquier caso, en lo relativo a la autenticación, en todo proceso que implique acceso remoto a sistemas de información o aplicaciones informáticas debe existir una verificación de que quien quiere acceder a la información o realizar una acción es realmente quien tiene derecho a hacerlo (control de acceso); por tanto, en este proceso de autenticación deben extremarse las precauciones para evitar que el sistema de presentación y verificación de credenciales sea vulnerado, y un tercero pueda acceder al sistema haciéndose pasar por otro, de modo que suplante su identidad y acceda a sus derechos en relación con la información o las funciones autorizadas.

En el caso del voto electrónico mediante Internet, las medidas de seguridad deben evitar los efectos descritos, garantizando en todo momento que quien accede a emitir el voto es realmente quien tiene derecho a hacerlo y que no se produce ni suplantación ni la posibilidad de votar más de una vez.

2.- Fase de emisión del voto

El hecho de utilizar redes públicas de telecomunicaciones (Internet) o redes privadas fuera del control de la autoridad electoral añade riesgos derivados de la posibilidad de que alguien capture la comunicación, ya sea como consecuencia de, por ejemplo, la instalación de *software* malicioso en los ordenadores de los usuarios (los denominados "troyanos"), el uso de redes de comunicaciones privadas inalámbricas no suficientemente protegidas (el acceso a *routers* ADSL inalámbricos) o la existencia de suplantaciones de servidor (*phising*).

Tal como hemos expuesto anteriormente respecto a los sistemas basados en una urna electrónica, es preciso velar por que el voto llegue correctamente a su destino final y no se produzcan suplantaciones. Por otro lado, en este sistema de votación adquiere aún más relevancia la protección de los sistemas que almacenan los votos emitidos, de modo que no se pueda acceder a ellos (consulta o alteración), en la medida en que se utilizan redes, públicas o privadas, no controladas por la autoridad electoral.

Del mismo modo, las medidas de seguridad deben evitar que alguien pueda conocer el contenido del voto de una persona concreta y que, mediante procesos de explotación de la información a partir de la exportación de bases de datos o la copia de esta información en otras ubicaciones, se pueda tener un acceso fuera de los canales habituales de explotación de la información. En ese sentido, como en los sistemas de voto electrónico presencial, deben extremarse las medidas de seguridad no sólo en relación con los usuarios de aplicaciones informáticas relacionadas con la explotación de los datos, sino también las vinculadas con el personal técnico o los administradores de sistemas que puedan tener relación con los servidores y las infraestructuras técnicas de soporte al proceso de votación electrónica.

También el hecho de utilizar Internet como mecanismo de acceso al sistema de votación implica que los servidores en los que reside la información y el propio proceso de votación pueden ser objeto de diferentes tipos de ataques, desde la saturación de los servidores mediante la generación de tráfico de datos que sólo tiene por objeto colapsar el sistema, lo que equivaldría a evitar el acceso al colegio electoral en los procesos de votación presencial (típicamente conocido como ataques de denegación de servicio, DOS) o ataques de suplantación del servidor (los conocidos como

phising), en los que se simula la apariencia de la página web que debe recoger el voto, de modo que el votante estaría revelando el sentido de su voto a terceros sin saberlo y su voto se perdería.

Por otro lado, aunque al analizar los riesgos inherentes a los sistemas de votación remota, en cuanto a que el individuo vota desde una ubicación sin las medidas de protección física que pueden existir en un colegio electoral, ciertamente pueden plantearse riesgos relacionados con la violencia o la coacción sobre las personas en el momento de la emisión del voto o también de uso fraudulento de credenciales electrónicas basado en relaciones de abuso de poder que deben valorarse.

En cualquier caso, tanto respecto a esta fase como en la anterior, si bien es innegable que los sistemas de voto electrónico remoto presentan considerables riesgos, éstos no son mayores que los que lleva asociado, por ejemplo, el sistema de voto por correo existente en la actualidad.

3.- Fase de escrutinio y destrucción de la información

En esta fase debe garantizarse que la información sobre los votos no es accesible hasta que finalice el plazo de votación del conjunto del proceso electoral. Por tanto, la información debe estar convenientemente custodiada hasta que los sistemas de escrutinio puedan empezar a contabilizar los votos recibidos, una vez cerrada la votación.

En el caso del voto electrónico remoto, también resultan especialmente relevantes en esta fase los riesgos derivados de la utilización de redes públicas o privadas para la transmisión del voto y adquiere especial importancia el uso de mecanismos de encriptación segura.

Por otro lado, al igual que sucede con el voto mediante urna electrónica, también surgen en esta fase riesgos relacionados con el almacenamiento y la explotación de la información. Es decir, hay que determinar una vez finalizado el escrutinio y cerrado oficialmente el proceso de votación en qué situación queda la información y debe concretarse si debe quedar bloqueada y de qué forma, así como los mecanismos de destrucción segura de la información y las condiciones de recuperación si fuera el caso.

