Asociación de delegados y delegadas de protección de datos de Parlamentos

GUÍA BÁSICA DE PROTECCIÓN DE DATOS EN LOS PARLAMENTOS

RESUMEN EJECUTIVO

Esta guía tiene por objeto ofrecer orientaciones básicas a los Parlamentos en materia de protección de datos, desarrollando y dando respuesta de forma práctica a numerosas cuestiones comunes que resultan de la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD), así como de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Este documento está dirigido principalmente a los Parlamentos, como responsables del tratamiento de datos personales que se generan en dichas instituciones, y en especial a aquellas unidades o departamentos que, dentro de la entidad responsable, tratan dichos datos. También está dirigido a aquellos con el rol de encargados, desarrolladores o suministradores, en la medida que proporcionan productos y servicios a los Parlamentos, puesto que también deben cumplir los requisitos exigidos en materia de protección de datos.

Finalmente, pretende ser un instrumento útil para los Delegados de Protección de Datos (DPD) de los citados organismos con el fin de contribuir a un mejor desempeño de sus funciones.

Palabras clave: Parlamentos. Guía práctica. Protección de datos. Datos personales. Consentimiento del interesado. Derechos de los interesados. Responsable del tratamiento. Delegado de Protección de Datos.

Asociación de delegados y delegadas de protección de datos de Parlamentos

ÍNDICE

Asociación de delegados y delegadas de protección de datos de Parlamentos

1. CONCEPTOS BÁSICOS EN MATERIA DE PROTECCIÓN DE DATOS

Diego Molpeceres Sanz, Letrado-DPD del Parlamento de Castilla y León
Isabel Cañas Palacios, Letrada-DPD del Parlamento de Navarra

1.1 ¿Qué es un dato personal?

Entendemos por dato personal toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

También se incluiría como dato personal la dirección personal, la dirección de correo electrónico de una persona física, el número de teléfono solo si se vincula a una persona, la imagen, la voz de una persona, la matrícula de un vehículo, siempre y cuando, sin exigir plazos o esfuerzos desproporcionados, tal dato pudiera permitir la identificación de una persona física.

1.2 ¿Qué es el tratamiento de datos personales?

Por tratamiento de datos personales entendemos cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

1.3 ¿Cuáles son los principios relativos al tratamiento?

Son una serie de criterios que informan y orientan cómo ha de ser el tratamiento de los datos personales y entre ellos figuran: la licitud, lealtad y transparencia; la limitación de la finalidad; la minimización de los datos; la exactitud; la limitación del plazo de conservación; la integridad y confidencialidad y la responsabilidad proactiva.

1.4 ¿En qué consiste la exigencia de licitud del tratamiento?

El tratamiento de los datos personales será lícito en la medida en que se cumpla al menos una de las condiciones que enuncia la normativa en materia de protección de datos: que son las siguientes:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño (no es de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones).

1.5 ¿Qué es un fichero?

Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

1.6 ¿Quién es el responsable del tratamiento?

Se define como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. El responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

1.7 ¿Quién es el encargado de tratamiento?

Se entiende por encargado de tratamiento la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable.

1.8 ¿Quiénes son los destinatarios y terceros en materia de protección de datos?

El destinatario es la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas

será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

El tercero en materia de protección de datos es la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

1.9 ¿Qué es la autoridad de control en materia de protección de datos?

Se conoce por autoridad de control a la autoridad pública independiente establecida por un Estado que se ocupa de supervisar la aplicación y cumplimiento de la normativa de protección de datos, gracias a los poderes de investigación y correctivos que le han sido otorgados.

1.10 ¿Cómo se define el consentimiento del interesado/a?

El consentimiento del interesado/a es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

1.11 ¿Cuáles son los derechos de los interesados/as en materia de protección de datos?

Los derechos de los interesados/as en materia de protección de datos son los siguientes:

- Derecho de acceso del interesado.
- Derecho de rectificación.
- Derecho de supresión o “derecho al olvido”.
- Derecho a la limitación del tratamiento.
- Derecho de oposición.

1.12 ¿En qué consiste el Registro de las actividades de tratamiento?

Es un registro que llevará el responsable y encargados del tratamiento o, en su caso, sus representantes, que deberá incluir, entre otros, los siguientes datos: el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos; los fines del tratamiento; una descripción de las categorías de interesados y de las categorías de datos personales; las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales; etc.

1.13 ¿Qué es la figura del Delegado de protección de datos?

Se trata de una figura clave, que es designada por el responsable y el encargado del tratamiento siempre se den alguno de los supuestos que se indican. Así, entre otros, la

designación es preceptiva si el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.

El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones encomendadas.

El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones.

En cuanto a sus funciones, habrán de corresponderle, entre otras: informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros; supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación; cooperar con la autoridad de control; etc.

2. ADECUACIÓN AL RGPD Y A LA LOPDPGDD DE LOS TRATAMIENTOS DE DATOS DE LOS PARLAMENTOS

2.1 EL PARLAMENTO COMO RESPONSABLE DEL TRATAMIENTO

Laura Seseña Santos, Letrada-ex DPD del Parlamento de Castilla y León

2.1.1 ¿Las instituciones parlamentarias están sujetas a la normativa de protección de datos personales de las personas físicas?

Sí, la institución parlamentaria como todo poder público está vinculada por los derechos y libertades reconocidos en el capítulo segundo de la Constitución, tal y como dispone su artículo 53.1 de la norma fundamental, y toda su actuación debe ser respetuosa con lo establecido al respecto en la propia norma constitucional, y con la legislación que desarrolla estos derechos y regula su ejercicio.

Actualmente la normativa de desarrollo del derecho fundamental a la protección de datos personales de las personas físicas se recoge en una regulación europea, completa y directamente aplicable en todos los Estados miembros, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).

Dicho RGPD ha sido desarrollado y complementado a su vez en el ámbito nacional por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales(LOPDPGDD).

2.1.2 ¿Existe diferencia en cómo incide la protección de datos personales en la actividad del Parlamento dependiendo del tipo de actividad que realice la Cámara, si ésta es parlamentaria o administrativa?

La aplicación de la normativa de protección de datos personales en el ámbito parlamentario en sus actividades de carácter administrativo, esto es aquellas que realiza para la gestión administrativa y de personal de la Cámara, no ofrece especiales peculiaridades a la que se lleva a cabo en el resto de administraciones públicas. Sin embargo, sí que las tiene respecto de las actividades realizadas en el ejercicio de sus funciones parlamentarias en las que también se acometen de uno u otro modo tratamientos de datos personales.

Estas peculiaridades derivan fundamentalmente de dos hechos que están entrelazados: la actividad parlamentaria, salvo excepciones justificadas, se rige por el principio de publicidad y en el Parlamento cuando los parlamentarios ejercitan sus facultades están ejerciendo el derecho fundamental a la participación política, pudiendo constituir ambos, límites al derecho fundamental a la protección de datos personales.

2.1.3 ¿Cómo se resolverá el conflicto en el que pueden entrar el derecho fundamental a la participación política de los parlamentarios y el derecho fundamental a la protección de datos personales de las personas físicas en el ejercicio por los parlamentarios de sus funciones?

Dentro de la actividad parlamentaria nos podemos encontrar con dos derechos fundamentales en conflicto: el de participación política y el de protección de datos personales, constituyendo ambos, recíprocamente, cuando confluyen, límites respectivos a su ejercicio.

Como todos los derechos fundamentales no son derechos ilimitados que no puedan verse restringidos cuando existan otros derechos del mismo carácter o bienes jurídicos constitucionalmente protegidos con los que confluyan. Este carácter limitado del derecho lo reconoce expresamente el Considerando 4 y el artículo 23 del RGPD respecto del derecho fundamental a la protección de datos, y, también, los reglamentos parlamentarios en su regulación prevén alguna limitación del derecho de participación política por la necesidad de conjugar su ejercicio con la existencia de otros derechos fundamentales, como es el caso del derecho de protección de datos.

2.1.4 ¿Qué figura adoptan las Cámaras parlamentarias en los tratamientos de datos personales de las personas físicas en el ejercicio de sus funciones?

Las Cámaras parlamentarias españolas, de conformidad con la definición dada por el artículo 4 apartado 7 del RGPD, se han constituido en el ejercicio de sus actividades desde el punto de vista de la protección de datos personales como responsables del tratamiento pues son autoridades públicas que llevan a cabo procedimientos sobre datos personales y determinan sus fines y los medios para realizarlos.

2.1.5 La nueva normativa europea sobre la protección de datos personales que ha instaurado el RGPD y que ha sido desarrollada en España por la LOPDPGDD ¿qué ha supuesto para los parlamentos españoles?

Las instituciones parlamentarias han tenido que abordar, como el resto de las administraciones públicas y órganos constitucionales y análogos en el ámbito de las Comunidades Autónomas, en aplicación del principio de responsabilidad proactiva, una serie de actuaciones que vienen recogidas a lo largo del RGPD y en la LOPDPGGD y que han conllevado la implantación de lo que se puede denominar una cultura de la protección de datos personales en la organización parlamentaria, una visión global de la misma atendiendo a las actuaciones que se realizan y los tratamientos de datos personales que se generan para llevarlas a cabo, apreciando los riesgos y efectos de los mismos.

Ha sido fundamental, en el ejercicio por el parlamento de esta responsabilidad proactiva un análisis profundo y una evaluación global del tratamiento de datos que se estaba realizando, y que tenía como punto de partida los ficheros de tratamiento que habían sido creados bajo la vigencia de la anterior normativa. De manera simultánea se ha abordado desde las Secretarias Generales de las Cámaras el estudio de las obligaciones en materia de protección de datos exigidas por el RGPD y posteriormente por la LOPDPGDD , procediéndose o bien a su actualización con el contenido exigido por la nueva normativa, o bien a su cumplimiento si se trata de la imposición de una nueva obligación como es el

caso de la creación de la figura del Delegado de Protección de Datos, adoptándose, en consecuencia y en su caso, los correspondientes acuerdos por las Mesa de las Cámaras, al ser éstas los órganos a quienes les corresponde tomar cuantas decisiones y medidas requiera la organización del trabajo y el régimen y gobierno interiores de la Cámara.

2.1.6 ¿Cuáles son en concreto estas medidas organizativas, técnicas y jurídicas, que se han debido adoptar por las instituciones parlamentarias para la adaptación de su funcionamiento y actividad al RGPD y a la LOPDPGDD?

En una simple enumeración de las mismas y señalando que son coincidentes con las que en general han debido asumir los responsables de tratamiento son:

- Creación de la figura del Delegado de Protección de Datos Personales en cada una de las Cámaras de las Cortes Generales y en cada uno de los Parlamentos.
- Creación y mantenimiento actualizado de un Registro de Actividades de tratamiento que sustituye a la notificación de los ficheros de tratamiento de datos a las autoridades de control.
- Obligación de transparencia del responsable del tratamiento.
- Cumplimiento del deber de facilitar a los interesados o afectados por los tratamientos de datos personales el ejercicio de los derechos que le son reconocidos en los artículos 15 a 22 del RGPD desarrollados a su vez en los artículos 12 a 18 de la LOPDPGDD.
- Obligación de realizar análisis de riesgos de seguridad de los datos personales que se tratan y de valorar los efectos que ese tratamiento puede ocasionar en la privacidad, intimidad y libertad de los sujetos que pueden directa o indirectamente verse afectados. El resultado determinará cuales son los requisitos de privacidad desde el diseño y la protección de datos por defecto, procesos previstos a los que se refiere el artículo 25 del RGPD.
- Como consecuencia de los anteriores procesos, existe la obligación de adoptar las medidas técnicas y organizativas apropiadas que garanticen la seguridad de los tratamientos y por ende los derechos de los interesados. La Disposición Adicional Primera de la LOPDPGDD establece que los responsables enumerados en el artículo 77.1 de la ley orgánica, entre los que se encuentran todas las Cámaras parlamentarias españolas, ya que se refieren en él a todos los órganos constitucionales y las instituciones de las comunidades autónomas análogas a los mismos, dispone que deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan en el Esquema Nacional de Seguridad, actualmente establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Por último, la obligación de notificar las violaciones de seguridad de los datos personales que se produzcan tanto a las autoridades de control como a los interesados que han podido ser comprometidos (artículos 33 y 34 RGPD).

2.1.7 ¿Las Cámaras parlamentarias deben publicar el denominado Inventario de Actividades de Tratamiento?

El Inventario de Actividades de Tratamiento es uno de los medios para garantizar la transparencia de los poderes públicos en el tratamiento de datos personales de las personas físicas que realizan.

El artículo 31.2 de la LOPDPGDD establece que los sujetos enumerados en el artículo 77.1 de la ley orgánica, entre los que se encuentran las Cortes Generales y los parlamentos autonómicos (apartado a) de este artículo 77.1 que se refiere a "a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos."), harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal. Esta publicidad que da transparencia a la información del Registro de Actividades de Tratamiento, coincidente, salvo en algún extremo, además con la que debe facilitarse a cualquier interesado del que se traten sus datos, debe constar en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

2.1.8 ¿Están sometidas las Cámaras parlamentarias al mismo régimen sancionador que el resto de los responsables de tratamientos de datos personales?

Las Cámaras parlamentarias se encuentran sometidas al mismo régimen sancionador que el resto de administraciones públicas por las infracciones cometidas respecto de las obligaciones previstas en el RGPD. El legislador comunitario ha determinado de manera general que las autoridades de control disponen de toda una serie de poderes correctivos que son aplicables a todos los responsables de tratamientos (artículo 58.2 RGPD) por los incumplimientos del RGPD y solo ha establecido en su artículo 83.7 la posibilidad de que los Estados miembros excepcionen a las autoridades y organismos públicos responsables del tratamiento de que le sean impuestas multas administrativas. Por esta razón, a la institución parlamentaria se le aplica el mismo régimen que al resto de administraciones, a pesar de la autonomía que constitucionalmente tienen reconocida las Cámaras parlamentarias, para garantizar su independencia de injerencias indebidas del ejecutivo, y de que las agencias de protección de datos, si bien son administraciones independientes no dejan de ser administraciones dentro de la órbita del gobierno, cuyo Presidente y su Adjunto son nombrados por éste.

El artículo 77.2 de la LOPDPGDD establece que cuando los responsables enumerados en su apartado 1, entre los que se encuentran las Cámaras, cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido excluyendo la posibilidad de imponerles multas administrativas previstas en el artículo 58.2 i) y 83 del RGPD.

2.2 EL DELEGADO DE PROTECCIÓN DE DATOS EN EL ÁMBITO PARLAMENTARIO

Iñaki González-Pol González, DPD del Parlamento de Andalucía

2.2.1 ¿Es obligatoria la designación de un Delegado de Protección de Datos por parte de Parlamentos y Asambleas legislativas?

Sí, en el caso de los Parlamentos y Asambleas legislativas la designación de un DPD resulta obligatoria.

2.2.2 ¿Qué cualidades profesionales debe tener un DPD?

Para ser designado DPD se requiere:

- Tener conocimientos especializados en la legislación nacional y europea en materia de privacidad y protección de datos.
- Tener conocimiento técnico de los sistemas de Tecnologías de la Información.
- Conocer la entidad, su estructura organizativa, su funcionamiento, los sistemas de información que emplea, las necesidades de seguridad y protección de datos y, cómo no, las normas y procedimientos por los que se rige.

2.2.3 ¿El DPD debe ser licenciado en Derecho?

No. El RGPD requiere tener conocimientos especializados del Derecho y la práctica en materia de protección de datos, si bien no obliga a tener la titulación de licenciado en Derecho.

2.2.4 ¿Cuánta experiencia se recomienda tener para ser designado DPD en el ámbito parlamentario?

En el ámbito parlamentario los DPD deberían contar con al menos 3 años de experiencia relevante, siendo recomendable que la misma se incremente hasta los 7 años en aquellos casos en los que se cuente con un volumen importante de operaciones tratamientos.

La experiencia relevante incluye la experiencia en la implementación de los requisitos de protección de datos y la experiencia dentro de la institución / organización designada, lo que se traduce en el conocimiento de cómo funciona. No debe entenderse necesariamente como experiencia específica como DPD, sino que cabría la generada en la redacción e implementación de políticas en la organización relevante (o una organización similar), o en áreas relevantes como TI.

2.2.5 Más allá del conocimiento y de la experiencia, ¿qué habilidades personales deben tener los DPD?

El DPD debe tener las siguientes habilidades para el desarrollo adecuado de sus funciones:

- Habilidades personales: integridad, alta ética profesional, iniciativa, organización, actitud firme e insistente, discreción, capacidad para soportar presiones y dificultades, interés en la protección de datos y motivación para ser un DPD.
- Habilidades interpersonales: comunicación, negociación, resolución de conflictos, capacidad para construir relaciones de trabajo.

De este modo, el proceso de designación de un DPD parlamentario debería articularse de tal modo que permitiese evaluar la tenencia de estas habilidades personales e interpersonales.

2.2.6 ¿Es posible la designación de un DPD compartido entre varias instituciones?

El artículo 37.3 del RGPD permite la designación de un DPD que preste servicio para varias autoridades u organismos públicos, si bien teniendo en cuenta el tamaño y la estructura organizativa de aquellas.

Esto podría llevar a cuestionar la oportunidad de designar un DPD conjunto para varios Parlamentos si bien la fórmula podría disponerse entre una Cámara legislativa y organismos de extracción parlamentaria de tamaño reducido y estructura organizativa afín a aquella, cuando resulte debidamente justificado.

2.2.7 ¿El DPD debe formar parte de la plantilla de personal del Parlamento o Asamblea legislativa o puede ser externo?

El artículo 37.6 del RGPD prevé que "*El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios*".

No obstante, se estima que con carácter general un DPD interno podría tener un conocimiento más adecuado de la organización, de su estructura y de su funcionamiento.

2.2.8 ¿Puede el DPD desarrollar funciones adicionales a las de su cargo?

El DPD puede desarrollar sus funciones bien a tiempo completo, bien a tiempo parcial, compatibilizándolas con otros cometidos que tenga atribuidos por la organización.

No obstante, debe tenerse presente que con un DPD a tiempo parcial se podrían dar situaciones de conflicto de interés o que hicieran prevalecer las otras funciones asignadas en detrimento de las de DPD.

2.2.9 ¿Cuáles son las funciones del DPD?

El DPD se encarga de la aplicación de la legislación sobre privacidad y protección de datos y sus funciones se recogen en el artículo 39 del RGPD y en los artículos 36 y 37 de la

LOPDPGDD.

