PD 7/2018

Informe en relación con el Proyecto de Decreto de establecimiento del sistema de voto electrónico en los procesos de elecciones a órganos de representación del personal de administración y técnico al servicio de la Administración de la Generalidad de Cataluña

Se presenta a la Autoridad Catalana de Protección de Datos el Proyecto de Decreto de establecimiento del sistema de voto electrónico en los procesos de elecciones a órganos de representación del personal de administración y técnico al servicio de la Administración de la Generalidad de Cataluña, para que la Autoridad emita su parecer al respecto.

El Proyecto de Decreto consta de un preámbulo, seis artículos y dos disposiciones adicionales. Se acompaña de la Memoria justificativa.

Examinado este Proyecto de Decreto y la documentación que le acompaña, y visto el informe de la Asesoría Jurídica, se informa lo siguiente.

Antecedentes

El artículo 44 del Texto refundido del Estatuto básico del empleado público, aprobado mediante el Real decreto legislativo 5/2015, de 30 de octubre, dispone que el procedimiento para la elección de las Juntas de Personal y por a la elección de los Delegados de Personal se determinará reglamentariamente, teniendo en cuenta, entre otros criterios generales, que la elección debe realizarse mediante sufragio personal, directo, libre y secreto que se puede emitir por correo o por otros medios telemáticos (apartado 1.a)).

Actualmente, los procesos electorales en órganos de representación del personal al servicio de la Administración de la Generalidad de Cataluña son objeto de regulación en la Ley 9/1987, de 12 de junio, de órganos de representación, determinación de las condiciones de trabajo y participación del personal al servicio de las administraciones públicas y, de forma supletoria, es aplicable el Real decreto 1846/1994, de 9 de septiembre, por el que se aprueba el Reglamento de las elecciones a órganos de representación del personal al servicio de Administración General del Estado.

El artículo 21 de la Ley 9/1987 dispone que la correspondiente administración pública facilitará el censo de funcionarios y los medios personales y materiales para la celebración de las elecciones.

El Decreto tiene por objeto exclusivamente implantar el sistema de votación electrónica en estos procesos electorales, con el fin de fomentar la participación y el ejercicio del derecho de sufragio a los electores, eliminar significativamente los costes en medios personales y materiales, proporcionar la accesibilidad evitando desplazamientos, facilitar el ejercicio del derecho a las personas discapacitadas o con movilidad reducida, prevenir los errores en el proceso de votación y asegurar la rapidez y precisión en los escrutinios.

Fundamentos jurídicos

(...)

II

El Proyecto de Decreto que se examina tiene por objeto "el establecimiento del sistema de votación electrónica para las elecciones a órganos de representación del personal de administración y técnico al servicio de la Administración de la Generalidad de Cataluña" (artículo 1).

Tal y como ha puesto de manifiesto esta Autoridad en ocasiones anteriores, desde la perspectiva de la protección de datos personales, en cualquier proceso electoral que se celebre empleando mecanismos de votación electrónica adquiere especial importancia una adecuada gestión de la información tratada. De hecho, de ello depende que la participación sea real y efectiva. Sólo si las condiciones en las que se desarrolla el proceso electoral garantizan la correcta identificación de las personas que participan, la confidencialidad de su información -y, en especial, de su voto- y la seguridad de toda la información relacionada, queda garantizada la libertad de participar y la fiabilidad del resultado.

En este sentido, es preciso hacer especialmente mención al Dictamen 3/2010 (disponible en la web http://apdcat.gencat.cat/), en el que se analizan, desde la perspectiva de la protección de datos, pero también desde un enfoque más amplio de seguridad de la información, diversas cuestiones relacionadas con la implantación de sistemas de voto electrónico que son de interés en relación al Proyecto de Decreto que se examina. Señalar que todo aquello que, a todos los efectos, se puso de manifiesto en aquel dictamen, sigue siendo válido, en especial, los apartados relativos a los riesgos de los diferentes sistemas de votación electrónica.

Dicho esto, recuerda la conveniencia de valorar en el presente caso la realización de la evaluación de impacto en la protección de datos a que se refiere el artículo 35 del Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD).

El RGPD requiere realizar una evaluación de impacto sobre la privacidad "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o finas, entrañe un alto riesgo para los derechos y libertades de las personas físicas" (artículo 35.1).

En relación con esta evaluación de impacto, la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), enumera, en su artículo 28.2, algunos supuestos en los que se entiende probable la existencia de un alto riesgo para los derechos y libertades de las personas, tales como "cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, (…)" (letra a)), "cuando el tratamiento pudiera privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales" (letra b)), o "cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (...)" (letra c)), entre otros.