Por tanto, las medidas de seguridad estarán relacionadas con el control de acceso e integridad de la información y de gestión de los soportes donde se encuentre almacenada, y con los mecanismos de borrado seguro de la información, aunque pueda resultar más difícil la implantación de medidas destinadas a garantizar la seguridad de las redes utilizadas para la transmisión, puesto que la propia dinámica de funcionamiento de Internet impide saber a priori cuál será el recorrido que seguirá la información incorporada al voto electrónico.

4.- Fase de control o verificación

En esta fase es preciso diferenciar los diversos tipos de controles, todos destinados a garantizar un adecuado funcionamiento del sistema.

En un sistema de votación tradicional, y también en determinados sistemas de voto presencial, este control se lleva a cabo a través de la misma composición de las mesas electorales, así como con la presencia de los representantes de los partidos políticos (interventores y apoderados) durante la jornada electoral y en el momento del

escrutinio. Pero esos controles no resultan posibles en un sistema remoto de votación electrónica. Para ello pueden preverse diferentes mecanismos de control o verificación.

En primer lugar, debe tenerse en cuenta la posibilidad de un control institucional a través de un sistema de auditorías realizado por alguna entidad independiente bajo la supervisión de la Administración electoral para determinar si la aplicación concreta del sistema de votación llevada a cabo ha sido correcta o no.

En segundo lugar, debería regularse también la participación de las formaciones políticas en este proceso de auditoría.

En tercer lugar, desde la perspectiva del control individual que pueda hacer cada ciudadano respecto a su propio voto, hay que tener en cuenta que se trata de un control que en el sistema de votación tradicional no existe, sin perjuicio, evidentemente, del recurso contencioso electoral. Ahora bien, la necesidad de transparencia y de reforzar la confianza del elector en el sistema puede hacer conveniente la adopción de este tipo de control. Dicho control puede extenderse básicamente a dos aspectos: comprobación de que se ha registrado el voto emitido y comprobación de que el sentido del voto registrado ha sido el correcto.

En lo relativo al primer aspecto, no parece que su implementación deba implicar mayores problemas que los que se pueden plantear actualmente con la anotación de los votantes que han ejercido su voto en la lista de votantes de las mesas electorales. Al respecto puede plantearse una publicación de una lista con los códigos alfanuméricos asignados a cada votante en el momento de la votación y que permitirían que él mismo identificase si su voto ha sido registrado, sin que esta circunstancia sea identificable por terceras personas.

En cambio, puede plantear más problemas la segunda de las comprobaciones apuntadas, en la medida en la que la disociación de los datos del votante respecto al voto emitido no debe poder ser reconstruida. Sin embargo, pueden implementarse sistemas en que esa comprobación pueda realizarse a través de mecanismos que requieran la participación conjunta del votante y de la Administración electoral bajo ciertas garantías (por ejemplo, un código compuesto en el que la Administración electoral tenga una parte y el votante electrónico otra).

Tal como apuntábamos antes, los riesgos se derivan de la posibilidad de que con estos sistemas de verificación o control a posteriori alguien pueda acceder al sentido del voto de personas identificadas o identificables, ya sea por suplantación de credenciales o por sustracción de la información de los servidores que almacenan la información.

Como en los sistemas presenciales, desde la perspectiva de la protección de datos nos situaríamos en el contexto de la obligación que tiene el responsable del tratamiento de salvaguardar la información que tiene almacenada y los soportes que la contienen (sistemas de copias de seguridad, por ejemplo), así como de garantizar que sólo puede acceder a dicha información la persona a la que corresponde el voto emitido.

VII

La evaluación concreta de los riesgos generados por un determinado sistema deberá realizarse tomando en consideración la solución tecnológica adoptada en cada caso. Y la tecnología, evidentemente, es cambiante. Por eso habrá que tener en cuenta la

evolución tecnológica, tanto de los nuevos sistemas de votación electrónica o de mecanismos específicos de identificación electrónica (por ejemplo, sistemas biométricos, dispositivos móviles, televisión digital, etc.) como de los nuevos riesgos derivados de la aplicación de esas nuevas tecnologías, que implicará la aparición de nuevas vulnerabilidades.

En este sentido, sea cual sea el sistema utilizado, éste debe garantizar su solidez técnica (disponibilidad, fiabilidad y seguridad), su verificación por parte de una autoridad independiente y la facilitación de información suficiente a los futuros electores sobre las características, el funcionamiento y las garantías del sistema.