Tiene como mínimo las siguientes funciones:

a) informar y asesorar al responsable, o al encargado del tratamiento, y a las personas autorizadas para tratar los datos personales bajo su autoridad directa, en virtud del RGPD, la LOPDPGDD y de otras disposiciones de protección de datos de la UE o de sus Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el RGPD, la LOPDPGDD y en otras disposiciones de protección de datos de la UE o de sus Estados miembros, y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales;

c) supervisar la asignación de responsabilidades;

d) supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento;

e) supervisar las auditorías correspondientes;

f) ofrecer el asesoramiento que se le solicite acerca de las evaluaciones de impacto relativas a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD;

g) cooperar y actuar como interlocutor con la autoridad de control para las cuestiones relativas al tratamiento de datos personales, incluida la consulta previa a que se refiere el artículo 36 del RGPD.

2.2.10 ¿Es el DPD la persona responsable de los posibles incumplimientos que pueda haber en materia de protección de datos?

No. El artículo 39.1.b) encomienda a los DPD, entre otras obligaciones, la de supervisar la observancia del RGPD, pero eso no significa que el DPD sea personalmente responsable de cualquier inobservancia de la normativa de protección de datos.

El RGPD establece claramente que es el responsable del tratamiento, es decir, el Parlamento o la Asamblea legislativa, quien está obligado a aplicar "*medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento*" (artículo 24.1 del RGPD).

2.2.11 ¿Es el DPD independiente y autónomo para el desarrollo de sus funciones?

El DPD, sea o no empleado del responsable del tratamiento, debe estar en condiciones de desempeñar sus funciones y cometidos de manera independiente y con el suficiente grado de autonomía, de tal modo que los responsables o encargados del tratamiento están obligados a garantizar que "*no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones*" (artículo 38.3 del RGPD).

De este modo, no debe instruirse al DPD sobre cómo abordar un asunto, ni qué resultado debería lograrse, o cómo investigar una queja o si se debe consultar a la autoridad de control, por ejemplo. Asimismo, no se debe intentar condicionar al DPD para que adopte

una determinada postura con respecto a un asunto concreto relacionado con la normativa de protección de datos.

Por contra, se debe garantizar que el DPD pueda expresar con claridad su opinión y, en su caso, sus discrepancias, reportándolas al más alto nivel de dirección en el seno de los Parlamentos.

2.2.12 ¿Puede ser destituido por el desempeño de sus funciones?

El DPD no podrá ser destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones.

Entre estas sanciones prohibidas por el legislador europeo se incluiría no sólo la destitución sino también la falta de ascenso o su dilación, el impedimento de la promoción profesional, la denegación de prestaciones que otros empleados reciban, etcétera.

2.2.13 ¿A quién debe rendir cuentas el DPD en el seno de los Parlamentos y Asambleas legislativas?

El DPD debe poder relacionarse con niveles jerárquicos que tengan la capacidad de adoptar o promover decisiones basadas en las recomendaciones, propuestas o evaluaciones que realice, lo que en el ámbito de la administración parlamentaria alcanzaría a la Secretaría General, al Letrado/a Mayor y a la Mesa.

2.2.14 ¿Qué recursos deben facilitarse al DPD por parte de los Parlamentos y Asambleas legislativas?

El artículo 38.2 del RGPD prevé que la organización respalde a su DPD "*facilitando los recursos necesarios para el desempeño de [sus] funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados*".

De este modo, procede que por parte de los Parlamentos y Asambleas legislativas:

- Se preste apoyo activo a la labor del DPD por parte de la dirección (Secretaría General, Letrado/a Mayor, Mesa del Parlamento).
- Se le asigne tiempo suficiente para que el DPD cumpla con sus funciones, lo cual es particularmente importante cuando se designa un DPD interno a tiempo parcial o cuando el DPD externo lleva a cabo la protección de datos de manera complementaria a otras obligaciones.
- Se le faciliten los recursos financieros, de infraestructura (locales, instalaciones, equipos) y de personal necesarios para el desarrollo adecuado de los cometidos propios del DPD.
- Se comunique formalmente la designación del DPD a todo el personal del Parlamento para garantizar que su existencia y funciones sean oportunamente conocidas.
- Se facilite el acceso necesario a otros servicios como recursos humanos, servicios jurídicos, TI, seguridad, etc., de modo que los DPD puedan recibir el apoyo, las aportaciones y la información necesaria para el desarrollo de sus desempeños.

- Se dé a los DPD la oportunidad de mantenerse al día con respecto a los avances que se den en el ámbito de la protección de datos, garantizándoles una formación adecuada.

2.3 EL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO PARLAMENTARIO

2.3.1 DECLARACIONES DE ACTIVIDADES Y BIENES: PUBLICIDAD ACTIVA Y PROTECCIÓN DE DATOS

Catalina Escuin Palop, Letrada de las Cortes Valencianas

2.3.1.1 ¿Qué son las declaraciones de actividades y de bienes patrimoniales?

Las declaraciones de actividades y de bienes patrimoniales se pueden definir como la acreditación por los cargos electos de ejercer su función de acuerdo con la legislación reguladora de las incompatibilidades y, en su caso, de conflicto de intereses.

2.3.1.2 ¿Tienen que ser publicadas las declaraciones de actividades y de bienes patrimoniales?

En cada Cámara legislativa, estatal (Congreso y Senado) o autonómicas, sus miembros están obligados a cumplimentar la declaración de actividades y de bienes patrimoniales y la institución de la que son miembros está obligada a darles publicidad en los términos previstos en sus normas internas.

La presentación de las declaraciones de actividades por los parlamentarios está sometida a plazo y procede realizarla, al acceder al cargo, cuando varían las actividades inicialmente declaradas o el régimen de dedicación y en algunas asambleas legislativas, también tras el cese.

Por lo que se refiere a las declaraciones de bienes patrimoniales la regla general es su presentación con carácter anual y al terminar el mandato.

2.3.1.3 ¿Qué es el Registro de Intereses de las asambleas legislativas?

Estos registros tienen naturaleza administrativa, pero están dotados de ciertas especialidades por encontrarse bajo la autoridad de un órgano parlamentario (Presidencia o Mesa) y contener, como regla general, información personal suministrada, en cada legislatura, por los representantes populares, siendo su función la inscripción, el depósito y la cancelación de las declaraciones de actividades y de bienes de los parlamentarios, aunque en alguna Cámara este Registro no incluye las declaraciones de bienes patrimoniales.

Los registros de intereses de las asambleas legislativas suelen contener también las copias de las autoliquidaciones del Impuesto sobre la Renta de las Personas Físicas y, en su caso, del Impuesto sobre el Patrimonio.

Estas declaraciones se ajustan al modelo o los modelos elaborados por la respectiva Mesa, que pueden ser independientes para cada tipo de declaración o incluir ambas

declaraciones en el mismo modelo.

La base jurídica de las declaraciones excluidas del Registro de Intereses se encuentra en una norma con rango de Ley como el Reglamento y su finalidad parece que puede ser la de cumplir con la obligación de publicidad; esto es, la transparencia. Este tratamiento está sometido a los mismos principios y obligaciones que el efectuado a través del Registro de Intereses, que se dan aquí por reproducidos.

2.3.1.4 ¿Está el Registro de Intereses sometido a la publicidad activa?

Sí, en la mayor parte de los parlamentos la publicidad activa de las declaraciones de actividades y de bienes patrimoniales está implantada.

En las Cámaras legislativa la información activa de las declaraciones está legitimada por el respectivo Reglamento, la Ley Electoral o por la Ley de transparencia, que cubren la reserva de Ley requerida para imponer la obligación de informar por la Cámara, para determinar el medio o los medios de publicidad activa y para someter el cumplimiento de esa obligación a un plazo.

2.3.1.5 ¿Incide la normativa estatal y autonómica en materia de transparencia en los parlamentos?

Las leyes de transparencia autonómica presentan un diferente grado de incidencia en el régimen de publicidad activa de las asambleas legislativas, pero en todo caso y sin diferencias, estas leyes son supletorias al régimen de publicidad de las declaraciones previsto en los reglamentos parlamentarios y, en su caso, en la correspondiente Ley electoral.

2.3.1.6 ¿Cómo se configura las declaraciones actividades y de bienes patrimoniales?

La presentación de las declaraciones al inicio de la legislatura se configura por los reglamentos parlamentarios como un deber de los parlamentarios que no condiciona el acceso al pleno ejercicio del cargo o como un deber de especial valor por constituir presupuesto de necesario cumplimiento para alcanzar la condición plena de miembro del Parlamento. De estas alternativas la utilizada con carácter casi general es la indicada en segundo lugar. Además, algunos reglamentos parlamentarios tipifican la falta de presentación o la presentación incompleta de las declaraciones como infracción disciplinaria.

2.3.1.7 ¿Cuál es el órgano responsable para ordenar la difusión de las declaraciones de actividades de bienes patrimoniales?

El órgano competente para ordenar la difusión de las declaraciones de actividades de bienes patrimoniales sometida a información activa es la persona que ocupa la presidencia o la Mesa de la Cámara, dependiendo de la concreta previsión reglamentaria.

2.3.1.8 ¿Existe el derecho de acceso pasivo a las declaraciones de actividades y bienes patrimoniales sometidas a información activa?

Cuando hay obligación de publicidad activa, la solicitud de información se puede plantear bien porque los documentos no están publicados o porque es difícil su localización.

Si la información está publicada, el parlamento cumpliría con la indicación al solicitante de la URL especifica que conduce a esta publicación

Ahora bien, de no haber publicidad previa, hay que tener en cuenta que la decisión de ofrecer la información al solicitante corresponde a un órgano parlamentario, el competente de acuerdo con el Reglamento, para ordenar su publicidad.

2.3.1.9 ¿Dónde se regula el procedimiento de acceso pasivo a las declaraciones no sometidas a información activa?

Cuando el Reglamento no contenga previsión de publicidad activa, la base jurídica para la cesión o comunicación de las declaraciones a terceros solicitantes se encuentra en la Disposición adicional décima de la LOPGDD.

2.3.1.10 ¿Es compatible la publicidad de la declaración de actividades y de bienes con la legislación de protección de datos personales?

La normativa en materia de protección de datos permite la publicidad activa de las declaraciones de los parlamentarios, sin perjuicio de que su publicidad pueda requerir algún tipo de adaptación.

2.3.1.11 ¿Pueden ser divulgados los datos identificativos, DNI y firma en la declaración de actividades y de bienes?

El nombre y los apellidos del parlamentario, como dato identificativo, en principio no plantea problema de inclusión en la divulgación de las declaraciones dada la finalidad de información activa que cumplen y su condición de autoridad.

Pero hay dos datos personales que requieren una referencia particular por ser datos de carácter personal: número del DNI y a la firma.

En ningún caso se debe publicar el nombre y apellidos de una manera conjunta con el numero completo del DNI fuera de los supuestos necesarios, así de la publicidad de las declaraciones se debe excluir el número del DNI, total o parcialmente, por exceder de la esfera pública de los parlamentarios y carecer de justificación para cumplir la finalidad de transparencia ya que la identificación de los declarantes se cumple dando publicidad al nombre y a los apellidos.

Por lo que se refiere a la firma manuscrita hay que tener en cuenta que la condición de los firmantes de las declaraciones tiene relevancia en la medida que garantiza su autoría por lo que, a diferencia de la inclusión del número del DNI, la inclusión de la firma manuscrita en la publicidad de las declaraciones puede prevalecer sobre la protección de datos en cuanto dota al documento difundido de la máxima integridad. No obstante, no es posible ignorar que la publicación de la firma manuscrita puede generar una situación de riesgo ya que la misma puede ser reproducida por terceros.

Por este motivo, una buena práctica sería la supresión de la firma manuscrita de la autoridad siempre que conste en el documento publicado algún tipo de mención que ponga de manifiesto que el original ha sido efectivamente firmado.

Por lo que se refiere a las declaraciones con firma electrónica también procede la adopción de cautelas pues el código seguro de verificación (CSV) del documento firmado electrónicamente deberá ser ocultado cuando su acceso pueda permitir el conocimiento de algún dato personal del parlamentario, no revelado en el documento, como, por ejemplo, el número del DNI.

2.3.1.12 ¿Hay límites a la publicidad de la declaración de bienes?

Cada asamblea legislativa debe valorar, si su Reglamento impone una obligación a la Cámara de publicar de forma íntegra las declaraciones de bienes o confiere cierto margen de apreciación para decidir sobre la información que puede ser publicada y cumplir la finalidad de transparencia.

Las previsiones reglamentarias y la normativa sobre protección de datos, permiten excluir de la publicidad: los datos especialmente protegidos, los datos que puedan revelar la localización de los bienes y los que arriesguen en exceso la privacidad y la seguridad de sus titulares o los datos referidos a terceras personas físicas, diferentes de la persona que ocupe el cargo representativo.

En suma, aquella información que, aunque conste en la declaración, pueda resultar innecesaria para evaluar la situación patrimonial del representante popular o suponga una intromisión excesiva en su privacidad.

2.3.1.13 ¿Cuáles son los principios que rigen el tratamiento de estos datos personales?

Los tratamientos que realizan las asambleas legislativas se rigen por la normativa reguladora de la protección de datos por lo que se les aplicarán los siguientes principios: lealtad y transparencia, minimización de datos personales, limitación temporal del tratamiento, compatibilidad del tratamiento con fines de investigación histórica y exactitud de los datos utilizados en el tratamiento.

2.3.1.14 ¿Hay que informar a los parlamentarios del tratamiento de sus datos personales?

Sí, las Cámaras legislativas están obligadas a proporcionar a los parlamentarios la información prevista en la normativa en materia de protección de datos consistente en: a) la identidad del responsable del tratamiento b) la finalidad del tratamiento y c) los derechos que les asisten frente al tratamiento, comunicándoles una dirección electrónica u otro medio que les permita acceder de forma sencilla e inmediata al resto de la información requerida, que sería la siguiente:

- Los datos de contacto del responsable del tratamiento;
- La identidad y los datos de contacto del delegado de protección de datos.
- La base jurídica del tratamiento; esto es, la norma con rango de ley que impone a la Cámara la realización del tratamiento.
- El derecho a presentar una reclamación ante la AEPD o ante la correspondiente

autoridad autonómica.

- La obligación del cargo representativo de presentar las declaraciones y las consecuencias que le puede deparar su falta o inadecuada presentación.

La información básica se puede ofrecer, generalmente, en los modelos de las declaraciones y por lo que se refiere a la información detallada, se puede facilitar por las asambleas legislativas mediante la comunicación a los parlamentarios del acceso electrónico al Registro de Actividades de Tratamiento.

2.3.1.15 ¿Hay que incluir el tratamiento de los datos relativos a los parlamentarios en el inventario de actividades de tratamiento (RAT)?

Sí, las Cámaras legislativas, están obligadas a publicar su inventario de actividades de tratamiento, por medios electrónicos y a comunicar al delegado de protección de datos cualquier adición, modificación o exclusión producida en el mismo.

En el inventario de las actividades de tratamiento deben constar respecto al Registro de Intereses los siguientes datos:

- El nombre y los datos de contacto del responsable y del delegado de protección de datos.
- La política de seguridad adoptada por cada cámara legislativa que deberá adecuarse a las previsiones del Esquema Nacional de Seguridad
- La finalidad asignada al tratamiento de las declaraciones incluidas en Registro de Intereses; esto es, la comprobación de que el parlamentario o la parlamentaria no ostenta cargo incompatible y que están en condiciones de ejercer su función de acuerdo con la legalidad.
- Las categorías de datos tratados.
- El medio o los medios por los que se someterá a información activa su declaración o sus declaraciones.
- El plazo previsto para la cancelación del tratamiento y cuando no se encuentre previsto normativamente, los criterios de supresión previstos por el responsable del tratamiento.

2.3.2 LA GESTIÓN DOCUMENTAL Y LA PROTECCIÓN DE DATOS

Esther de Alba Bastarrechea, Letrada-DPD de la Asamblea de Madrid

2.3.2.1 ¿Existen criterios de normalización de la gestión documental relacionados con la protección de datos?

La gestión documental está sometida a normalización a través de la Norma ISO 15489:2016. Ante la normativa sobre transparencia y protección de datos, es preciso que la gestión documental incluya en la normalización de sus procesos la rendición de cuentas, en este sentido, es necesario definir los procesos para evitar la omisión de datos o la pérdida o manipulación de estos.

2.3.2.2 ¿Cuál es el aspecto más importante de la protección de datos vinculado a la gestión documental?

La protección de datos es fundamental para prevenir y adoptar medidas que eviten el acceso no autorizado, la pérdida de información y garantizar la privacidad de la información sensible y confidencial manejada en los documentos.

2.3.2.3 ¿Cómo se puede asegurar la integridad de los documentos en la gestión documental?

A través de la implementación de controles de versiones, auditorías regulares, y el uso de firmas digitales y técnicas de hash para verificar que los documentos no han sido alterados.

2.3.2.4 ¿Por qué es importante integrar la protección de datos desde el diseño en la gestión documental?

Es importante porque garantiza que la privacidad y la seguridad de la información se consideren desde el principio, minimizando riesgos, cumpliendo con la normativa y protegiendo los derechos de los individuos.

2.3.2.5 ¿Cómo se puede asegurar la minimización de datos en la gestión documental?

Se puede asegurar identificando los datos estrictamente necesarios para cada proceso y evitando la recopilación de información innecesaria.

2.3.2.6 ¿Cómo garantizamos la transparencia en el manejo de datos documentales?

La transparencia se garantiza mediante políticas claras y accesibles sobre la recopilación, el uso y la retención de datos e informando adecuadamente a los usuarios y empleados sobre cómo se tratan sus datos.

2.3.2.7 ¿De qué manera se puede incorporar la anonimización y seudonimización en los documentos?

Estas técnicas se pueden incorporar transformando datos personales en datos que no puedan atribuirse a una persona específica sin información adicional.

2.3.2.8 ¿Cuáles son las principales amenazas a la protección de datos en la gestión documental?

Las principales amenazas traen causa del acceso no autorizado, el robo de información, la pérdida de datos debido a fallos técnicos, el malware, los ciberataques y el manejo inadecuado de los documentos.

2.3.2.9 ¿Qué herramientas tecnológicas pueden ayudar a proteger los datos en la gestión documental?