Hay que tener en consideración que, en el presente caso, el Proyecto supone el tratamiento de información personal que, si bien estrictamente no revelaría la afiliación sindical de los afectados, sí puede comportar la revelación de su ideología. Por tanto, supondría el tratamiento de datos merecedores de especial protección (artículo 9.1 RGPD).

Teniendo en cuenta la naturaleza de los datos tratados, cuyo tratamiento puede afectar a otros derechos como el ejercicio del derecho de sufragio, que pérdidas de esta información o tratamientos inadecuados de la información vinculada al proceso electoral podrían no sólo afectar al resultado del mismo sino dar lugar a situaciones discriminatorias o de coacción para los afectados, y que el

tratamiento podría afectar a un número amplio de personas, debería llevarse a cabo esta evaluación de impacto.

El artículo 35.10 del RGPD establece que si en el procedimiento de aprobación de la norma se somete el Proyecto a una evaluación de impacto sobre la privacidad después no será necesario realizarla cuando se lleven a cabo los tratamientos que se n deriven.

Ahora bien, recuerda que, en el presente caso, dicha evaluación de impacto debería comprender la evaluación no sólo de las previsiones normativas sobre el sistema de votación electrónica establecidas en el Proyecto sino especialmente la evaluación de la concreta solución tecnológica escogida para llevar a cabo tal votación. Es decir, con carácter previo a la adopción de un sistema de votación electrónica, debería llevarse a cabo una evaluación de la afectación que puede tener dicho sistema para la privacidad de las personas afectadas y un análisis de las diferentes alternativas disponibles para alcanzar la finalidad perseguida, de forma que se pueda optar por aquella que ofrezca mayores garantías para los derechos de las personas.

Dicho esto, conviene señalar que, a fin de efectuar un examen cuidadoso de las implicaciones que, para la protección de datos de los afectados, pueden derivarse de la implementación de un sistema de votación electrónica en el proceso de elección a que hace mención el Proyecto, hubiera sido conveniente haber dispuesto de dicha evaluación de impacto en el momento de emitir el presente informe.

Por último, cabe advertir que el Proyecto contempla, principalmente, aspectos y características propias de los sistemas de votación electrónica existentes pero no describe propiamente la opción tecnológica escogida, por lo que el examen se centrará únicamente en estos aspectos generales.

III

Hechas estas consideraciones iniciales, nos referimos a continuación al modelo de procedimiento de votación electrónica que configura el proyecto.

De acuerdo con el artículo 2.2 del Proyecto, el sistema de votación electrónica consiste "en la emisión del voto en soporte electrónico de forma remota a través de un dispositivo conectado a Internet (...)". Por lo que se infiere del artículo 6 del Proyecto, el elector puede ejercer el derecho de voto mediante una "Plataforma de votación electrónica por Internet".

De estas previsiones y otras contempladas en la Memoria justificativa que le acompaña (apartados III a V) parece desprenderse que el procedimiento de votación se configura como un sistema de voto electrónico remoto, que el elector podrá ejercer a través de esta "Plataforma", a la que podrá acceder a través de Internet, por tanto, a través de sus propios dispositivos (por ejemplo, un ordenador) y no de terminales facilitados y controlados por la autoridad correspondiente en un espacio determinado.

Ahora bien, el Proyecto también contiene diversas referencias expresas en la "urna digital" y en la "urna electrónica", que sería un elemento propio de los sistemas presenciales de voto electrónico.

Así, el mismo artículo 2.2 del Proyecto dispone que el voto "es almacenado en una urna digital protegida criptográficamente". El artículo 3.i) del Proyecto explicita que el elector, una vez emitido el voto, puede descargarse un justificante del sistema "que deje constancia de la efectiva emisión del voto y de su depósito en la urna electrónica (...)". Y el artículo 5.1 del Proyecto, en relación con las funciones atribuidas a las Mesas coordinadoras, prevé que éstas supervisen "el proceso de creación de la urna digital" (letra a)), así como que se encarguen de "la custodia de las claves

criptográficas de acceso a la urna digital que permiten el escrutinio disociado de votos electrónicos" (letra b)).

Como recuerda esta Autoridad en el Dictamen 3/2010, antes citado, los sistemas presenciales y los sistemas de voto remoto son dos modelos de sistemas de votación electrónica claramente diferenciados (FJ IV), que, desde la perspectiva de la protección de datos y del modelo de seguridad, pueden presentar riesgos particulares en las distintas fases clave de desarrollo del procedimiento de votación: fase de identificación y autenticación; fase de emisión del voto; fase de escrutinio y destrucción de la información; fase de control o verificación (FJ VI y VII).