Sin embargo, sí que pueden avanzarse en este dictamen algunas recomendaciones que deberían tenerse en cuenta en una futura ley electoral catalana, con independencia de cuál sea el sistema concreto elegido.

En este sentido, la ley electoral, en lo que respecta a la seguridad de la información, debería ir encaminada, por un lado, a prever grandes principios de protección de la información, principios a los que deberán dar respuesta las tecnologías, siguiendo el ejemplo del artículo 9 de la LOPD, que da contenido al principio de seguridad, y, por otro lado, la regulación deberá ser neutra tecnológicamente, sin ligar las soluciones de seguridad a tecnologías concretas.

Por eso, sin perjuicio de que las soluciones finales de tipo técnico y organizativo puedan añadir otros elementos de reflexión a los que contiene este dictamen, podemos destacar las siguientes cuestiones o recomendaciones que deben tenerse en cuenta:

a) A los sistemas de voto electrónico, sean presenciales o remotos, se les deberían aplicar las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal, para hacer efectivo el principio de seguridad.

b) El sistema que se implante debe garantizar la identificación y la autenticación del votante evitando la suplantación o la duplicidad de votos, garantizar el secreto del voto, el carácter libre del derecho de sufragio, así como la existencia de un nivel de transparencia y verificabilidad del sistema que, preservando el carácter secreto del voto, permita controlar su adecuado funcionamiento.

c) Es preciso informar adecuadamente a los ciudadanos de las características y el funcionamiento del sistema, así como de las garantías de su correcto funcionamiento.

d) Hay que realizar un análisis de riesgos detallado y adaptado a cada proceso electoral, en función de sus características y especialmente de las tecnologías utilizadas.

e) Deben aplicarse metodologías de evaluación del impacto sobre la privacidad, con el fin de elegir en cada caso las opciones que sean más respetuosas o menos “peligrosas” para la información de carácter personal relacionada con el proceso de votación, y siguiendo el modelo habitual de esas evaluaciones hacer llegar a la opinión pública el resultado de dicha reflexión (evaluación de impacto), con el objeto de generar confianza en el sistema.

f) En general será útil la aplicación de técnicas de disociación de la información en algunas fases del ciclo de voto electrónico, aunque sea necesario prever sistemas reversibles, requiriendo la concurrencia de más de una persona o sistema para volver a asociar los datos a personas, pero que en ningún caso permitan que alguien

diferente al votante pueda conocer el contenido de su voto. El secreto del voto debe garantizarse en cualquier circunstancia.

g) El cifrado de la información también será una técnica que debe tenerse presente en todo el proceso, tanto en las cuestiones relacionadas con las redes de telecomunicaciones como en el acceso y el almacenamiento de la información.

h) Es preciso establecer previsiones para verificar que las empresas que participen en la implementación del sistema de votación electrónico cumplen con todos los requisitos de seguridad y también con el resto de las garantías establecidas por la normativa de protección de datos, como por ejemplo, en su caso, la formalización de un contrato en los términos del artículo 12 de la LOPD, así como la devolución de todos los ficheros que obren en su poder al finalizar el proceso. Del mismo modo, habrá que velar por el cumplimiento de dichas exigencias en los simulacros que puedan llevarse a cabo.

i) En general hay que prever el control de la integridad de todo el sistema sobre la base de auditorías de seguridad realizadas por entidades independientes a priori, es decir, antes del inicio de los procesos de votación, que verifiquen que ninguno de los elementos del sistema de información que soporta el proceso electrónico de votación altera la información y que, en definitiva, cumple con los requisitos de seguridad definidos, y auditorías a posteriori para verificar que realmente han sido eficaces las medidas de seguridad implantadas.

j) En la definición de la arquitectura técnica y los procedimientos operativos, el principio de segregación de funciones en materia de seguridad de la información debe estar presente en todos los sistemas de información que soporten el voto electrónico.

De acuerdo con las consideraciones realizadas en estos fundamentos jurídicos, se llega a las siguientes

Conclusiones

Aunque desde el punto de vista estricto de la protección de datos la implantación de sistemas de voto electrónico no aporta ventajas significativas, pese a que sí pueda aportarlas desde otros perspectivas, la implantación de dichos sistemas no resulta contraria al derecho a la protección de los datos personales si se llevan a cabo con las debidas garantías, a las cuales se ha hecho referencia en el presente dictamen.

No obstante, dado el estado actual de la técnica, parece que la incorporación de esos medios sólo puede llevarse a cabo con plenas garantías de seguridad en sistemas de voto electrónico presencial, mientras que no parece que el voto electrónico remoto pueda ofrecer suficientes garantías. Por ello, sobre todo mientras los canales de voto electrónico remoto no sean universalmente accesibles, parece que un sistema de esas características debería limitarse a su uso como medio alternativo a los actuales sistemas de votación por correo.