Tecnologías como el cifrado de datos, la autenticación multifactor, los sistemas de gestión de identidad y acceso (IAM), el almacenamiento seguro en la nube, y las soluciones de copia de seguridad y recuperación de datos pueden ser fundamentales para proteger los datos, también es muy importantes contar con instrumentos de software de detección y prevención de intrusiones.

Los avances tecnológicos, como la inteligencia artificial y la computación en la nube, pueden ofrecer nuevas herramientas y métodos para mejorar la protección de datos. Bien es cierto que también son susceptibles de presentar vulnerabilidades que deben ser abordados de manera proactiva mediante la revisión y la actualización continuas de las medidas de seguridad.

2.3.2.10 ¿Cuáles son las prácticas recomendadas existen para asegurar la protección de datos en la gestión documental?

- Implementar políticas de acceso basadas en roles.
- Capacitar a los empleados en la importancia de la seguridad de los datos.
- Realizar auditorías regulares y evaluaciones de riesgos.
- Utilizar software de gestión documental con funciones de seguridad avanzadas.
- Mantener copias de seguridad periódicas de los documentos críticos.
- Aplicar medidas de cifrado tanto en tránsito como en reposo.

2.3.2.11 ¿Qué es el control de acceso basado en roles?

El control de acceso basado en roles asegura que solo las personas con los permisos adecuados puedan acceder a documentos específicos, limitando la exposición de información sensible y reduciendo el riesgo de filtraciones.

2.3.2.12 ¿Qué son las políticas de retención de documentos y por qué son importantes?

Las políticas de retención de documentos establecen cuánto tiempo se deben conservar los documentos antes de ser eliminados. Son importantes para asegurar el cumplimiento legal, la eficiencia operativa y la protección de datos personales.

2.3.2.13 ¿Cuál es el papel del cifrado en la gestión documental?

El cifrado protege la información almacenada y transmitida, asegurando que solo los usuarios autorizados puedan acceder y leer los documentos, reduciendo el riesgo de acceso no autorizado.

2.3.2.14 ¿Cómo ayudan las copias de seguridad en la gestión documental?

Las copias de seguridad garantizan que, en caso de pérdida de datos por un ciberataque o falla del sistema, la información pueda ser recuperada, minimizando el impacto en las operaciones de la organización.

2.3.2.15 ¿Cómo influye la capacitación del personal en la ciberseguridad de la gestión documental?

La capacitación del personal en ciberseguridad aumenta la conciencia sobre las amenazas y las mejores prácticas, ayudando a prevenir errores humanos que pueden llevar a brechas de seguridad.

2.3.2.16. ¿Qué normativas y estándares existen para la ciberseguridad en la gestión documental?

Existen diversas normativas y estándares como ISO 27001, GDPR, y NIST, que proporcionan directrices para implementar prácticas de ciberseguridad efectivas en la gestión documental.

2.3.2.17. ¿Cómo se puede evaluar la efectividad de las medidas de ciberseguridad en la gestión documental?

La efectividad puede evaluarse mediante auditorías de seguridad regulares, pruebas de penetración, análisis de vulnerabilidades, y monitoreo continuo de actividades sospechosas.

2.3.2.18. ¿Qué papel pueden jugar las tecnologías emergentes en la ciberseguridad de la gestión documental?

Tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y el blockchain están revolucionando la ciberseguridad, proporcionando herramientas avanzadas para la detección de amenazas, la gestión de identidades, y la trazabilidad de documentos.

2.3.2.19. ¿Cuál es el papel de la gestión de riesgos en la protección de datos?

La gestión de riesgos es fundamental para identificar, evaluar y mitigar las amenazas a la seguridad de los datos. Esto implica realizar evaluaciones de riesgos regulares, implementar controles adecuados y mantener un plan de respuesta a incidentes para abordar posibles brechas de seguridad de manera eficaz y rápida.

2.3.2.20. ¿Cuáles son las consecuencias de no proteger adecuadamente los datos en los procesos de gestión documental?

Las consecuencias pueden incluir pérdida de información confidencial, daños a la reputación de una organización, sanciones legales y financieras, pérdida de confianza por parte de la ciudadanía y exposición a fraudes y ciberataques.

2.3.2.21. ¿Cómo influye la cultura organizacional en la seguridad de la información en la gestión documental?

Una cultura organizacional que valora la seguridad de la información fomenta buenas prácticas entre los empleados, aumenta la conciencia sobre la importancia de la seguridad y asegura una mejor adherencia a las políticas y procedimientos de seguridad, por lo que minimiza riesgos.

2.3.2.22. ¿Qué papel juega la educación y formación de los empleados en la protección de datos?

La formación de los empleados es esencial para garantizar que todos comprendan la importancia de la seguridad de los datos y sigan las mejores prácticas y políticas establecidas por la organización para proteger la información.

Los empleados son cruciales en la protección de datos. Deben estar capacitados en buenas prácticas de seguridad, como el uso de contraseñas seguras, la identificación de correos electrónicos de phishing y el manejo adecuado de la información confidencial.

2.3.3 SOLICITUDES DE INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Blanca Belmonte Peláez, Letrada-DPD de la Junta General del Principado de Asturias

2.3.3.1 ¿En qué consiste el derecho de los diputados a solicitar información y cuál es la naturaleza de ese derecho?

Es una de las formas de ejercer la función de control sobre la acción del Gobierno y constituye un derecho fundamental del diputado perteneciente al núcleo de su función representativa. Además, es un derecho individual de cada parlamentario, pues quien reclama la información no es la Cámara, sino el diputado. Por último, no es un derecho absoluto y, por eso, los reglamentos parlamentarios prevén que la Administración pueda denegar la documentación interesada si lo impiden razones fundadas en derecho.

2.3.3.2 ¿Y el derecho a la protección de datos?

También es un derecho fundamental, y en su virtud se garantiza a la persona el control sobre sus datos y sobre su uso y destino. De esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

2.3.3.3 ¿Cuál es el procedimiento para la tramitación de las solicitudes de información?

Presentada la solicitud por el diputado, corresponde a la Mesa la calificación y admisión a trámite y su remisión al Gobierno por conducto del presidente de la Cámara. Recibida ésta por el correspondiente órgano de la Administración, y tras su análisis y, en su caso, consulta al delegado de protección de datos, procede la recepción de la contestación por la Secretaría General del Parlamento y su traslado al diputado, quien, en caso de no obtener satisfacción, podrá acudir a la vía interna de la queja o a la vía judicial.

2.3.3.4 ¿Existe la posibilidad del tratamiento de datos personales en la tramitación de solicitudes de información?

Sí. Cualquier operación realizada sobre datos personales es considerada tratamiento: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

2.3.3.5 En la calificación y admisión a trámite de solicitudes de información, ¿corresponde a la Mesa de la Cámara examinar la posible vulneración del derecho a la protección de datos personales?

En principio, no. La Mesa lleva a cabo un análisis sobre su viabilidad formal, obviando a priori si la solicitud viene referida a datos de carácter personal o no. Quedan a salvo, no obstante, aquellos supuestos en los que el contenido de la solicitud sea manifiestamente contrario a derecho o inconstitucional, extraño a las finalidades establecidas en el Reglamento o bien cuando el propio Reglamento imponga límites o condiciones a la iniciativa. La mayoría de los reglamentos no exigen más requisitos que los puramente formales del previo conocimiento del portavoz y su traslado por conducto del presidente, por lo que, con carácter general, la Mesa remite sin más valoraciones.

2.3.3.6 ¿Corresponde al diputado evaluar si su solicitud de información vulnera el derecho a la protección de datos personales?

No. El diputado, más allá del juicio interno sobre la pertinencia o no de recabar determinados datos personales, es libre para decidir cómo articula el control parlamentario al Ejecutivo.

2.3.3.7 Entonces, ¿a quién corresponde valorar si prevalece el derecho del diputado a solicitar información o el derecho a la protección de datos personales?

El órgano de la Administración responsable del tratamiento de los datos que se solicitan será quien evalúe el cumplimiento de la normativa sobre protección de datos personales, asesorado, en su caso, por el delegado de protección de datos.

2.3.3.8 ¿El hecho de que la respuesta a una solicitud de información contenga datos personales justifica su denegación?

No. La sola existencia de datos personales no resulta suficiente para justificar la denegación de información al diputado. No constituye por sí misma una razón fundada en derecho que ampare la negativa de la Administración a proporcionar la información. En todo caso, si aquella considera que los datos personales que se solicitan no son realmente necesarios para llevar a cabo el control de la acción del Gobierno, son desproporcionados para tal objetivo o no existen garantías suficientes para su protección deberá motivarlo en su respuesta.

2.3.3.9 En caso de denegación de información, ¿qué puede hacer el diputado/a?

Los reglamentos recogen diferentes mecanismos internos que pueden activar los diputados solicitantes, sin perjuicio de hacer uso, en su caso, de la alternativa jurisdiccional. El más común es la formulación de queja o protesta ante la Mesa de la Cámara, a la que corresponderá determinar la procedencia o improcedencia de aquella limitación al derecho del diputado, apoyándose igualmente, si fuera necesario, en el asesoramiento del delegado de protección de datos del Parlamento.

2.3.3.10 ¿Cuál es la base legitimadora del tratamiento de datos personales en el caso de las solicitudes de información?

La base legitimadora que permite que el tratamiento de los datos personales sea lícito, incluso sin el consentimiento del interesado, reside en el hecho de que el tratamiento es necesario para el cumplimiento de una obligación legal y de una misión realizada en interés público, esto es, el control del Gobierno. Además, la exigencia para estos casos de que el tratamiento esté previsto en una norma con rango de ley queda cubierta con su previsión en el Reglamento parlamentario, que tiene valor de ley.

2.3.3.11 Y si se trata de categorías especiales de datos personales, ¿también es lícito su tratamiento?

En principio, el tratamiento de los llamados "datos ultraprotegidos" quedaría prohibido salvo que concurran los siguientes requisitos: debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. Por consiguiente, habrá que verificar si el Reglamento ha previsto las referidas medidas como pueden ser: el acceso a la documentación en el lugar en el que se encuentre depositada sin posibilidad de obtener copias ni de estar acompañado de asesor, el acceso parcial a la información, la anonimización o disociación de los datos cuando no sea un obstáculo para los fines legítimos perseguidos o la advertencia al diputado de su responsabilidad en cuanto al uso de los datos y tratamiento posterior.

2.3.3.12 Verificada la existencia de garantías en el Reglamento, ¿cómo valorar si el tratamiento de estos datos sensibles es proporcional al objetivo perseguido?

Se deberá constatar que se cumplen los tres requisitos siguientes: a) la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad), lo que nos llevará a preguntarnos, por ejemplo, si con el acceso parcial o el acceso en el lugar donde se encuentre depositada se podría conseguir el objetivo de obtención de información suficiente para llevar a efecto el control del Gobierno; b) la medida es necesaria y no existe otra más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); c) la medida es equilibrada por derivarse de ella más beneficios para el interés general que perjuicios sobre otros bienes en conflicto (juicio de proporcionalidad en sentido estricto), lo que nos obliga a poner en la balanza el derecho a la intimidad de la persona frente al control de la arbitrariedad de la Administración.

2.3.3.13 Recibida la información del Gobierno que contiene datos de carácter personal, ¿quién es el responsable del tratamiento de dichos datos?

Tanto el diputado solicitante como el propio Parlamento. Ambos quedan sujetos al cumplimiento de la normativa sobre protección de datos personales, debiendo aplicar las medidas apropiadas para proteger los derechos y libertades de los interesados, garantizar la seguridad de los datos e impedir su tratamiento no autorizado o ilícito.

2.3.3.14 ¿Qué uso puede hacer el diputado de la información obtenida por esta vía?

El diputado no puede hacer un uso de la información recibida que responda a fines diferentes a los originales, esto es, que responda a otra finalidad que no sea la del control parlamentario de la acción del Gobierno. Conviene no olvidar que estamos en presencia de un derecho fundamental que no puede quedar en manos del juego político. Por ello, ante un uso indebido de la información, el diputado deberá responder por el incumplimiento de la normativa sobre protección de datos personales.

2.3.3.15 El tratamiento de datos personales derivado de solicitudes de información, ¿ha de incluirse en el Registro de tratamiento del Parlamento?

Sí. El tratamiento de estos datos personales se debe incorporar como una categoría más en el Registro de actividades de tratamiento, en el que constará la finalidad del tratamiento, los destinatarios y la base jurídica legitimadora, entre otros extremos, quedando este Registro a disposición de la autoridad de control que lo solicite.

2.3.4 LA INCIDENCIA DE LA PROTECCIÓN DE DATOS EN LAS COMPARECENCIAS ANTE LOS PARLAMENTOS

Olga Herráiz Serrano, Letrada de las Cortes de Aragón

2.3.4.1 ¿Hay que solicitar el consentimiento para tratar los datos personales de los comparecientes si estos son miembros del Gobierno o altos cargos?

Cuando los comparecientes son miembros del Gobierno o altos cargos, sus datos personales van unidos a su condición de datos públicos con lo cual no hace falta recabar su consentimiento para que estos se difundan porque es una consecuencia del cumplimiento de las funciones que regulan los reglamentos parlamentarios, que como sabemos son normas con rango de ley.

2.3.4.2 Si el compareciente es un miembro del Gobierno o alto cargo, ¿necesita disponer del consentimiento de terceros para revelar datos personales de estos durante su comparecencia?

Durante la comparecencia de un miembro del Gobierno o algo cargo y para el correcto funcionamiento de la función de información y control que ejercen sobre ellos los diputados, en la mayoría de los casos no será necesario que los miembros del Gobierno tengan que manejar datos que no sean públicos y que hagan identificables a personas físicas concretas.

Si lo fuera, la prohibición de ceder esos datos verbalmente a los diputados sin el consentimiento del interesado queda subordinada al interés público en la divulgación de esa información en aras de la transparencia.

El representante político podría vulnerar el derecho a la protección de datos de terceros si, durante su comparecencia, los emplea innecesariamente o los utiliza de un modo inadecuado, no pertinente o excesivo en relación con los fines perseguidos con la iniciativa de control político de que se trate.

La reacción del tercero, en su caso, solo podrá realizarse cuando se constate efectivamente que dicha violación se ha producido.

2.3.4.3 ¿Hay que solicitar el consentimiento para tratar los datos personales de los comparecientes si estos son personas anónimas?

Cuando quienes comparecen ante el Parlamento son personas anónimas, en su calidad de personas físicas o de representantes de colectivos sociales, tanto si lo hacen por haber pedido voluntariamente comparecer como si son llamadas por iniciativa propia de los órganos parlamentarios (sin ir más lejos, en las audiencias ciudadanas en el procedimiento legislativo), la base que legitima el tratamiento de sus datos personales seguirá siendo el carácter público que tiene la actividad parlamentaria en cumplimiento de una obligación legal contenida en los Reglamentos de las Cámaras. Eso significa que, en principio, no hay que pedirles su consentimiento expreso.

No obstante, son dudosas aquellas comparecencias que se realizan en nombre de asociaciones constituidas en razón de circunstancias vinculadas a datos de los considerados especialmente protegidos (piénsese en los sanitarios, relativos al padecimiento de determinadas enfermedades, por ejemplo), o aquellas comparecencias en las que puede deducirse que se manejaran datos personales relativos a menores. En tales casos, al no haber mayor garantía que la que representa el consentimiento expreso o inequívoco, deberá valorarse su exigencia (de las personas afectadas o de sus representantes legales si hablamos de menores) antes de sustanciar la comparecencia.

En todo caso, el ciudadano deberá ser informado de los fines para los que el Parlamento tratará sus datos.

2.3.4.4 ¿Qué información habrá de darse a los interesados sobre el tratamiento de sus datos personales que hará el Parlamento?

Con motivo de las comparecencias, el Parlamento no solo maneja nombre, apellidos, DNI, domicilio, dirección de correo electrónico, entre otros datos personales, sino que grabará, retransmitirá y almacenará la imagen y voz de los comparecientes, haciéndola accesible a los medios de comunicación que dan cuenta de la actividad parlamentaria.

Pese a que, como hemos visto, en la mayor parte de los casos, no habrá que pedir consentimiento, los Parlamentos sí deben informar sobre la identidad del responsable del tratamiento, la finalidad del mismo y la posibilidad de ejercer los derechos de acceso, rectificación, supresión y portabilidad.

El lenguaje con que se informa al interesado deberá ser claro y sencillo de forma que el contenido sea perfectamente inteligible.

2.3.4.5 ¿Se puede limitar en el tiempo el mantenimiento de los datos de las comparecencias? ¿Deben actualizarse?

Aunque la legislación en la materia exige que el mantenimiento de los datos no se prolongue más tiempo del necesario, en el caso de las comparecencias, la supresión periódica de los datos casaría mal con el deber de publicitar la actividad parlamentaria tanto histórica como presente por lo que aquella limitación no operaría en nuestro caso.

Tampoco lo haría la necesidad de actualización de los datos habida cuenta que lo que importa en este caso es que la información sea fidedigna en un momento específico, el de la comparecencia en sede parlamentaria.

2.3.4.6 ¿Cómo puede ejercitarse el ejercicio de los derechos de acceso, rectificación, supresión, limitación de tratamiento y portabilidad por los comparecientes interesados?

Los procedimientos para el ejercicio de tales derechos deben ser accesibles a la ciudadanía a través de la propia web del Parlamento.

No obstante, tales derechos han de interpretarse a la luz del principio de transparencia y publicidad que rigen la actividad parlamentaria según los cuales, incluso después de haberse tramitado y concluido una iniciativa, sigue siendo necesario que la ciudadanía pueda acceder a los documentos y archivos que la contienen. Ello hace que, en particular,

el derecho de supresión y el derecho al olvido revistan particularidades en relación con las comparecencias parlamentarias.

Si un ciudadano solicitara con posterioridad a su comparecencia en la Cámara la supresión de los datos personales que obren en poder de la misma y que fueron tratados con motivo de la tramitación de dicha iniciativa, solo podría hacerlo por una razón que, analizada, se entienda de peso suficiente como para prevalecer sobre la obligación de transparencia del Parlamento.

Por su parte, el popularizado como derecho al olvido, que consiste en poder solicitar, bajo ciertas condiciones, que los enlaces a los datos personales no figuren en los resultados de una búsqueda en internet realizada por el nombre de una determinada persona (es decir, el derecho no a que el dato se suprima, sino a que no aparezca en dicha búsqueda), igualmente estaría condicionado a que las circunstancias particulares que llegara a invocar el interesado debieran prevalecer sobre la obligada publicidad parlamentaria.