Por este motivo, si, como parece, el Proyecto configura un procedimiento de votación electrónica por Internet como sistema de voto remoto, convendría revisar las referencias hechas en la urna electrónica o digital y sustituirlas, en su caso, por las que correspondan, a efectos de clarificar el modelo configurado por el Proyecto.

IV

Desde la perspectiva de la protección de datos, resulta especialmente relevante el artículo 3 del proyecto, que enumera las garantías del sistema de votación electrónica.

Estas garantías hacen referencia expresa, entre otras cuestiones, a la identificación y autenticación del elector; al carácter secreto del voto ya su integridad y unicidad; a la seguridad del procedimiento de votación electrónica; oa la posibilidad de verificar su correcto funcionamiento, así como de auditarlo.

De entrada, es necesario valorar positivamente estas previsiones en las que se fundamenta el Proyecto desde la perspectiva de la protección de datos y de los elementos de seguridad a tener en cuenta en el diseño y la implantación del procedimiento de votación electrónica que se examina, tal y como exige el propio RGPD, que establece la protección de datos desde el diseño y por defecto (considerando 78 y artículo 25).

Tomando como punto de partida estas garantías, dado que el Proyecto no describe propiamente el procedimiento de votación electrónica, se considera pertinente señalar:

- La importancia de implementar mecanismos y procedimientos suficientemente seguros a la hora de identificar a las personas con derecho a voto y de proporcionarles la credencial que debe permitirles votar por Internet, a efectos de evitar la votación de personas sin derecho a hacerlo, la suplantación de las personas que sí tienen derecho, así como la duplicidad de votos. Es decir, establecer mecanismos que garanticen la correcta identificación y autenticación de los votantes.

Al respecto, el artículo 3 del Proyecto dispone que se garantiza, por un lado, la identificación del elector "mediante los procedimientos de identificación del directorio corporativo" (letra c)), y, por otro, su autenticación robusta, utilizando "el aprovisionamiento seguro de credenciales de directorio corporativo" (letra g)).

En la Memoria justificativa que le acompaña se explicita, al respecto, que "cada votante censado dispone de un certificado/código de acceso a la aplicación donde se realiza la selección personalizada de opciones y candidatos" (apartado III) .

De estas previsiones parece desprenderse que el sistema únicamente permitirá el acceso a la plataforma de votación a aquellas personas previamente dadas de alta en el directorio corporativo de la Generalitat, aspecto a valorar positivamente. Ahora bien, en lo que se refiere al proceso de autenticación de los electores, no queda suficientemente claro si ésta se llevará a cabo mediar

basados en certificados electrónicos o bien a través de mecanismos basados en la atribución de un usuario y contraseña.

En un caso como el examinado, si bien la identificación y autenticación de las personas con derecho a participar en el proceso electoral no plantearía mayores problemas, desde el punto de vista de la protección de datos, si se llevara a cabo mediante sistemas basados en certificados electrónicos o sellos electrónicos, dado que estos mecanismos ofrecen suficientes garantías, tampoco puede descartarse la utilización de mecanismos basados en la atribución de un usuario y contraseña.

Este tipo de mecanismos es el método más extendido para impedir accesos no autorizados a sistemas o contenidos dentro de un sistema de información. Se trata de una medida establecida en estándares internacionales y en certificaciones en materia de seguridad informática (como la Norma ISO/IEC 27001 sobre la gestión de la seguridad de la información) y también reconocida por nuestro ordenamiento jurídico (por ejemplo, en la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (artículo 9)).

Apuntar que, de optar por este mecanismo de identificación y autenticación de los electores, habría que velar por establecer un procedimiento de gestión de las contraseñas que garantice la confidencialidad y la integridad de las mismas.

- La importancia de adoptar las medidas adecuadas para garantizar que el voto que emite la persona que participa en el proceso electoral es único, secreto y anónimo.

Al respecto, el artículo 3 del Proyecto dispone expresamente que el sistema “no permite establecer un vínculo entre el sentido del voto y la persona que lo ha emitido” (letra b)), garantiza asimismo que “la voluntad expresada por el elector es auténtica, inequívoca y que no ha sido alterada ni cualitativa ni cuantitativamente” (letra d)) y que “el elector puede emitir un solo voto y se elimina toda posibilidad de duplicidad o multiplicidad de voto por parte de una misma persona” (letra e)).

También prevé que se garantiza "la seguridad técnica de los procedimientos de transmisión y almacenamiento de la información, con medidas que garanticen la trazabilidad y medidas contra adiciones, sustracciones, manipulaciones, suplantaciones o tergiversaciones del procedimiento de voto" (artículo 3.f)).