En definitiva, la cancelación de los datos personales de los comparecientes en sede parlamentaria será excepcional en la práctica y, en esa misma medida, lo será el derecho al olvido complementario del de cancelación, sobre la base de la desindexación o supresión de sus datos de los motores de búsqueda.

2.3.5 MEDIOS DE COMUNICACIÓN SOCIAL Y REDES SOCIALES. ESPECIAL MENCIÓN DEL TRATAMIENTO DE LAS IMÁGENES

María Aneiros Gónzalez, Letrada-DPD del Parlamento de Galicia

2.3.5.1 ¿Acceden los medios de comunicación a los parlamentos?

Si, con carácter habitual. Su acceso y permanencia se regula por cada Parlamento con el fin de establecer diversas limitaciones y determinar aspectos tales como: concesión de acreditaciones; sistemas de controles de acceso; delimitación de zonas de trabajo; espacios de uso exclusivo, etc.

2.3.5.2 ¿Asisten los medios de comunicación a las sesiones parlamentarias?

Salvo determinadas excepciones, en general las sesiones plenarias de las Cámaras son públicas, lo cual conlleva la presencia del público y de los medios de comunicación.

Las sesiones de las comisiones parlamentarias en general son a puerta cerrada, si bien pueden asistir los representantes de los medios de comunicación social debidamente acreditados.

Además, los medios de comunicación acuden a diario a las sedes parlamentarias a otros actos y eventos diversos.

¿Tienen los Parlamentos la obligación de adoptar medidas en materia de protección de datos en su relación con los medios de comunicación?

Respecto de las actuaciones que realicen con los medios de comunicación que conlleven tratamientos de datos personales, los parlamentos están obligados a publicar en su página web dicha actividad, identificando quién trata los datos, con qué finalidad y qué base jurídica legitima ese tratamiento, así como a cumplir el resto de las obligaciones previstas en la LOPDGDD.

2.3.5.3 ¿Tienen los medios de comunicación la obligación de adoptar medidas de prevención al respecto del tratamiento de datos de carácter personal que efectúen?

El tratamiento de los datos personales con fines exclusivamente periodísticos está sujeto a excepciones o exenciones de determinadas disposiciones del RGPD, con el fin de conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información.

La LOPDGDD no reguló tales exenciones y excepciones. No obstante, existe una numerosa jurisprudencia, en la que se aborda el contenido y límites de los derechos fundamentales a la libertad de expresión, a la libertad de información y a la protección de datos de carácter personal.

2.3.5.4 ¿Qué se entiende por tratamiento con fines periodísticos a los efectos de las exenciones o excepciones dispuestas en el RGPD?

El término periodismo no se limita solo a los medios de comunicación profesionales, sino que incluye actividades que tienen por finalidad divulgar al público información, opiniones o ideas por cualquier medio de transmisión.

2.3.5.5 ¿Qué son los derechos constitucionales a la libertad de expresión y a la información, y cuáles son sus límites?

La libertad de expresión hace referencia a la libertad para expresar y difundir libremente los pensamientos, ideas y opiniones por cualquier medio de difusión, mediante la palabra, el escrito o cualquier otro medio de reproducción. La libertad de información se refiere a la comunicación de hechos mediante cualquier medio de difusión de forma veraz.

Estos dos derechos no tienen un carácter absoluto. Uno de sus límites es su coexistencia con otros derechos fundamentales, tales como los derechos al honor, a la intimidad y a la propia imagen.

2.3.5.6 ¿Cuál es el contenido del derecho fundamental a la protección de datos y cuáles son sus límites?

Ese contenido consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Sin embargo, el derecho a la protección de datos no es un valor absoluto ni es ilimitado, y en determinados casos, ha de ceder ante otros valores constitucionales.

2.3.5.7 ¿Cómo se dirime la colisión entre los derechos a la protección de datos y a las libertades de expresión e información?

La libertad de información puede llegar a ser considerada prevalente sobre los derechos de la personalidad, pero no con carácter absoluto.

Para dirimir la colisión entre esos derechos, es necesario realizar una ponderación e identificación de los intereses en conflicto en cada caso concreto, teniendo en cuenta, criterios tales como: la veracidad de la información y su relevancia para la formación de la opinión pública; la notoriedad de la persona afectada (personajes públicos, autoridades, funcionarios); el objeto del reportaje; el comportamiento anterior del interesado; el contenido y las repercusiones de la publicación; etc.

2.3.5.8 ¿Cuáles son los riesgos más comunes relacionados con los datos de carácter personal en las redes sociales?

Las personas usuarias aportan una gran cantidad de información y de datos personales, tanto a las empresas proveedoras de los servicios coma al resto de personas usuarias, lo cual comporta riesgos para su seguridad y privacidad.

En la fase inicial de registro del usuario se identifican los siguientes riesgos: que el tipo de datos solicitados en el formulario de registro, aunque no obligatorios, sean excesivos; que el grado de publicidad del perfil de usuario sea demasiado elevado; que la finalidad de los datos no esté correctamente determinada; que se realicen tratamientos de datos no autorizados habida cuenta la transferencia internacional de datos que de ordinario se produce.

En la fase intermedia, en la que las personas usuarias desarrollan su actividad en la plataforma, se identifican los siguientes riesgos: que la información personal publicada sea excesiva; que se instalen "cookies" sin conocimiento del usuario; que se posibilite la recopilación de información personal más allá de lo necesario para el propósito del tratamiento; que el perfil de usuario sea indexado automáticamente por los buscadores de Internet, lo cual supone una amenaza en la medida en que los datos personales básicos de las personas usuarias y principales contactos podrían exponerse públicamente en la Red, pudiendo llegar a ser empleadas esas informaciones de forma descontrolada por terceros, sin que éstos queden en el "círculo cerrado" de la red social; que se recepcione publicidad hipercontextualizada; que se recepcionen comunicaciones comerciales electrónicas no solicitadas (spam); que se suplante la identidad de los usuarios de la red social.

En la fase en la que el usuario pretende darse de baja del servicio, se identifican los siguientes riesgos: que sea imposible realizar la baja del servicio de manera efectiva, debido a la complejidad de algunos procedimientos; la conservación de los datos de tráfico generados por las personas usuarias en el sistema, para utilizarlos posteriormente con diversas finalidades.

2.3.5.9 ¿Cuáles son las recomendaciones de interés a tener en cuenta?

- La red social si bien no es un entorno pensado inicialmente para el uso administrativo, los tratamientos que se efectúen tienen que cumplir con lo establecido en el RGPD.
- Cuando se ofrece información o servicios a los ciudadanos a través de una red social, no se puede obligar al administrado a contar con perfiles en la misma.
- El servicio proporcionado a través de la red social deberá cumplir con todas las obligaciones establecidas en el RGPD, entre ellas el deber de informar.
- Respecto de la implementación de servicios orientados específicamente a menores, en las actividades de tratamiento de sus datos, hay que garantizar que el consentimiento para dicho tratamiento ha sido prestado por los padres o tutores.
- La mayoría de las redes sociales no ofrecen niveles de calidad de servicio lo suficientemente contrastados para que se puedan convertir en instrumentos de notificación.
- No existen garantías de confidencialidad en la transmisión de una información a la red social.

2.3.5.10 ¿Qué medidas, entre otras, debieran adoptarse por los parlamentos para determinar el uso y para reducir los riesgos de las redes sociales?

- Diseñar el tratamiento a través de las redes sociales y analizar los riesgos que pudieran existir para los derechos y libertades de las personas.

- Disponer de una política de comunicación en redes sociales que refleje los aspectos relativos a la política de protección de datos.
- Establecer una política interna clara y bien conocida por todas las personas de la Institución sobre las implicaciones y consecuencias de la participación en las redes sociales, detallando, entre otras cuestiones:
  a) la estrategia de comunicación, las directrices de gestión y la determinación de la responsabilidad en la cadena de responsabilidades de la organización.
  b) la clarificación de los contenidos y los datos personales que pueden ser o no objeto de publicación, atendiendo al principio de minimización, evitando la identificación de las personas siempre que no sea necesario.
  c) Los recursos personales y materiales adecuados para el uso diario de las redes sociales y la administración.
  d) Las actividades de formación del personal, informándole sobre lo que puede y lo que no puede hacer y sobre la forma en la que se debería dialogar.
- Proporcionar una declaración inequívoca sobre la condición oficial de la cuenta de redes sociales.
- Utilizar técnicas lícitas para buscar un posicionamiento o influencia.
- Velar por el cumplimiento de las directrices establecidas y por la seguridad de los tratamientos mediante la realización de comprobaciones periódicas.
- Garantizar que en la publicación de la documentación anonimizada no se divulguen datos tales como los de la firma electrónica de la persona firmante o el código seguro de verificación que permitiría recuperar todo el documento de que se trate.
- Trazar un plan de comunicación para situaciones de crisis, y dar una respuesta proactiva ante cualquier incidencia que pudiera surgir.

2.3.5.11 ¿Qué es la imagen personal?

A falta de una definición legal de la propia imagen, la jurisprudencia la ha definido como “la representación gráfica de la figura humana mediante un procedimiento mecánico o técnico de reproducción”.

2.3.5.12 ¿Es la imagen un dato personal?

El RGPD establece que los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable.

Se dispone también que se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Por lo tanto, la imagen de una persona es un dato personal, al igual que cualquier información que permita determinar, directa o indirectamente, su identidad.

2.3.5.13 ¿Qué es la intromisión en el derecho a la propia imagen?

Se considera intromisión ilegítima en ese derecho la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos. No se apreciará intromisión ilegítima en los supuestos expresamente autorizados por ley o cuando el titular del derecho otorgase su consentimiento expreso.

No obstante, el derecho a la propia imagen no impedirá su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.

2.3.5.14 ¿Tiene límites el derecho a la propia imagen?

Por regla general, para poder captar, reproducir y/o publicar la imagen de una persona es indispensable su consentimiento expreso e inequívoco. Sin embargo, el derecho a la propia imagen no es un derecho absoluto e incondicionado, y encuentra límites relacionados con el ejercicio de otros derechos fundamentales, como es el caso de la libertad de información.

La protección del derecho a la imagen cede, por tanto, en aquellos casos en los que la publicación de la imagen, por sí misma en relación con la información escrita a la que acompaña, posea interés público, es decir, contribuya a la formación de la opinión pública.

2.3.6 TELETRABAJO Y PROTECCIÓN DE DATOS

Francisco Javier López Hernández, Letrado del Parlamento de Canarias

2.3.6.1 ¿Cómo se previenen los riesgos del uso de tecnologías de la información y comunicación en el teletrabajo?

El teletrabajo se configura como una prestación de servicios a distancia mediante el uso de tecnologías de la información y comunicación. Para garantizar la ciberseguridad de los sistemas digitales de información y prevenir los riesgos que se derivan del tratamiento de datos personales, debe aprobarse una política de seguridad de la información (art. 12 del Real Decreto 311/2022, de 3 de mayo) que en el ámbito de los Parlamentos corresponderá a la Mesa de cada Cámara.

2.3.6.2 ¿Es necesario aprobar una política de seguridad específica para el teletrabajo en las Asambleas Legislativas?

El teletrabajo, basado en las tecnologías de la información y comunicación, no presenta riesgos significativamente distintos al trabajo presencial. Por tanto, no es necesaria una política de seguridad específica o alternativa para esta modalidad de prestación, pero sí se debe ajustar la política que exista a esta fórmula a distancia.

2.3.6.3 ¿Cómo se ajusta la política de seguridad de la Cámara para prevenir los riesgos que se deriven del tratamiento de datos en el teletrabajo?

El uso de dispositivos digitales debe tener un tratamiento concreto en la política de seguridad, dado que con carácter general la prestación en la modalidad presencial se articula sobre la base de dispositivos digitales corporativos. El ajuste del teletrabajo, consecuencia de la virtualización, se traduce primero, en la adopción de la decisión organizativa o bien, de la entrega de dispositivos digitales que permitan la salida de la Asamblea Legislativa, o bien la autorización del uso de dispositivos propios (bring your own device, BYOD) junto a los anteriores; y segundo, en la determinación de las reglas de movilidad de los dispositivos digitales corporativos y la consecuente instauración de mecanismos de seguridad de conexiones remotas (VPN, DLP, etc.).

2.3.6.4 ¿Cuál es el uso a que pueden destinarse los dispositivos digitales puestos a disposición por la Cámara a favor de sus empleadas y empleados públicos?

En principio, los usos de los dispositivos digitales serán siempre profesionales. No obstante, las Cámaras pueden permitir usos privados. Por ello, las Mesas de las Asambleas Legislativas deben aprobar, previa negociación con la representación de las empleadas y empleados públicos, los criterios de utilización de los dispositivos digitales (art. 87.3 de la Ley Orgánica 3/2018, de 5 de diciembre) que determinen los derechos, obligaciones y prohibiciones sobre los mismos, garantizando los estándares mínimos de protección de la intimidad conforme a los usos sociales y a los derechos reconocidos en la Constitución y

las leyes. Y en dichos criterios podrá autorizarse el uso de dispositivos digitales de la Cámara con fines privados, con la determinación de los usos autorizados, períodos en los que podrán realizarse, y el establecimiento de garantías que preserven la intimidad de las empleadas y empleados públicos.

2.3.6.5 ¿Es posible la monitorización de dispositivos digitales?

La monitorización es posible pero sólo sobre dispositivos digitales puestos a disposición por la Cámara, a los efectos de controlar el cumplimiento de las obligaciones laborales o estatuarias y de garantizar la integridad de los dispositivos (art. 87.2 de la Ley Orgánica 3/2018, de 5 de diciembre), lo cual se ha de verificar de acuerdo con los criterios de utilización de dispositivos digitales aprobados por la Mesa de la Cámara, y que han de informarse a todas las empleadas y empleados públicos como requisito previo a su exigencia.

2.3.6.6 ¿También existe un derecho a la intimidad en el uso de dispositivos digitales en teletrabajo ante una eventual monitorización?

El derecho a la intimidad y la protección de datos deben salvaguardarse también en el uso de dispositivos digitales en el teletrabajo ante una eventual monitorización. No obstante, el derecho a la intimidad es absoluto en la utilización de dispositivos propios de las empleadas y empleados públicos, en los que no es admisible la monitorización. Por ello, cuando los dispositivos digitales sean puestos a disposición por la Asamblea Legislativa, la monitorización que pudiera realizarse ha de respetar el derecho a la intimidad de las empleadas y empleados públicos en el uso de tales dispositivos (art. 87.1 de la Ley Orgánica 3/2018, de 5 de diciembre).

2.3.6.7 ¿La monitorización ha de ajustarse a un procedimiento?

La monitorización debe atender a los fines de control del cumplimiento de las obligaciones laborales, y tomar como elemento de contraste a los criterios de utilización de dispositivos digitales. Sin embargo, la garantía de la intimidad y la protección frente a los riesgos que se derivan del tratamiento de los datos obliga su ajuste a la política de seguridad y hacen necesario que se siga un procedimiento similar al establecimiento de los criterios de uso, es decir, previa negociación e información a las empleadas y empleados públicos tras la aprobación de los criterios o política de monitorización, que por su naturaleza requiere una especial motivación.

2.3.6.8 ¿Existe un derecho a la desconexión digital cuando la prestación de servicios es mediante teletrabajo?

Todas las empleadas y empleados públicos tienen derecho a la desconexión digital en garantía del respeto a su tiempo de descanso, permisos y vacaciones y del derecho a la intimidad personal y familiar (art. 88.1 de la Ley Orgánica 3/2018, de 5 de diciembre), con independencia de que la prestación de servicios sea presencial o en teletrabajo.

2.3.6.9 ¿Cómo se articula el derecho a la desconexión digital?

El derecho a la desconexión en el ámbito laboral se articula mediante la aprobación por las Mesas de las Cámaras, previa audiencia de la representación de las empleadas y empleados públicos, de una política interna de desconexión digital en la que se definan las modalidades de ejercicio de este derecho, las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. La política interna deberá tener en cuenta que la regulación de la jornada de trabajo es el límite objetivo al derecho a la desconexión digital. Finalmente, la garantía del derecho a la desconexión digital se vincula a la publicación de la política interna.

2.3.6.10 ¿La flexibilidad del horario en régimen de teletrabajo afecta al derecho a la desconexión digital?

Las normas reguladoras del teletrabajo aprobadas en el ámbito de las Asambleas Legislativas especifican la jornada y, en su caso, el régimen de flexibilidad asociado al cumplimiento del horario. No obstante, el teletrabajo no supone una especial dedicación ni altera los límites horarios que se derivan del establecimiento de la jornada de las empleadas y empleados públicos, fuera de los cuales rige con plenitud el derecho a la desconexión digital.

2.3.6.11 ¿Se tiene aprobar una política de desconexión digital distinta para el teletrabajo?

No es necesario aprobar una política de desconexión digital específica para el teletrabajo, pues las modalidades del ejercicio de este derecho que se contemplen en la política interna, pueden reflejar las peculiaridades que se derivan del teletrabajo, preservando el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

2.3.6.12 ¿Cómo se concilia el derecho a la desconexión digital para las empleadas y empleados públicos que teletrabajen con jornadas parcial o totalmente flexibles?

El fichaje de control horario acota los límites temporales del derecho a la desconexión digital marcando el inicio y el final de la jornada, y en tal sentido, la comunicación con la empleada o empleado público ha de realizarse dentro de la misma. Por ello, ante la dificultad de conocer cuándo es posible contactar con el teletrabajador o teletrabajadora en los supuestos de jornadas con una franja de horario flexible, o jornadas totalmente flexibles, es necesario que la política interna de desconexión digital permita la comprobación del fichaje de la empleada o empleado público.

2.3.6.13 ¿El derecho a la desconexión digital es ilimitado en caso de teletrabajo?

El teletrabajo no supone la desaparición de las necesidades del servicio en el ámbito del empleo público de las Asambleas Legislativas. En ese sentido, la política interna de desconexión digital debe articular la garantía de este derecho junto al servicio objetivo a los intereses generales que desempeña la Administración parlamentaria de modo que, este

derecho podría sacrificarse, ponderando el principio de proporcionalidad, ante circunstancias excepcionales o de fuerza mayor que no admitan demora, y que demanden la rápida intervención de la empleada o empleado público.

2.3.6.14 ¿Se puede establecer un control de geolocalización en los supuestos de teletrabajo?

El teletrabajo es una modalidad de prestación de servicios a distancia, fuera las dependencias de la Asamblea Legislativa. Sin embargo, las normas que regulan el teletrabajo en las Cámaras podrán anudar la prestación remota a su realización en el domicilio, o en el domicilio junto a otros lugares, o en un ámbito geográfico o demarcación territorial, o simplemente, a su realización fuera del Parlamento sin otro condicionante. Por tanto, en el teletrabajo solo puede articularse un control de geolocalización si se ha limitado el lugar desde el que se puede teletrabajar.

2.3.6.15 ¿Se puede geolocalizar a las empleadas y empleados públicos sin información previa?

No se puede geolocalizar a las empleadas y empleados públicos sin la previa información expresa, clara e inequívoca acerca de la implantación de sistemas de geolocalización y las características de estos dispositivos. Como quiera que se producirá un tratamiento de datos, quienes sean objeto de geolocalización deben recibir información sobre el posible ejercicio de sus derechos de acceso, rectificación, limitación del tratamiento y supresión sobre sus datos personales.

2.3.6.16 ¿Cómo se establece un sistema de geolocalización para los supuestos de teletrabajo?

Un sistema de geolocalización en general, y no solo en el teletrabajo, tiene carácter instrumental y solo podrá servir para la función de control de las empleadas y empleados públicos (art. 90 de la Ley Orgánica 3/2018, de 5 de diciembre), siempre de acuerdo con la normativa de empleo público y garantizándose el respeto al derecho a la intimidad de quienes son objeto de geolocalización. El establecimiento de estos sistemas requiere un acto expreso de las Mesas de las Cámaras con la motivación de su necesidad y proporcionalidad, sobre la base del ejercicio de los poderes de dirección, así como la debida publicidad e información.

2.3.6.17 ¿Se puede geolocalizar a los empleados o empleadas públicas fuera de la jornada laboral?

En el acuerdo de establecimiento del sistema de geolocalización se deberá justificar el sistema escogido: satelital, mediante redes de comunicación, u otros, y, sobre todo, el dispositivo digital sobre el que se efectuará el control de geolocalización. Sólo es posible geolocalizar a las empleadas y empleados públicos dentro de la jornada laboral dada la finalidad que cumple la misma. En los dispositivos digitales cedidos por la Cámara que admitan un uso con fines privados, el acuerdo de establecimiento del sistema de geolocalización deberá precisar la prohibición de geolocalizar fuera de la jornada laboral en garantía del respeto al derecho a la intimidad y la protección de datos personales.

2.3.6.18 ¿Pueden utilizarse datos biométricos en el control de la jornada en teletrabajo?

El artículo 9.1 del Reglamento General de Protección de Datos prohíbe el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física con carácter general y sin perjuicio de las excepciones del apartado 2 del mismo artículo. Fuera de las excepciones del precepto, de acuerdo con las directrices del Comité Europeo de Protección de Datos no resulta admisible la utilización de datos biométricos tanto para la identificación a la que alude el artículo 9 del RGPD como para la autenticación y/o verificación de las personas en el control horario de la jornada presencial o mediante teletrabajo.

2.3.7 DERECHO DE SUPRESIÓN (DERECHO AL OLVIDO: SU TRATAMIENTO EN LOS PARLAMENTOS)

Montserrat Auzmendi del Solar, Letrada-DPD del Parlamento Vasco

2.3.7.1 ¿Cómo podríamos definir el derecho al olvido o derecho de supresión de datos de carácter personal?

El capítulo III del Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD), establece los derechos de la ciudadanía en relación con la protección de datos de carácter personal. Entre estos derechos se encuentra el derecho a la supresión de los datos o derecho al olvido, en terminología generalizada en los últimos tiempos.

Este derecho al olvido puede definirse como "una manera de reprobar e intentar hacer frente a la difusión permanente y universal de la información personal en Internet cuando pueda lesionar los derechos e intereses de los interesados"

En realidad, el derecho al olvido no supone una novedad. Es, sencillamente, el derecho de supresión de datos personales, pero circunscrito al entorno digital, al ámbito de Internet.

2.3.7.2 ¿Dónde se desarrolla normativamente el derecho al olvido?

Se encuentra regulado en el artículo 17 del RGPD, así como por el artículo 15 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2.3.7.3 ¿Puede, quien ha participado en un procedimiento parlamentario (por ejemplo, como compareciente), solicitar y conseguir que los datos sobre su persona que obran en la página web de la Cámara, sean suprimidos?

Por supuesto que lo puede solicitar, es un derecho que asiste a toda persona cuyos datos son tratados.

Sin embargo, en cuanto a la consecución de que esos datos sean efectivamente suprimidos de la página web, se habrá de hacer una ponderación de derechos en juego. Es decir, si la persona interesada alega una afectación de un derecho protegible y que pudiera verse seriamente vulnerado en caso de no suprimirse los datos en cuestión, sí procedería la efectiva cancelación de los mismos. En caso contrario, si el mantenimiento de los datos en la web no supone un peligro para derechos más protegibles que el principio de publicidad de las Cámaras, no cabría dicha cancelación. En todo caso, habrá de realizarse una oportuna valoración y ponderación por parte del responsable del tratamiento. Y, con carácter general, y salvando el caso apuntado de grave afectación de un derecho, no procede la supresión de datos.

2.3.7.4 Y, en cuanto a la indexación en motores de búsqueda generales (Google y otros), a través de los cuales se accede de manera sencilla a datos que obran en las webs, ¿cuál sería el proceder correcto si alguien solicita la eliminación de datos en dichos motores? ¿Realmente la actividad de los motores de búsqueda es un tratamiento de datos?

Comenzando por la segunda cuestión, hemos de responder que sí, se trata de un tratamiento de datos. El gestor de un motor de búsqueda recoge los datos que extrae, registra y organiza posteriormente en el marco de sus programas de indexación. Además, conserva estos datos en sus servidores, y, en su caso, comunica y facilita el acceso en forma de listas de resultados de sus búsquedas. Todas estas operaciones son tratamiento de datos según la normativa en vigor.

Y, en cuanto a la primera pregunta, si se solicita la toma de medidas de desindexación para evitar que buscadores tipo Google puedan indexar los datos de las personas interesadas, si nos encontramos con una petición que se circunscribe a una actuación parlamentaria (siguiendo con el ejemplo precedente, el caso de una comparecencia), la respuesta ha de ser similar a la dada en la cuestión 3. Si una persona participa en una actividad parlamentaria, sus datos tales como audio y vídeo, son datos personales asociados a esa actividad parlamentaria. En virtud del principio de publicidad que preside la actividad de las Cámaras, esa información debe ponerse a disposición de la ciudadanía. Y para facilitar dicho acceso, procede su indexación en los motores de búsqueda habituales.

Como en el caso de las páginas web, de peligrar algún derecho fundamental, el responsable del tratamiento deberá analizar la situación para poder determinar si procede la desindexación que se solicita, pero con carácter excepcional.

2.3.7.5 ¿Qué sucede con los datos de particulares que obran en las webs de nuestras instituciones, pero que han sido recabados en procedimientos puramente administrativos? (Por ejemplo, en procesos selectivos)

En estos casos es de plena aplicación la doctrina al respecto de las autoridades de control de protección de datos. Cuando se trata de datos que fueron tratados en su momento, y cuando la finalidad de ese tratamiento ya produjo sus efectos, habrá de accederse a la supresión que se solicita, tanto de la página web como de los motores de búsqueda (por ejemplo, el caso de datos de una persona que participó en un proceso selectivo y pasados los años esa circunstancia sigue apareciendo en los motores de búsqueda que se remiten a los boletines oficiales).

2.3.7.6 ¿Qué apuntes jurisprudenciales pueden sernos de utilidad a la hora de valorar los aspectos referentes al derecho al olvido?

a) En primer lugar debemos recordar la famosa Sentencia C 131/12, del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, caso Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos y Mario Costeja González, que se ha popularizado como la ‘Sentencia Google’, de la que nace además la denominación de ‘derecho al olvido’. Esta sentencia declaró el derecho de la ciudadanía a ser ‘olvidada en la red’. Determinó que no cabe la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información de que se trate sea obsoleta o ya no tenga relevancia ni interés público, aunque la publicación original sea

legítima. Desde que esta sentencia fue dictada, gran cantidad de enlaces han sido eliminados por el buscador predominante en Internet, Google.

Pero téngase en cuenta que esta misma sentencia hace alusión al hecho de que se trate de datos cuya finalidad ya surtió su efecto y cuyo mantenimiento no obedezca a ninguna base legal de tratamiento.

b) También es de tenerse en cuenta la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 22 de noviembre de 2019, en la que se estimó el recurso planteado por Google frente a la Agencia Española de Protección de Datos. Se sentaron algunos principios importantes:

- Si la información obrante en una URL es de interés público, prevalece la libertad de información y dicho interés público.
- También es importante la índole del dato personal de que se trate: puede tratarse de un dato referente a la esfera privada de la persona o puede ser un dato de la vida pública o profesional. Es más aceptable el mantenimiento de la información a disposición del público cuando se trata de datos públicos o profesionales.
- El derecho al olvido no puede ser una herramienta para que cada persona construya un pasado a medida, no puede servir para maquillar posibles hechos o circunstancias que no se consideren positivos a juicio de la persona interesada.

2.3.8. ACTOS NO PARLAMENTARIOS: VISITAS, EXPOSICIONES, JORNADAS. DATOS DE MENORES DE EDAD

Roberto Mayor Gómez, Letrado-DPD de las Cortes de Castilla-La Mancha

2.3.8.1 ¿Están sujetas a la normativa de protección de datos personales las actuaciones no parlamentarias como las puertas abiertas, visitas guiadas, exposiciones, eventos, jornadas, actos protocolarios u oficiales, o la asistencia a la tribuna de público de las sesiones plenarias de la Cámara?

En este tipo de actividades se suele solicitar por los parlamentos o asambleas legislativas datos personales de los visitantes o participantes, principalmente para su identificación o contacto (documento identificativo, dirección postal, teléfono, correo electrónico, firma manual o electrónica...), además, muchas de ellas pueden implicar también la toma de fotografías o grabación de imágenes/voz para su publicación en el portal web institucional de la Cámara o en las redes sociales corporativas, por lo que en estos casos sí estarían sujetas a la normativa en materia de protección de datos.

2.3.8.2 ¿Es necesario incluir esta actividad en un registro e inventario de tratamiento de datos personales?

En la medida que estas actividades puedan generar tratamiento de datos personales se exige que consten reflejadas en el registro e inventario de las actividades de tratamiento del parlamento o asamblea legislativa.

2.3.8.3 ¿Qué sucede si la recopilación de datos personales para este tipo de eventos es efectuada por personal ajeno al parlamento (¿fuerzas y cuerpos de seguridad pública o por empresas privadas de seguridad?

En este supuesto tendrá que valorarse la necesidad de formalizar un contrato entre el responsable y el encargado de tratamientos personales o un acto jurídico que vincule al encargado respecto al responsable, siendo obligación del parlamento o asamblea elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.

2.3.8.4 ¿Cuál es la base jurídica del tratamiento de este tipo de actividades?

Con carácter general, la mayor parte de las actuaciones no parlamentarias (puertas abiertas, visitas guiadas, exposiciones, eventos, jornadas, actos protocolarios u oficiales, asistencia a la tribuna de público de las sesiones plenarias de la Cámara...) pueden ser incluidas, como base jurídica más idónea, adecuada y práctica del tratamiento de datos personales, dentro de la relativa al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes público.

En el caso de las visitas que se realizan a la sede parlamentaria para cualquier actuación no parlamentaria que fueran acompañadas de la captación y registro de la imagen y/o la voz en un soporte físico, para su divulgación y publicación en el portal web institucional, redes sociales, memorias, guías o revistas del ámbito del propio parlamento, la base jurídica más adecuada para el tratamiento de estos datos personales sería el consentimiento del interesado/a.

2.3.8.5 ¿Cuáles serían los fines del tratamiento para este tipo de actividades?

Estos fines estarán identificados de forma individualizada con el objeto propio de la actividad que se vaya a realizar y la gestión necesaria para poder realizarla.

2.3.8.6 ¿Quiénes configurarían la categoría de interesados/as?

Dentro de este conjunto de actividades no parlamentarias la categoría de interesados/as estaría constituida por colectivos como el "público" en general, "invitados", "visitantes", "ciudadanos/as", "autoridades" ...sin descartar también la participación de "empleados/as" o "diputados/as" de cada Cámara.

2.3.8.7 ¿Y qué sucede en el caso de las visitas o actividades de menores de edad en la sede de los parlamentos (plenos infantiles, visitas de colegios u otros centros educativos…)?

Los datos personales de los menores tienen una especial protección y su tratamiento únicamente puede fundarse en su consentimiento cuando sea mayor de catorce años. Si tiene una edad inferior a catorce años el tratamiento de sus datos fundado en el consentimiento solo será válido si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

2.3.8.8 ¿Hay que tener en cuenta alguna previsión en el caso de las visitas o actividades en las que participen menores de 14 años?

Si los participantes en una actividad en la sede parlamentaria son menores de catorce años, y la base de tratamiento va a ser el consentimiento, es recomendable preparar un formulario específico, que prevea y advierta, en su caso, de la aparición del menor en la toma de imágenes fotográficas y/o material audiovisual (vídeo) que pudieran realizase para la difusión y promoción de esta a través del portal web institucional y otras redes sociales asociadas.

Asimismo, se tendrá que habilitar en el formulario el espacio preceptivo para la firma autorizante de el/los titulares/es de la patria potestad o tutela del menor y el resto de los requisitos para acreditar la información básica sobre protección de datos.

2.3.8.9 ¿Cuánto tiempo se pueden conservar los datos personales recopilados en estas actividades?

Hay que partir de la base del principio de limitación del plazo de conservación de los datos personales, que se conservarán durante no más tiempo del necesario para los fines del

tratamiento de los datos personales.

La valoración y determinación del plazo máximo de conservación de los datos personales es una cuestión ciertamente compleja en la que también deben valorarse los plazos de conservación derivados de las obligaciones legales y las circunstancias específicas de cada asamblea o parlamento, con el objetivo de garantizar la protección de los datos de carácter personal de los afectados, y que debe contar también con la participación y colaboración de otros sujetos, como las comisiones de valoración de documentos competentes en materia de archivos.

2.3.8.10 ¿Hay que adoptar alguna medida técnica y organizativa de seguridad?

Las medidas de seguridad que se implanten para la protección de los datos personales en este tipo de actividades no parlamentarias, como en otros tratamientos, tendrán que garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.

En principio, por la tipología de datos facilitados y tratados en este tipo de actividades no parlamentarias las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, en función de los riesgos detectados en el análisis previo que sea elaborado, no conllevarían una especial protección al no afectar a datos personales especialmente protegidos (datos genéticos, biométricos, orientación sexual...).

2.3.9 CANAL DE DENUNCIA

Julián Manteca Pérez, Letrado del Parlamento de La Rioja

2.3.9.1 ¿Qué es el canal interno de información o canal de denuncias?

El canal interno de información de los parlamentos o asambleas legislativas, más conocido como “canal de denuncias” o “buzón de denuncias”, permite la comunicación por parte de personas físicas de aquella información que conozcan en el contexto laboral o profesional sobre posibles infracciones, acciones u omisiones contrarias al ordenamiento jurídico incluidas en el ámbito de la Ley 2/2023, de 20 de febrero, reguladora de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Esta ley tiene como fin garantizar la protección adecuada frente a represalias o perjuicios que puedan sufrir aquellas personas que denuncien, mediante el establecimiento de un canal de información efectivo, confidencial y seguro.

2.3.9.2 ¿Qué infracciones o irregularidades son denunciables?

El canal de denuncias tiene como finalidad servir de cauce preferente de recepción de la información sobre posibles casos de fraude y otras irregularidades establecidas en la Ley 2/2023, tales como:

- Infracciones penales (delitos) o administrativas graves o muy graves, incluyendo aquellas que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.
- Infracciones del derecho laboral en materia de seguridad y salud en el trabajo.
- Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea y que afecten a los intereses financieros de la Unión Europea, enumerados en el Anexo de la Directiva (UE) 2019/1937: contratación pública, servicios, protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.
- Infracciones relativas al mercado interior.

2.3.9.3 ¿Deben los parlamentos y asambleas legislativas contar con un canal interno de información?

Todas las entidades u organismos del sector público deben disponer de un canal interno de denuncias, incluidos los órganos constitucionales y de relevancia constitucional e instituciones autonómicas análogas, al estar así previsto legalmente.

La Mesa del respectivo parlamento o asamblea será el órgano responsable de la implantación del canal de denuncias, aprobando a tal efecto las normas reguladoras del sistema interno de información, previa consulta con los representantes de los trabajadores.

La gestión generalmente recae en la Secretaría General o en un órgano colegiado designado por la Mesa, siendo lo habitual que la persona responsable del sistema de información sea el letrado mayor o un letrado de la cámara.

2.3.9.4 ¿Qué obligaciones se asumen con el sistema interno de información?

Los parlamentos o asambleas legislativas deben:

- Integrar un canal interno que permita denunciar irregularidades.
- Aprobar una política o protocolo de actuación.
- Designar un responsable de gestión del sistema.

2.3.9.5 ¿Cómo debe gestionarse el canal interno de información?

La gestión del canal interno de información se podrá llevar a cabo internamente, dentro de la propia entidad u organismo, o acudiendo a un tercero externo.

Como criterio general debe ser una persona física quien asuma la responsabilidad de su gestión, debiendo actuar de manera independiente y autónoma respecto de los órganos de los parlamentos o asambleas legislativas que la nombren, y disponiendo de los medios personales y materiales necesarios.

El canal de denuncias debe estar gestionado de una forma segura, garantizando la protección y la confidencialidad del informante y de cualquier tercero.

2.3.9.6 ¿Qué debe permitir el canal de denuncias?

El canal interno de información que habilite cada parlamento o asamblea legislativa debe contar con un canal de denuncias que permita:

- La comunicación por escrito o verbalmente, por personas identificadas o de forma anónima.
- La recepción, tramitación y seguimiento de la información recibida, de forma segura y confidencial.
- Documentar la denuncia recibida verbalmente mediante grabación o transcripción, previo consentimiento del informante.
- Contar con un libro-registro que recoja las informaciones recibidas y las investigaciones desarrolladas, al que no se tendrá acceso público y al que solo podrá accederse a petición de la autoridad judicial.
- Garantizar la confidencialidad de la identidad del informante y de cualquier otra persona afectada, del contenido de la denuncia, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma.
- Asegurar el derecho a la presunción de inocencia y el derecho al honor de la persona denunciada, así como a ser informada y oída en cualquier momento.
- Garantizar la protección de los datos personales, debiendo informar a los informantes, denunciados, testigos y cualquier tercero afectado, del tratamiento de sus datos.