Y, al mismo tiempo, que se garantiza "el cumplimiento de la normativa de protección de datos personales, aplicando las medidas de seguridad de nivel alto en atención a la naturaleza de los datos" (artículo 3.k)).

Por su parte, en la Memoria justificativa se explicita (apartado III) al respecto que “los votos son cifrados en los dispositivos de votación y sólo la Mesa electoral única puede reconstruir la clave privada y descifrar los votos. El proceso garantiza que se rompa la correlación entre la identidad de los votantes y los votos descifrados (...). (...) los votos que se almacenan en los servidores están protegidos criptográficamente -cifrados y firmados digitalmente- en todo momento, por tanto, nadie puede manipularlos, ni siquiera los administradores de los sistemas con accesos privilegiados -no tienen acceso en la clave privada-. (...) También se garantiza el voto libre -evitando la coerción o venta de votos- con el recibo de voto que es un código alfanumérico que no revela la opción del voto, es decir, ningún votante puede acreditar ante terceros cuál es el sentido de su voto. (...)”.

Desde la perspectiva de la protección de datos, es necesario valorar positivamente la previsión de implementar este conjunto de medidas de seguridad que abarcarían las diferentes fases del proceso de votación electrónica.

Sin embargo, hay que advertir, en lo que se refiere específicamente a la adopción de “medidas que garanticen la trazabilidad” (artículo 3.f)), que éstas única y exclusivamente deben permitir verificar que

un determinado elector ha ejercido su derecho de voto por el procedimiento de votación electrónica. Es decir, en ningún caso deben permitir establecer un vínculo entre la identidad del elector y el sentido de su voto.

Si bien, cabe decir, el Proyecto prevé que el sistema no permite establecer tal vínculo (artículo 3.b)), la falta de concreción sobre el alcance de la trazabilidad en el presente caso hace necesario advertir de ese eventual riesgo para el secreto del voto y para otros derechos e intereses del afectado, tales como el riesgo de ser coaccionado en base al sentido de su voto.

Dicho esto, recuerda, en este punto, que el RGPD configura un sistema de seguridad que no se basa en los niveles de seguridad básico, medio y alto que se preveían en el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre, sino al determinar, a raíz de una previa valoración de los riesgos, qué medidas de seguridad son necesarias en cada caso (considerando 83 y artículo 32).

Por este motivo, convendría modificar la redacción dada en la letra k) del artículo 3 del Proyecto, en el que se prevé la aplicación de "medidas de seguridad de nivel alto", a efectos de utilizar una terminología adaptada a la RGPD.

En este sentido, se sugiere una redacción similar a la siguiente:

"k) Cumplimiento de la normativa en materia de protección de datos personales, aplicando las medidas técnicas y organizativas que resulten necesarias, atendiendo a la naturaleza de los datos ya la gravedad y probabilidad de los riesgos para los derechos y libertades de las personas electoras. "

Recuerde también que, en el caso de las administraciones públicas, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero, que, actualmente , está siendo objeto de revisión.

En este sentido, la LOPDDDD, antes citada, dispone que:

> "Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.
>
> 1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de las datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.
>
> 2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetos al Derecho privado.
>
> En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad."

Señalar que, entre los responsables del tratamiento incluidos en el artículo 77.1 del LOPDDDD, al que expresamente hace referencia esta DA1a, se encuentran las administraciones de las comunidades autónomas, así como sus organismos públicos y entidades de derecho público, entre otros.

Por tanto, hay que tener presente que, en el presente caso, en que el Proyecto prevé el tratamiento de datos del personal de administración y técnico al servicio de la Administración de la Generalidad de Cataluña, la aplicación de las medidas de seguridad establecidas en el Esquema Nacional de Seguridad resultará obligatoria.

V

Todavía en relación con este artículo 3 del Proyecto, conviene también señalar que este precepto no concreta las condiciones en las que se almacenarán los datos personales vinculados al procedimiento de votación electrónica, más allá de indicar la adopción de medidas de seguridad "técnicas " al respecto (letra f)), que, por lo que se desprende de la Memoria justificativa, consisten en proteger criptográficamente a los servidores. Se desconoce sin embargo si se trata de servidores propios o de terceros, así como su ubicación.

Por este motivo, se recuerda la necesidad de valorar la existencia de un posible encargo del tratamiento (artículo 4.8) RGPD), por ejemplo, en caso de contratar con un tercero la prestación de servicios de alojamiento o almacenamiento de la información relacionada con el procedimiento de votación electrónica, incluidos servicios que operan en la nube. De ser así, debería formalizarse un contrato de encargo del tratamiento en los términos establecidos en el artículo 28.3 del RGPD.