- Dar publicidad al canal de denuncias, su regulación y procedimiento, a través de la página web institucional.

2.3.9.7 ¿Cómo y dónde deben presentarse las denuncias?

La información o denuncia podrá presentarse:

- En la sede electrónica del parlamento o asamblea legislativa.
- Por escrito, mediante correo postal o electrónico; o verbalmente, de forma presencial, telefónica, o por mensajería de voz.
- Podrá facilitarse un lugar a efectos de recibir las notificaciones (domicilio o dirección de correo electrónico), o bien renunciar expresamente a la recepción de cualquier comunicación sobre las actuaciones.
- Con la comunicación deberá aportarse la siguiente información:
- Cuantos datos conocidos sean necesarios para la identificación de las personas implicadas, así como de las irregularidades que se les atribuyan.
- Descripción detallada de los hechos que puedan constituir infracción. En su caso, indicación de la relación laboral o profesional que vincula al informante con la entidad o empresa a efectos de aplicar las medidas de protección pertinentes.
- Cualesquiera otros hechos que puedan considerarse oportunos o relevantes.
- Acompañar la documentación de que se disponga para acreditar los hechos.

2.3.9.8 ¿Cuál es la tramitación de la denuncia desde su presentación?

Registrada la información, y una vez acusado recibo de la misma en el plazo de cinco días, se llevarán a cabo los siguientes trámites:

- Admisión: Si los mismos carecieran de verosimilitud o fundamento, se inadmitirá la información en un plazo de diez días. Tanto la admisión como la inadmisión se notificarán al informante en el plazo de cinco días. Si los hechos presentasen indicios de delito se remitirán al Ministerio Fiscal, o a la autoridad competente para su tramitación.
- Instrucción: Comprende toda actuación encaminada a comprobar los hechos denunciados, respetando siempre la identidad del denunciante, y respetando los derechos de defensa y a la presunción de inocencia de la persona afectada, a la que se dará audiencia y se le permitirá formular alegaciones y aportar las pruebas pertinentes. Es importante recordar que existe un deber de colaboración y atender los requerimientos de información que se cursen durante la investigación, incluyendo datos personales si fuera necesario.
- Conclusión: Terminada la instrucción, se emitirá un informe final comprensivo de los hechos denunciados, actuaciones realizadas, y las conclusiones con su motivación. Con ello, se dictará resolución acordando, según los casos, el archivo del expediente, su remisión a otra autoridad competente o al Ministerio Fiscal si los hechos pudieran ser constitutivos de delito, o declarando la comisión de irregularidades y el inicio de un procedimiento sancionador.

Salvo que el informante haya renunciado a la recepción de cualquier comunicación sobre las actuaciones llevadas a cabo, será informado en un plazo que no podrá ser superior a tres meses de la decisión adoptada, contra la que no cabrá recurso.

2.3.9.9 ¿Cuáles son las garantías y derechos de los informantes?

El canal interno de información debe estar gestionado de forma segura, de manera que garantice la confidencialidad de la identidad del informante y de terceras personas, así como de las actuaciones que se desarrollen durante la tramitación de las denuncias, incluyendo la protección de datos a los que se refiere la información, impidiendo el acceso de personal no autorizado. Las medidas de protección se aplicarán también a los representantes legales, compañeros de trabajo o familiares del informante y a las personas con las que tenga relación laboral o profesional.

La identidad del informante sólo podrá ser comunicada, en el caso en el que resulte legalmente exigible, a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, previo conocimiento del informante, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. La persona denunciada no será en ningún caso informada de la identidad del informante.

Quedan prohibidos los actos administrativos que tengan por objeto impedir o dificultar las denuncias, así como los que constituyan represalia o trato discriminatorio tras la presentación de aquellas, pudiendo dar lugar, además, a medidas correctoras disciplinarias o a la responsabilidad que proceda.

Si el informante que hubiera participado en la comisión de la infracción coopera en el procedimiento aportando medios de prueba o datos relevantes para la investigación, podrá ser eximido del cumplimiento de la sanción administrativa, o ver atenuada la misma, siempre que no haya sido sancionado anteriormente, y repare el daño que le sea imputable.

2.3.9.10 ¿Qué medidas se prevén para la protección de las personas denunciadas y terceros afectados?

Se garantiza a la persona a la que se refiere la información la misma protección que para las personas informantes, y especialmente, la presunción de inocencia, el derecho a la defensa, el acceso al expediente, presentar alegaciones, y la confidencialidad de sus datos personales y de los hechos, con el objeto de evitar la posible difusión de los mismos.

2.3.9.11 ¿Qué régimen sigue el tratamiento de datos personales en el sistema interno de información?

Corresponde al parlamento o asamblea legislativa como “responsable del tratamiento” adoptar las medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales obtenidos y tratados a través del canal de denuncias, y determinar los fines y medios del tratamiento, a través de instrumentos como el registro de actividades del tratamiento, el análisis de riesgos o la evaluación de impacto en la protección de datos personales obtenidos y tratados a través del canal de denuncia interno.

2.3.9.12 ¿Quiénes pueden acceder a los datos personales obtenidos en el canal de denuncias interno?

El acceso a los datos personales contenidos en el canal interno de información queda limitado, dependiendo de las competencias y funciones de cada entidad y organismo, exclusivamente a:

- El responsable del canal y quien lo gestione directamente.
- El responsable de recursos humanos (u organismo competente en una entidad pública), cuando sea necesario llevar a cabo un procedimiento disciplinario contra el denunciado.
- El responsable de los servicios jurídicos de la empresa u organismo público, a fin de adoptar las medidas legales correspondientes.
- Los encargados del tratamiento (si estuvieran designados).
- El delegado de protección de datos.

2.3.9.13 ¿Qué papel tiene el delegado de protección de datos en el canal de denuncias?

Entre las obligaciones del responsable del tratamiento se encuentra la de designar un delegado de protección de datos (DPD) cuyas funciones son:

- Informar al responsable o al encargado del tratamiento de las obligaciones legales que les incumben en materia de protección de datos.
- Supervisar el cumplimiento de las disposiciones y las políticas en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control, actuando como intermediario para cuestiones relativas al tratamiento, y recibir o realizar consultas, en su caso, sobre cualquier otro asunto.
- Acceder a los datos personales obtenidos a través del canal de denuncias y en las operaciones de tratamiento, debiendo guardar secreto y confidencialidad.
- Ser notificado de las violaciones de seguridad de los datos personales de las que se tenga conocimiento.

2.3.9.14. ¿Cuánto tiempo deben conservarse los datos personales de las denuncias?

Los datos personales contenidos en la información suministrada y en las averiguaciones posteriores podrán conservarse un máximo de diez años.

Si la denuncia no tuviera verosimilitud, los datos se hubieran recopilado involuntariamente, o estuvieran sujetos a protección especial, se procederá a la inmediata supresión, salvo que el tratamiento sea necesario por razones de un interés público esencial o en el ejercicio

de poderes públicos conferidos al responsable del tratamiento. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

2.3.9.15 ¿Qué ocurre si fallan las medidas de protección? ¿Qué sanciones se prevén para los responsables?

La potestad sancionadora corresponde a la Autoridad Independiente de Protección al Informante, u órgano autonómico competente, sin perjuicio de otro tipo de responsabilidades.

En general, cualquier actuación que suponga una vulneración de los derechos y medidas de protección previstos en la ley 2/2023 supone una infracción sancionable, y especialmente aquella que implique la vulneración de las garantías de confidencialidad o de secreto, así como la adopción de represalias sobre los informantes o su entorno.

Las sanciones se graduarán teniendo en cuenta la naturaleza de la infracción, y las circunstancias concurrentes en cada caso, siendo las mismas mayormente de carácter pecuniario, diferenciando si el infractor es una persona física o jurídica, caso este último en el que la sanción puede oscilar entre los 100.000 y el millón de euros.

2.4 SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

2.4.1 INVENTARIO DE ACTIVOS DE TRATAMIENTO

Ana Francisca Martínez Conesa, Letrada-DPD de la Asamblea Regional de Murcia

2.4.1.1 ¿Qué son los activos de una organización?

En una organización sus activos son el conjunto de bienes, derechos, valores y otros recursos que la misma posee, referidos a todo tipo de bienes, tanto materiales como inmateriales. Y, como cualquier otra organización, los Parlamentos también cuentan con sus propios activos.

2.4.1.2 ¿Cómo se definen los activos en el ámbito de los datos personales?

La Agencia Española de Protección de Datos en la Guía de "Gestión del riesgo y evaluación de impacto en tratamiento de datos personales", define el activo en este ámbito como todo bien o recurso que puede ser necesario para implantar o mantener una operación de tratamiento en cualquier etapa de su ciclo de vida, desde su concepción y diseño hasta la retirada del tratamiento.

2.4.1.3. ¿Qué es, por tanto, un inventario de activos del tratamiento de datos personales?

El Diccionario de la Real Academia de la Lengua Española contiene dos acepciones del término "inventario":

- "Asiento de los bienes y demás cosas pertenecientes a una persona o comunidad, hecho con orden y precisión";
- Y "Papel o documento en el que consta el inventario".

Partiendo de estas acepciones y teniendo en cuenta la definición de activo dada por la Agencia, un "inventario de activos del tratamiento de datos personales" será aquel documento -normalmente en soporte electrónico- que contenga las anotaciones de los diferentes bienes o recursos que pueden ser necesarios para implantar o mantener una operación de tratamiento de un dato personal en cualquier etapa de su ciclo de vida, desde su concepción y diseño hasta la retirada de dicho tratamiento.

Con el inventario se trata, pues, de documentar la trazabilidad del tratamiento a través de los bienes y recursos –"activos"- empleados en él.

2.4.1.4 ¿Qué vinculación tiene este inventario con la seguridad en el tratamiento?

El Instituto Nacional de Ciberseguridad afirma, en referencia a la información en general, que "El inventario de activos conforma el primer elemento de la cadena en un sistema de

gestión de la seguridad de un sistema. Un inventario de activos se define como una lista de todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones, etc.) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos".

Así, cuanto mayor sea la certeza del recorrido que sigue la información en la organización -incluyendo aquella que contiene datos personales- mayor será el conocimiento que se tenga de ella, mayor será la certidumbre respecto a las medidas que se consideren necesarias para asegurarla y, por tanto, mayor será la seguridad.

En este sentido, para la Agencia Española de Protección de Datos, el inventario de activos forma parte del proceso de gestión del riesgo para los derechos y libertades, que exige el conocimiento y análisis de los tratamientos con el mayor nivel de detalle posible. Así, en la Guía mencionada con anterioridad la Agencia afirma que, "Una correcta gestión del riesgo para los derechos y libertades exige conocer los detalles del tratamiento" e indica que, "la granularidad que debe alcanzar la descripción del tratamiento ha de ser la suficiente para que sea posible realizar dicha gestión". Y junto a los tres niveles de detalle con los que se podría estudiar el tratamiento (Estudio a alto nivel del tratamiento; análisis de la estructura del tratamiento, o descomposición del tratamiento en fases para realizar el estudio individual de las mismas; y análisis del ciclo de vida de los datos), añade como análisis adicional el inventario de activos.

En todo caso, indica la Agencia, que "cualquier aproximación que se adopte en la descripción del tratamiento ha de tener como objetivo disponer de un instrumento útil para «garantizar y poder demostrar» de forma eficiente, la gestión del riesgo para los derechos y libertades". Y afirma, en cuanto al nivel de detalle del activo a incluir en el inventario que "debería ser el necesario para identificar y gestionar el riesgo de manera eficiente y, al mismo tiempo, poder demostrar dicha gestión".

Identificar y delimitar dónde se encuentran los activos de la Institución en relación con el tratamiento de datos personales, permite a esta adoptar decisiones más adecuadas y certeras sobre cuáles pudieran ser las medidas técnicas y organizativas más apropiadas en relación con la protección de los datos personales que trata, en orden a mitigar el riesgo para los derechos y libertades de las personas en su tratamiento. Lo que convierte al inventario de activos en un valioso instrumento de apoyo para cumplir con el principio de responsabilidad proactiva que impone el Reglamento General de Protección de Datos.

2.4.1.5 ¿Cómo se podría elaborar un inventario de activos del tratamiento?

Identificar, delimitar y reflejar dónde se encuentran los activos de información de una organización con datos personales puede resultar una tarea compleja, pero para simplificarla se podría dividir el proceso para su elaboración en las siguientes fases:

1. De examen e identificación de los activos.

2. De clasificación de los activos.

3. De confección del inventario, dotando a cada activo identificado de un contenido sobre el tratamiento o tratamientos en los que interviene.

4. De revisión y continua actualización de los activos implicados en el tratamiento.

2.4.1.6 ¿Qué supone cada una de las fases?

Fases 1. En esta fase se han de identificar los activos implicados en el tratamiento de datos personales. Lo deseable para afrontarla es que la organización conozca y tenga identificados todos sus recursos y definidos todos sus procedimientos.

Fase 2. Una vez identificados, los activos se clasifican según las categorías que previamente se determinen.

Una posible clasificación de los activos es la que recoge la Agencia en su Guía, que distingue entre las siguientes categorías:

- Activos humanos.
- Activos organizativos.
- Activos materiales.
- Activos técnicos/sistemas de información.

Otra posible clasificación es la que propone el Instituto Nacional de Ciberseguridad (INCIBE), que distingue entre:

- Activos físicos.
- Activos de información.
- Activos de servicios (Cortafuegos, Switches, etc.)
- Activos personales.

Fase 3. La confección se ha de realizar a partir del análisis estructurado del tratamiento, o mediante cualquier otro procedimiento determinado por la Institución, de igual o mayor eficacia. Los activos figurarían ordenados en el inventario en atención a su clasificación, agrupados por las categorías por las que se haya optado.

Con relación a cada activo, la Agencia establece que sería posible documentar los mismos atendiendo al modelo de la tabla denominada “Descripción de los activos involucrados en el tratamiento”, en la que se recoge la información que en ella se detalla para cada uno de los activos involucrados en el tratamiento de datos personales dentro de la Institución.

Activo	Un identificador del activo
Tecnologías involucradas:	
Tratamientos y fases en las que se emplean:	Puede utilizarse el mismo activo en distintos tratamientos
Operaciones de tratamiento en las que es necesario:	
Datos que son tratados:	
Datos que son generados:	
Roles con acceso al activo:	

Vulnerabilidades (Inherentes al activo):	
Amenazas (internas y externas) asociadas al activo:	

Fase 4. Esta última fase es esencial, ya que un inventario actualizado permite conocer en profundidad en qué momento, quién y cómo se tratan los datos, elevando el nivel de seguridad del tratamiento. O a sensu contrario, podemos afirmar que un inventario desactualizado de poco sirve para la gestión del riesgo en el tratamiento de datos ya que difícilmente podremos asegurar aquello que no conocemos.

2.4.1.7 ¿Qué diferencias y similitudes existen entre el inventario de activos del tratamiento y el registro de actividades de tratamiento?

Respecto a las diferencias:

- El registro de actividades de tratamiento se impone como una obligación –art. 30 del RGPD- para determinadas organizaciones, mientras que el inventario de activos no es en ningún caso obligatorio. Además, el Registro tiene un contenido mínimo –art. 30 del RGPD-, exigible en el caso de que sea obligatorio para la organización.
- El registro se confecciona sobre la base de las “actividades” de tratamiento atendiendo a la finalidad que se persigue con el mismo, mientras que el inventario lo hace sobre la base de los “activos” que se ven implicados en el tratamiento.

Respecto a las similitudes:

- Ambos -registro e inventario- son instrumentos para la gestión de riesgos en materia de protección de datos personales. Permiten conocer los orígenes del riesgo que pudiera existir en los tratamientos de datos personales, aunque desde enfoques diferentes: desde la actividad del tratamiento atendiendo a la finalidad que persigue o desde el activo implicado en el mismo.
- Y contribuyen a cumplir con el principio de responsabilidad proactiva que impone el Reglamento General de Protección de Datos.

2.4.1.8 En definitiva, ¿qué puede suponer para la Institución parlamentaria contar con un buen inventario de activos del tratamiento?

En términos generales, le permite mejorar en la toma de decisiones y en el cumplimiento de la normativa en materia de datos personales, ya que contribuye a:

- Reducir los riesgos y, por tanto, mejorar la seguridad en la gestión del tratamiento.
- Optimizar las actividades de mantenimiento e inspección sobre el tratamiento.
- Mejorar la toma de conciencia del personal de la Institución en la importancia de tratar correctamente los datos personales y la información en general.

2.4.2 UTILIZACIÓN DE DISPOSITIVOS Y PROGRAMAS ELECTRÓNICOS: ACCESO POR PARTE DE LA ORGANIZACIÓN, NORMAS Y CRITERIOS DE USO

Nicolás Pulido Azpíroz, Letrado-DPD del Parlamento de Cantabria

2.4.2.1 Con carácter general, ¿puede una Cámara parlamentaria limitar el uso de los dispositivos y aplicaciones que pone a disposición de sus miembros?

La LOPDGDD prevé que tanto las organizaciones del sector público como del privado cuenten con protocolos o normas de uso de sus medios digitales, que son elaborados en ejercicio de sus facultades de vigilancia y control sobre el personal a su servicio. En ellos se especificarán los usos que están permitidos y los que se excluyen –dentro de estos últimos, generalmente, aquéllos con fines privados o ajenos al trabajo parlamentario– y las medidas correctoras que podrán adoptarse. En ausencia de dichas instrucciones o protocolos de uso, habrán de aplicarse las normas y principios generales que rigen las relaciones laborales y estatutarias, que se concretan en la práctica habitualmente seguida en el seno de la institución.

Como medida correctora o de vigilancia, es posible que la organización acceda al dispositivo o programa en cuestión cuando tenga indicios de que se está haciendo un uso indebido del mismo. No obstante, dicho acceso no será total, sino que está limitado por la intimidad del usuario, que, sin embargo, será menor cuando el equipo que haya utilizado haya sido facilitado por la Cámara y no se trate de un dispositivo personal, aun cuando ambos se hayan empleado para un fin profesional.

En este último caso, dado lo habitual que resulta acceder a programas y cuentas de correo profesionales tanto desde dispositivos personales como corporativos, será conveniente ponerlo previamente en conocimiento de la Cámara, sin perjuicio de que las normas de uso puedan exigir autorización para su instalación en un dispositivo que no sea el suministrado por la Cámara a fin de garantizar la seguridad interna.

2.4.2.2 Con carácter específico, ¿puede limitarlo con base en la normativa de protección de datos?

Según la normativa aplicable, el Parlamento no puede permitir el acceso desde sus dispositivos y aplicaciones a datos personales que no sean esenciales para el ejercicio de la función representativa, o bien que gocen de una especial protección. Es decir: el acceso a los datos ha de ser siempre proporcionado y necesario al fin que permite su consulta.

Si una aplicación provee dicha información en su totalidad (como son las usadas, p. ej., para el archivo de la actividad parlamentaria o para la gestión de nóminas), deberán promoverse las actuaciones necesarias para restringir la facultad de consulta a quien no sea el sujeto competente. En supuestos de acceso desproporcionado, la Cámara ha de poder intervenir sobre el dispositivo o cuenta para limitar el acceso –y, de ser el caso, aplicar las medidas disciplinarias que sean procedentes–. Por otro lado, en materia de transparencia activa, las cámaras legislativas han de facilitar el acceso público a la información

preservando al mismo tiempo la privacidad mediante los correspondientes procesos de disociación de los datos.

2.4.2.3 Y en sentido inverso: ¿puede la protección de datos limitar el acceso del Parlamento a dichos dispositivos?

Las facultades de control pueden ceder ante la protección de la intimidad en la medida en que las herramientas de trabajo contengan información de carácter personal de la persona interesada y de terceros. Para saber de antemano el ámbito de protección garantizado por la intimidad, un factor a tener en cuenta será la práctica habitualmente seguida en el entorno laboral, o, en otras palabras, qué usos privados son consentidos o por lo menos no son objeto de sanción en el trabajo cotidiano (lo que se conoce como la «expectativa razonable de privacidad» que puede albergar el usuario).

Por otro lado, cuando su intimidad se vea potencialmente afectada, el acceso al equipo del usuario siempre requerirá su consentimiento, que únicamente podrá sustituirse cuando lo establezcan una norma con rango legal o una autorización judicial –si bien esto último tendrá lugar en el correspondiente procedimiento incoado al efecto, al margen de los poderes de vigilancia que la administración parlamentaria ejerce de forma ordinaria sobre su personal–.

2.4.2.4 ¿Qué valor normativo tienen los criterios de uso?

Dependerá del instrumento en que se contengan, lo cual servirá para delimitar, principalmente, el régimen de recursos internos. Lo previsible será que se fijen en resoluciones o circulares aprobadas por el correspondiente órgano de la Cámara –v.gr. la Mesa– o por la Secretaría General. En cualquier caso, es necesario que en su elaboración participen los representantes de los y las trabajadoras, y, al hilo de lo apuntado en el punto 2.4.2.1, en la medida en que se empleen dispositivos corporativos y particulares, en el ámbito parlamentario será especialmente valiosa la aportación de los sujetos relevantes para su elaboración y puesta en práctica –p. ej., mediante la coordinación de los grupos parlamentarios a través de sus DPD con el DPD de la Cámara para evitar que queden lagunas o supuestos sin regular–.

2.4.2.5 ¿Hay un tratamiento de datos en el uso de dispositivos, software y aplicaciones?

El uso de equipos electrónicos no supone necesariamente un acto de tratamiento de datos personales, sobre todo cuando el sujeto usuario no sea el responsable del tratamiento; tampoco, a priori, el acceso a los dispositivos y programas por la organización, ya que es un acto de fiscalización de una herramienta facilitada con fines laborales a una persona física. Sin embargo, en el uso de los equipos y sistemas sí se ven implicados datos que tienen la condición de dato personal, como son las claves de acceso y la dirección IP, y que por ello son objeto de protección.

El motivo que justificaría que la Cámara accediese a dispositivos que pueden alojar datos personales no sería, por tanto, una base legítima del tratamiento –v.gr. en ejecución de una obligación legal–, sino su poder de vigilancia o control.

2.4.2.6 ¿Qué medidas de control son compatibles con la protección de datos?

Puede resultar conveniente distinguir entre peligros de origen interno y externo.

Dentro de los primeros se incluirían los usos estrictamente privados de cuya prohibición se haya advertido de manera clara y previa (pensemos en un usuario que utiliza un ordenador de sobremesa ubicado en la sede del Parlamento para consultar direcciones de correo personal o realizar compras de interés particular). Cabría el control conforme a los criterios de uso vigentes. Por su parte, ante un peligro externo que afecte a la seguridad de la institución –v.gr. virus informáticos–, el parámetro de legalidad vendrá determinado por la misión de interés público u obligaciones de rango legal que el Parlamento debe cumplir para garantizar la seguridad de la institución.

En ambos supuestos será necesario ponderar y justificar la prevalencia del interés de la institución en acceder al terminal o cuenta de la persona usuaria, para lo cual las medidas que se adopten deberán superar el test de proporcionalidad (idoneidad, necesidad y proporcionalidad en sentido estricto). Un ejemplo de medida que se podría tomar sería requerir el suministro de logs o historiales de navegación cuando se detecten interferencias en la señal de la actividad del Parlamento, para lo cual sería necesario recabar el consentimiento del interesado.

2.4.2.7 ¿De qué modo afecta a la protección de datos los requisitos técnicos que la normativa exige a los dispositivos y programas electrónicos?

Los equipos informáticos que se comercializan en el mercado han de cumplir con los requisitos que la normativa establece en materias sectoriales como seguridad, accesibilidad para los usuarios o interoperabilidad con otras Administraciones Públicas (AAPP). Dichas exigencias técnicas están diseñadas para facilitar un uso final por los compradores que, entre otros aspectos, respete la protección de datos personales.

Un tema relevante es el de la seguridad, pues los responsables del tratamiento están obligados a aplicar las medidas que correspondan de acuerdo con el Esquema Nacional de Seguridad en relación con la protección de datos. Así pues, les compete verificar que el equipo que van a adquirir reúne esas especificidades técnicas –señaladamente, en los pliegos de los correspondientes procesos de contratación–.

Deben garantizar igualmente las exigencias que se susciten en materias conexas, como son, por citar las más relevantes, la accesibilidad e interoperabilidad. Respecto a la interoperabilidad, la LRJSP establece la reutilización del software libre que haya sido desarrollado por otras AAPP. En concreto, se refiere a las soluciones informáticas disponibles que hayan sido desarrolladas por otras Administraciones y cuya titularidad conserven, para lo cual existen a día de hoy repositorios de aplicaciones a nivel nacional y autonómico. No obstante, hay que tener en cuenta que dicha obligación de reutilización se circunscribe al ámbito de la actividad puramente administrativa, no exigiéndose para la actividad parlamentaria.

2.4.2.8 ¿Qué sanciones cabe adoptar y cuál es el régimen aplicable ante un uso indebido de las herramientas informáticas?

Respecto del personal de la Cámara, cabrá imponer las sanciones que estén previstas en el régimen disciplinario aplicable. Asimismo, de haberse vulnerado la intimidad de terceros,

y según la magnitud del uso (p. ej. divulgación de secretos o intromisión ilegítima en la privacidad), la persona afectada podrá acudir a las correspondientes vías judiciales para reclamar responsabilidad civil o penal.

Pueden darse las siguientes situaciones:

- Uso de cuenta parlamentaria desde un dispositivo del Parlamento: Sujeción a criterios de uso y régimen disciplinario aplicable.
- Uso de cuenta personal desde un dispositivo del Parlamento: El Parlamento puede acceder al dispositivo en función de la práctica laboral habitual y si previamente advirtió al usuario.
- Uso de cuenta parlamentaria desde un dispositivo personal: Sujeción a criterios de uso, que pueden exigir autorización de la Cámara para su instalación, y en todo caso es conveniente que el usuario informe previamente de su uso.

2.4.2.9 ¿Responde jurídicamente el Parlamento por el uso indebido de los medios digitales facilitados?

El Parlamento facilita los medios de trabajo, pero no es el usuario. Sin embargo, cuando la actuación del personal a su servicio –ya sea funcionarial o de otra clase– pueda comprometer jurídicamente a la Cámara ante terceros (relaciones ad extra), ésta podrá repercutirle posteriormente la responsabilidad imputada conforme a su normativa interna (relaciones ad intra).

Además, en su condición de responsable del tratamiento, responderá de las infracciones que le sean imputables en la omisión en la adopción de medidas de protección o salvaguarda –principalmente, ante una brecha de seguridad o por tratar los datos con una finalidad distinta a la inicial sin consentimiento previo o base legítima–. En estos supuestos, el afectado podrá plantear la oportuna denuncia ante la AEPD y, llegado el caso, actuar en sede judicial.

2.4.2.10 ¿En qué manera condiciona la responsabilidad el uso de software para alojar datos en la nube?

Ante el frecuente uso de tecnologías o servidores “en la nube” por motivos de eficiencia para el alojamiento de datos, no es raro que para su gestión se contrate a empresas especializadas en cloud computing, las cuales asumen la condición de encargado del tratamiento. De ser así, las responsabilidades del responsable y del encargado quedarán delimitadas en el correspondiente contrato que suscriban.

2.4.3 VIDEOVIGILANCIA, CONTROL DE ACCESOS Y DATOS BIOMÉTRICOS

Miguel Ángel Andúgar Moreno, DPD de la Asamblea de Extremadura

2.4.3.1 ¿Es totalmente lícito la implantación de sistemas que controlen, vigilen o supervisen las posibles incidencias que puedan alterar el normal funcionamiento de la institución?

Sí, es lícito tal y como recoge el Reglamento General de Protección de Datos (RGPD) o la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2.4.3.2 ¿Una imagen es un dato de carácter personal? ¿Las imágenes están sujetas al RGPD?

La imagen de una persona en la medida que identifique o pueda identificar a la misma constituye un dato de carácter personal. Por tanto, operaciones como la captación, grabación, transmisión, almacenamiento, conservación, o reproducción en tiempo real o posterior, entre otras, son consideradas tratamiento de datos personales y, en consecuencia, se encuentran sujetas al RGPD.

2.4.3.3 ¿Qué usos pueden tener lo sistemas de videovigilancia en una institución?

Toda imagen recabada por un sistema de videovigilancia (SV) que permita identificar a una persona, será considerada un dato de carácter personal.

Los datos de carácter personal resultantes de las imágenes captadas por un SV pueden ser objeto de tratamiento para varias finalidades. La más común persigue el objetivo de garantizar la seguridad de personas, bienes e instalaciones, aunque también podrían usarse para fines como el control laboral de trabajadores.

2.4.3.4 ¿Qué limitaciones o restricciones tiene el uso de los sistemas de videovigilancia?

Las imágenes y datos personales, únicamente se usarán con el fin establecido por el Responsable del Tratamiento (RT), como la seguridad de bienes y personas y/o el control de las obligaciones laborales, y no para otros fines distintos.

La videovigilancia sólo debe utilizarse cuando no sea posible acudir a otros medios que causen un menor impacto en la privacidad.

Las cámaras de videovigilancia instaladas en espacios privados no pueden obtener imágenes de espacios públicos salvo, excepcionalmente, que resulte imprescindible para la finalidad de vigilancia que se persigue, o resulte imposible evitarlo por razón de la ubicación de las cámaras.

Las cámaras de videovigilancia solo podrán colocarse en los lugares permitidos por la ley, como son la zona de recepción o entrada, en los puntos de acceso, en las áreas de trabajo, etc. No podrán colocarse cámaras de seguridad en baños, vestuarios, zonas comunes o

de descanso, ya que se consideran lugares de uso privado o donde las personas esperan tener privacidad.

Cuando la finalidad de las cámaras de seguridad es la seguridad de bienes o personas, no será necesario obtener el consentimiento de los empleados, aunque sí existe el deber de informar sobre la presencia y finalidad de las mismas.

2.4.3.5 ¿Se pueden utilizar sistemas de videovigilancia para tratar categorías especiales de datos?

Si se utiliza un sistema de videovigilancia con el fin de tratar categorías especiales de datos, el RT debe justificar tanto una excepción para el tratamiento de categorías especiales de datos en virtud del artículo 9 del RGPD, como una base jurídica con arreglo al artículo 6 del RGPD.

En todo caso cabe señalar, que el simple hecho de entrar en el alcance de una cámara de videovigilancia, no implica en ningún caso que el interesado pretenda hacer públicas categorías especiales de datos relacionadas con su persona.

2.4.3.6 ¿Existe un plazo de conservación de imágenes?

El principio de minimización afecta al plazo de conservación de los datos personales, de tal forma que en el caso de las imágenes de videovigilancia no ha de superar los 30 días, eliminándose al llegar a este plazo máximo.

La única excepción contemplada al respecto es que las imágenes deban ser preservadas, durante el tiempo necesario y con las medidas de seguridad pertinentes, en el caso de ser necesarias para una investigación policial o judicial. En ningún caso podrá guardarse una copia una vez las imágenes hayan sido recogidas por la policía o los juzgados.

2.4.3.7 ¿Es preciso avisar del uso de un sistema de videovigilancia?

El principio de transparencia del RGPD aplicado a la videovigilancia conlleva que el RT debe cumplir con el deber de informar a los interesados de que sus datos van a ser tratados, por quién van a ser tratados, qué derechos pueden ejercer sobre ellos y de qué manera.

El RT debe facilitar la información de la siguiente forma:

- Colocar obligatoriamente, en las zonas videovigiladas, un cartel informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados, en el que se incluya lo referente a la existencia del tratamiento, identidad del responsable, la posibilidad del ejercicio de derechos de los artículos 15 a 22 del RGPD, y una indicación de dónde pueden obtener más información sobre el tratamiento de sus datos personales.
- Tener a disposición de los interesados el resto de información referida en el artículo 13 del RGPD.

En el uso de un sistema de videovigilancia, ¿qué papel desempeña el Responsable del Tratamiento?

De conformidad con los artículos 24 y 25 del RGPD, el RT debe aplicar todas aquellas medidas técnicas y organizativas necesarias para proteger los principios de la protección de datos durante el tratamiento y establecer medios para que los interesados puedan ejercer sus derechos como se define en los artículos 15 a 22 del RGPD.

Se deberá inscribir el tratamiento de datos de carácter personal en su Registro de Actividades del Tratamiento (RAT), regulado en el artículo 30 del RGPD, como un tratamiento independiente.

2.4.3.8 ¿Es posible externalizar el tratamiento de datos personales?

En lo que respecta a videovigilancia y al RGPD, es necesario establecer quién es el responsable del tratamiento y quién el encargado del tratamiento. En el caso de que exista un prestador de servicios externo con acceso a las imágenes captadas por los SV, éste deberá asumir la figura de encargado del tratamiento.

En esta situación es preciso firmar un contrato de acceso a datos por cuenta de terceros, conforme al artículo 28 del RGPD.

2.4.3.9 ¿Qué medidas técnicas de seguridad se precisan?

Tanto el responsable del tratamiento como el encargado del tratamiento en su caso, estarán sometidos al cumplimiento del artículo 32 del RGPD referente a las medidas de seguridad del tratamiento. Dicho cumplimiento persigue el establecimiento de las medidas técnicas y organizativas necesarias para garantizar el nivel de seguridad adecuado al riesgo.

El RT debe proteger adecuadamente todos los componentes de un SV y los datos en todas las fases, es decir, durante la conservación, la transmisión y el tratamiento.

2.4.3.10 ¿En qué consiste la autenticación mediante un sistema biométrico?

La autenticación por un sistema biométrico es el proceso de comparación entre los datos biométricos de una persona física, con una única plantilla biométrica almacenada en un dispositivo. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona. Es el proceso de validar la identidad de un individuo.

Los sistemas biométricos se utilizan en cualquier aplicativo que requiera de control de acceso, control de presencia, identificación o autorización de una persona física.

El control de acceso biométrico es un sistema de identificación que permite registrar algunas características únicas de las personas físicas con la finalidad de autorizar la entrada y salida de un lugar, o para controlar la jornada laboral de los trabajadores.

2.4.3.11 ¿Qué consideración tienen los datos biométricos?

Los datos biométricos tendrán la consideración de tratamiento de categorías especiales de datos personales con arreglo al artículo 9 del RGPD, si son tratados técnicamente de manera específica para que sirvan para identificar de manera unívoca a una persona física.

De manera general, el tratamiento de datos biométricos exige, la concurrencia de alguna de las bases jurídicas recogidas en el artículo 6 del RGPD y de alguna de las excepciones del artículo 9 apartado 2 del RGPD.

2.4.3.12 ¿Se permite el tratamiento de datos biométricos en el control de acceso o control horario?

La utilización de datos biométricos conlleva altos riesgos para los derechos de las personas. Por ello es preciso realizar previamente una Evaluación de Impacto relativa a la protección de datos, acorde al artículo 35 del RGPD, y considerar medios menos intrusivos para lograr la finalidad legítima del tratamiento.

El tratamiento de datos biométricos de trabajadores para llevar a cabo el control de acceso y el control horario está permitido y fundamentado por el artículo 6 apartado 1 letra b) del RGPD y por el artículo 9 apartado 2 letra b) del RGPD.

En todo caso, el RT deberá tomar todas las medias técnicas necesarias con el fin de salvaguardar la disponibilidad, integridad y confidencialidad de los datos biométricos tratados. Se deberá incluir el tratamiento en el RAT.

2.4.3.13 ¿Se permite la creación de plantillas biométricas?

El RT, de acuerdo al principio de minimización de datos, se hará cargo de que todos los datos biométricos extraídos para ser utilizados en la creación de una plantilla biométrica, no serán excesivos y únicamente contendrán la información imprescindible para el fin legítimo perseguido. Además, se asegurarán las medidas técnicas necesarias para evitar que las plantillas biométricas puedan ser transferidas.

En el caso de que, durante el tratamiento, los sistemas biométricos generen plantillas biométricas temporales o intermedias, el RT deberá asegurar que una vez se haya terminado el proceso, se eliminan de manera segura, inmediata y procedente.

Las plantillas biométricas y los datos sin procesar o los datos identificativos, se almacenarán en bases de datos distintas. Además, se utilizarán tecnologías de cifrado y se evitará toda reutilización de información biométrica para cualquier otro fin distinto al que justificó su tratamiento.

El sistema biométrico utilizado debe permitir la revocación del vínculo de identidad.

2.5 EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS

Montserrat Auzmendi del Solar, Letrada-DPD del Parlamento Vasco
Roberto Mayor Gómez, Letrado-DPD de las Cortes de Castilla-La Mancha

2.5.1 ¿Qué es una Evaluación de Impacto en Protección de Datos (en adelante EIPD)?