También debería valorarse la existencia de posibles transferencias internacionales de datos (en adelante, TID), por ejemplo, en caso de que los datos se almacenen en servidores ubicados fuera del ámbito territorial de aplicación del RGPD (artículo 3) . De ser así, debería tenerse en consideración que las TID se encontrarían sometidas al régimen previsto en los artículos 44 a 50 del RGPD.

Apuntar, al respecto, que el RGPD prevé que la Comisión de la UE puede decidir que un tercer país, un territorio o uno o varios sectores específicos de un país, garantiza un nivel de protección adecuado (artículo 45), por la que cosa no habría inconvenientes en poder realizar la TID, siempre que se cumplan también el resto de principios y obligaciones del RGPD y del LOPDDDD.

A falta de esta decisión de la Comisión, sólo se podría transmitir datos personales a un tercer país si se ofrecen garantías adecuadas y los interesados disponen de derechos exigibles y acciones legales efectivas (el RGPD establece, en este sentido, diferentes mecanismos por considerar que se ofrecen garantías adecuadas, tales como normas corporativas vinculantes, cláusulas tipos, mecanismos de certificación, etc.(artículo 46.2 RGPD)) o bien si concurre alguna de las excepciones previstas en el artículo 49 del RGPD.

Para más información sobre esta cuestión en concreto, puede ser de interés consultar los dictámenes CNS 5/2018 o CNS 6/2018, disponibles en la web de la Autoridad (http://apdcat.gencat.cat/).

VI

El artículo 5 del Proyecto establece, en su apartado 1, las funciones que, en relación con el sistema de votación electrónica, corresponderán a las mesas coordinadoras, que incluyen actuaciones como la supervisión del proceso de creación de la urna digital (letra a)), la custodia de las claves criptográficas de acceso a la urna digital (letra b)) o la resolución de las incidencias tecnológicas (letra c)).

Asimismo, prevé que las mesas coordinadoras contarán con el apoyo de un equipo de expertos, a efectos de obtener el asesoramiento técnico que requieran (apartado 2).

Sin perjuicio de valorar positivamente esta previsión, debe tenerse presente la necesidad de garantizar que el personal que conforme a dichas mesas coordinadoras (artículo 10 Real Decreto 1846/1994) dispondrá de los conocimientos técnicos suficientes para poder desarrollar correctamente las funciones que tienen asignadas. Cabe recordar que un modelo integral de seguridad, en el que se determine qué medidas de seguridad deben aplicarse a partir de un análisis de riesgos en los términos del RGPD (considerantes 83 y 84), exige también la adopción de las medidas organizativas necesarias y la implantación de medidas de formación del personal que debe tratar los datos personales.

VII

El artículo 6 del Proyecto dispone que "la Administración de la Generalidad de Cataluña, a través de los órganos, entes o entidades que tienen atribuidas las competencias en materia de administración electrónica, TIC y ciberseguridad, da asesoramiento y soporte continuo en estas materias a fin de garantizar la seguridad y el correcto funcionamiento de la Plataforma de votación electrónica por Internet en todas las fases del procedimiento de votación electrónica".

Recuerda, al respecto, la necesidad de definir las condiciones en las que participarán estos terceros en el procedimiento de votación electrónica y las consecuencias de esta participación desde el punto de vista de la protección de datos.

Así, hay que tener presente que, en la medida en que la prestación de estos servicios de asesoramiento y apoyo comporte el tratamiento de datos personales por cuenta del responsable del proceso electoral, deberá formalizarse un contrato de encargo del tratamiento en los términos establecidos en el artículo 28.3 del RGPD.

VIII

Por último, valorar positivamente la previsión de informar a los electores del sistema de votación electrónica, del procedimiento de uso y de las medidas de seguridad aplicables mediante la web oficial del proceso electoral (disposición adicional segunda).

Recuerda, al respecto, que esta información también deberá comprender el conjunto de aspectos a los que hace mención el artículo 13 del RGPD y que deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso , en un lenguaje claro y sencillo (artículo 12 RGPD).

Por todo esto se hacen las siguientes,

Conclusiones

Examinado el Proyecto de Decreto de establecimiento del sistema de voto electrónico en los procesos de elecciones a órganos de representación del personal de administración y técnico al servicio de la Administración de la Generalidad de Cataluña, se considera adecuado a las previsiones establecidas en la correspondiente normativa sobre protección de datos de carácter personal, siempre que se tengan en cuenta las consideraciones hechas en este informe.

Barcelona, 16 de enero de 2019