Es una herramienta con carácter preventivo, que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

2.5.2 ¿Dónde se regula el mecanismo de la EIPD?

Está regulado en el artículo 35 del Reglamento General de Protección de Datos. En este precepto, el RGPD pide y exige que los responsables del tratamiento realicen una completa evaluación de la situación e implementen medidas adecuadas para garantizar y poder demostrar el cumplimiento del propio Reglamento cuando existan riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, en el caso de que se prevea que un determinado tratamiento pueda acarrear estos riesgos.

2.5.3 Teniendo en cuenta la regulación existente, ¿en qué casos se debe llevar a cabo una EIPD?

La decisión de si una determinada actividad de tratamiento de datos merece una EIPD siempre entrañará una valoración por parte del responsable del tratamiento, pero, para dotar de objetividad a esta valoración, podemos señalar los siguientes factores que nos llevarían a pensar que un tratamiento exige una EIPD:

- Que se lleve a cabo una evaluación o puntuación de aspectos sensibles, como la salud, situación económica, rendimiento en el trabajo, etc.
- Que el tratamiento suponga una decisión con efecto jurídico como, por ejemplo, un tratamiento que pueda provocar la exclusión o discriminación contra las personas.
- Que el tratamiento suponga una observación sistemática (caso paradigmático, el de la videovigilancia)
- Que suponga manejo de datos sensibles o muy personales (categorías especiales de datos personales definidas en el artículo 9 RGPD)
- Que suponga manejo de datos a gran escala.

- Que el tratamiento conlleve el cruce de datos obtenidos para fines concretos, pero que al conectarse la utilización tiene un objeto diferente y desconocido para la persona interesada.
- Que los datos sean relativos a personas interesadas vulnerables.
- Que el tratamiento suponga un uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas.
- Cuando el propio tratamiento impida a las personas interesadas ejercer un derecho o utilizar un servicio o ejecutar un contrato.

Pues bien, se entiende que cuando un tratamiento cumple al menos dos de estos nueve criterios, el responsable del tratamiento habría de llevar a cabo una EIPD.

2.5.4 ¿Quién debe llevar a cabo una EIPD?

Debe llevarla a cabo el responsable del tratamiento. Aunque su realización material se puede encomendar a otra persona.

El Delegado o Delegada de Protección de Datos deberá asesorar al responsable del tratamiento. Si el responsable se apartara del consejo dado por el DPD sobre esta cuestión, ello deberá constar documentalmente.

2.5.5 ¿Cuál es el contenido mínimo de una EIPD?

Lo señala el artículo 35.7 del RGPD. Este contenido mínimo es el siguiente:

- La descripción sistemática de los activos y operaciones de tratamiento.
- La evaluación de la necesidad y proporcionalidad del tratamiento.
- El riesgo que ese tratamiento supone para los derechos y libertades de las personas interesadas.
- Las salvaguardas para afrontar los riesgos existentes, medidas de seguridad, mecanismos que garanticen la protección de los datos personales.
- El establecimiento de un sistema de supervisión y control del plan de seguridad.

2.5.6 Ciñéndonos al caso de los parlamentos, ¿qué tratamientos que se llevan a cabo en nuestras instituciones serían susceptibles de ser evaluados a través de una EIPD?

Sin ánimo de exhaustividad, exponemos los tratamientos que merecen una EIPD, de entre los que se llevan a cabo en las asambleas legislativas:

a) Los tratamientos de imágenes con fines de seguridad: cámaras de videovigilancia.

Este supuesto se incardina en el expuesto en el artículo 35.3 del RGPD. El caso de la ‘observación sistemática a gran escala de una zona de acceso público’.

En las cámaras legislativas, cada responsable del tratamiento, con asistencia y colaboración del Delegado o Delegada de Protección de Datos, habrá de realizar un

análisis o estudio específico en el que, teniendo en cuenta, entre otros factores, el número, finalidad y tipología de cámaras de videovigilancia, la ubicación geográfica y tamaño de las sedes, número de personas captadas… poder valorar y justificar la necesidad o no de realizar una EIPD.

Si se llega a la conclusión de que debe llevarse a cabo esta evaluación, es muy útil el modelo de informe de evaluación de impacto para las Administraciones Públicas puesto a disposición por la AEPD en su portal web.

b) Tratamiento de datos personales en el control horario del personal empleado de los parlamentos.

Refiriéndonos a los casos en los que el control de la jornada laboral de las personas empleadas se realiza mediante un sistema de reconocimiento de datos biométricos, tales como la huella digital o el reconocimiento facial, debemos señalar que este tipo de datos son datos de carácter personal, en tanto en cuanto son información sobre una persona física identificada o identificable según lo dispuesto en el artículo 4.1 RGPD.

Hemos de resaltar que, sobre este particular, la doctrina marcada por la AEPD ha cambiado. Si bien en un primer momento admitía la posibilidad de que se utilizaran estos sistemas para llevar a cabo el control de acceso y horario, en 2023 se dio un giro a esta interpretación. No se contempla la posibilidad de utilización de datos biométricos como control de acceso, puesto que este control no exige *per se* que sea llevado a través de estos sistemas.

Para poder tratar datos biométricos es imprescindible hacer un triple test:

1. Este tratamiento debe ser necesario (no cabe otro modo de llevar a cabo ese control).
2. Debe ser idóneo.
3. Debe ser proporcional.

Llevado a cabo este triple test podemos concluir que este tratamiento de datos biométricos no es necesario para la finalidad que se persigue (el control de acceso y control horario); sí pudiera ser un tratamiento idóneo, es decir, a través de él se puede llegar a conseguir la finalidad de llevar a cabo el control, pero de ninguna manera podemos llegar a la conclusión de que el tratamiento guarda una proporcionalidad entre el bien que se pretende proteger y el bien que se vulnera con la captación de datos especialmente protegidos.

Y, por supuesto, de plantearse un sistema que utilizara datos biométricos, sería imprescindible llevar a cabo una EIPD.

2.5.7 ¿Cabe una EIPD en el caso de proyectos normativos?

Por supuesto, en aquellos casos en que las medidas legislativas que se proponen impliquen el tratamiento de datos personales. Por ejemplo, las normas relativas a salud pública, sistema educativo o normas reguladoras de la Administración y del empleo público, entre otras, son normas que, en general, van a incluir medidas que comportan el tratamiento de datos de carácter personal.

Los elementos a ser evaluados en una EIPD de un proyecto normativo serían:

- Las limitaciones y riesgos que el proyecto normativo suponga para los derechos y libertades.

- Si se respeta la esencia del derecho a la protección de datos.
- La legitimidad de los tratamientos que se prevén.
- La idoneidad, necesidad y proporcionalidad de esos tratamientos.

Habrán de proponerse también en la EIPD las medidas correctoras precisas que minimicen los riesgos que los tratamientos previstos comporten. Estas medidas podrán ser de diferentes tipos:

- Establecimiento de límite geográfico o temporal para los tratamientos de datos.
- Medidas de control específicas.
- Medidas de carácter jurídico.
- Medidas de protección de datos desde el diseño.

El papel del Delegado o Delegada de Protección de Datos en esta tarea, una vez el proyecto normativo ha tenido entrada en la Cámara, es fundamental para detectar la necesidad de que ese proyecto precise una EIPD (caso de que no se haya llevado a cabo previamente en el Ejecutivo), o, caso de que la EIPD vaya incluida en la documentación aportada a la Cámara, para validar la misma, los análisis y las medidas y salvaguardas que esa EIPD plantea.

2.6 LOS DERECHOS DE LOS AFECTADOS: EJERCICIO DE DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS Y TRAMITACIÓN Y RESOLUCIÓN DE LOS MISMOS

Mercè Arderiu Usart, Letrada-DPD del Parlamento de Cataluña

2.6.1 ¿En qué consiste el derecho de información?

El Parlamento debe informar al ciudadano de los datos personales que va a tratar, ya sea un compareciente de una comisión parlamentaria, el público que asiste al Pleno o a una comisión como invitados o bien una visita escolar en la que participan los alumnos, generalmente menores de edad, y los profesores. También debe informar al ciudadano, en general, de la política de protección de datos de la institución y, en concreto, de la finalidad para la que se recogen sus datos personales y cuáles son sus derechos y cómo puede ejercitarlos. En el caso de menores, además, el Parlamento debe contar con el consentimiento de los padres o tutores legales para realizar cualquier tratamiento de sus datos. Además, si los datos personales han sido facilitados por el ciudadano se deberá facilitar la siguiente información: la identidad y los datos de contacto del responsable y del delegado de protección de datos, la finalidad del tratamiento y su fundamento jurídico o legitimidad, los destinatarios de los datos si es el caso, es decir si se prevé enviar los datos a otro organismo o entidad o a otro país u organización internacional, el plazo de conservación de los datos o criterios para determinarlo, sobre los derechos de acceso, de rectificación, de cancelación, oposición, limitación y, en algunos casos, portabilidad, sobre el derecho a retirar el consentimiento o bien a presentar una reclamación. Además, también debe informarse de la fuente de obtención de los datos si no han sido facilitados por el propio ciudadano.

2.6.2 ¿Qué es el derecho de acceso?

Consiste en la facultad del ciudadano de poder acceder a la información personal que le afecta y que trata el Parlamento, con la finalidad de conocer y verificar la legalidad del tratamiento de sus datos personales, y si considera que dicho tratamiento no es legítimo poder ejercer otros derechos como son el de rectificación de los datos, su limitación o, en su caso, la supresión o cancelación total de dichos datos. Esta última facultad puede permitir al interesado el denominado “derecho al olvido”, es decir que sus datos personales sean cancelados definitivamente y no puedan aparecer nuevamente.

2.6.3 ¿Qué es el derecho de rectificación?

El derecho de rectificación consiste en la posibilidad que tiene el ciudadano de solicitar, si los datos de qué dispone el Parlamento son incorrectos, la rectificación de los mismos o bien que se complementen indicando los datos que deben rectificarse y cómo debe hacerse. Cuando sea preciso el Parlamento puede solicitar la documentación justificativa de la inexactitud o del carácter incompleto de los datos objeto de tratamiento. Si el interesado prueba que son inexactos o erróneos el Parlamento está obligado a rectificarlos.

2.6.4 ¿Qué es el derecho de supresión?

El ciudadano tiene derecho a que se cancelen sus datos personales si ya no son necesarios o si retira su consentimiento, si se han tratado de forma ilegal o bien existe una obligación legal de cancelación. Ahora bien, el derecho de supresión, también llamado derecho de cancelación, tampoco es un derecho absoluto, sino que encuentra ciertos límites cuando se pondera con otros derechos fundamentales como la libertad de expresión e información, el cumplimiento de una obligación legal o el cumplimiento de una misión en interés público o en el ejercicio de poderes públicos, fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos o bien la presentación, el ejercicio o la defensa de reclamaciones.

2.6.5 ¿Qué es el derecho de limitación?

Este derecho consiste en reducir el número de datos personales que se conservan por el Parlamento. En general, no existirá ningún obstáculo para la limitación del tratamiento o supresión si ha finalizado la necesidad y finalidad del tratamiento ya que este tratamiento sería ilícito. Es decir, no se pueden conservar indefinidamente los datos personales sin una base legítima, por lo que si se solicita su limitación deberá analizarse la licitud de los datos personales a los que afecta la solicitud y, si procede, limitar su tratamiento. Son supuestos legítimos para poder limitar los datos personales el supuesto de inexactitud de los datos o la falta de legalidad o necesidad del tratamiento.

2.6.6 ¿Qué es el derecho de oposición?

El derecho de oposición consiste en manifestar el desacuerdo con el tratamiento total o parcial de ciertos datos personales. Si el tratamiento no es legal porque no existe el consentimiento ni ninguna otra base legal que fundamente el tratamiento de dichos datos el Parlamento estará obligado a suprimirlos.

2.6.7 ¿Qué es el derecho a la portabilidad y el derecho a no ser objeto de una decisión individual automatizada?

Estos derechos no resultan aplicables en el ámbito parlamentario. En cuanto al derecho a la portabilidad, resulta de aplicación en el caso de ciertos contratos como, por ejemplo, la contratación telefónica, por cuanto permite cambiar de compañía y que se trasladen los datos personales necesarios de una a otra sin necesidad de que el usuario deba hacer una solicitud expresa o facilitarlos de nuevo.

En cuanto al derecho a no ser objeto de una decisión individual automatizada tampoco no resulta de aplicación en el ámbito parlamentario por cuanto el Parlamento no elabora perfiles de usuarios ni para fines comerciales ni tampoco para otros fines.

2.6.8 ¿Cómo se ejercitan los derechos?

El Parlamento dispone en su portal web de la Política de protección de datos personales, que incluye la información sobre el registro de las actividades de tratamiento de datos personales, los datos de contacto del Delegado de protección de datos [DPD] y del

responsable del tratamiento, los derechos que corresponden a los ciudadanos junto a los formularios-modelo para ejercerlos, incluidas las versiones accesibles para personas con discapacidad, así como los códigos de conducta suscritos y certificaciones o sellos reconocidos obtenidos.

Por consiguiente, cuando un ciudadano desee ejercer un derecho puede utilizar el formulario que se facilita en la web del Parlamento, aunque también puede efectuar la solicitud sin utilizar dicho formulario. Para la presentación tampoco no existen formalidades ya que podrá realizarse por vía telemática mediante un correo electrónico al DPD o al Parlamento, presencialmente o por correo certificado.

El Parlamento facilitará al interesado cualquier información relativa al tratamiento de sus datos “en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida especialmente a un niño”. La información se puede facilitar por escrito o por otros medios, incluso electrónicos, pero también verbalmente, acreditando, evidentemente de forma previa, la identidad. Si la solicitud de información se realiza por medios electrónicos, la información debe facilitarse por dichos medios a no ser que la voluntad expresa del interesado se haya manifestado en sentido contrario. El Parlamento proporciona los medios para que las solicitudes se presenten por medios electrónicos en particular cuando los datos personales se traten por dichos medios. Ahora bien, si el ciudadano opta por un medio distinto no se puede denegar el ejercicio del derecho, sea cual sea, por este sólo motivo.

El ejercicio de los derechos reviste carácter gratuito y el plazo máximo para responder es el de un mes, que puede prorrogarse en dos meses adicionales teniendo en cuenta la complejidad y el número de solicitudes. Si el responsable no da curso a la solicitud del interesado o bien no accede a la petición formulada deberá informar, como máximo en el plazo de un mes, de las razones de no dar respuesta o de la justificación de la respuesta dada y de la posibilidad de presentar una reclamación ante la autoridad de control o bien de ejercitar acciones judiciales o administrativas. Todos los derechos pueden ejercerse directamente o por medio de representante legal o voluntario. La reclamación puede hacerse personalmente o por medio de una entidad sin ánimo de lucro.

2.7 PRIVACIDAD DESDE EL DISEÑO

Mercedes Araujo Díaz de Terán, Letrada-DPD del Congreso de los Diputados

2.7.1 ¿Qué significa e implica el concepto de la privacidad por diseño o desde el diseño?

Supone que los desarrolladores de sistemas, plataformas, programas, aplicaciones, páginas web y demás tecnología que impliquen un tratamiento de datos personales incorporen los principios de privacidad desde su diseño para lograr un marco de protección integral de los datos, lo que actualmente es exigido en el artículo 25 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (en adelante RGPD).

2.7.2 ¿De qué manera se logra la privacidad como el modo de operación predeterminado de una organización?

La privacidad como el modo de operación predeterminado de una organización se puede lograr a través del cumplimiento de una serie de principios: el principio proactivo y preventivo, la privacidad como configuración predeterminada, la privacidad incorporada en la fase de diseño.

2.7.3 ¿Qué supone el principio proactivo, no reactivo; preventivo, no correctivo?

Este principio implica la adopción de medidas proactivas que se anticipan a las amenazas, identificando las debilidades de los sistemas para minimizar los riesgos en lugar de aplicar medidas correctivas. Tal política requiere:

- Compromiso por parte de la organización y de cada uno de sus integrantes, asignando responsabilidades concretas.
- Acciones igualmente concretas y mejoras continuas.
- Desarrollo de indicadores para la detección temprana de procesos y prácticas que no garanticen eficientemente la privacidad.

2.7.4 ¿Qué implica la privacidad como configuración predeterminada?

Equivale a la protección de datos por defecto, pues supone que la privacidad del sujeto debe estar garantizada y mantenerse intacta sin necesidad de que este realice acción alguna. La garantía de la privacidad deriva de la propia configuración del sistema, de manera que los datos personales están automáticamente protegidos en cualquier sistema, aplicación, producto o servicio.

Para dar cumplimiento a ese principio se debe:

- Fijar criterios de recogida limitados a la finalidad que persigue el tratamiento.
- Limitar el uso de los datos personales a las finalidades para las que fueron recibidos y asegurarse de que existe una base legitimadora del tratamiento.
- Restringir los accesos a los datos a quienes tengan que conocerlos y crear perfiles diferenciados de acceso según sus funciones.
- Definir plazos estrictos de conservación y establecer mecanismos operativos que garanticen su cumplimiento.
- Crear barreras tecnológicas y procedimentales que impidan la vinculación no autorizada de fuentes de datos independientes.

2.7.5 ¿Qué supone la privacidad incorporada en la fase de diseño?

La realización de este principio supone:

- Considerar la privacidad como un requisito necesario en el ciclo de vida de los sistemas.
- Realizar análisis de riesgos y, en su caso, evaluaciones de impacto relativas a la protección de datos, con carácter previo al diseño de cualquier iniciativa de tratamiento.
- Documentar todas las decisiones que se adopten en el seno de la organización con un enfoque *privacy design thinking*.

En el caso de los parlamentos la perspectiva de la privacidad o el pensar en términos de protección de datos, no sólo se impone como requisito para su actividad administrativa, sino también respecto de su función esencial como órgano constitucional: la actividad legislativa.

2.7.6 ¿Qué se pretende con la funcionalidad total: pensamiento "todos ganan"?

Se pretende una aproximación a la privacidad desde una perspectiva integradora de los diversos intereses a proteger. Para tal fin la organización debe asumir que puedan coexistir intereses diferentes y legítimos; identificarlos y evaluarlos, con la colaboración de los actores implicados, y buscar, desde el diseño, las fórmulas que mejor garanticen todos ellos, en el mayor grado posible en cada caso.

Al margen de los intereses comunes con cualquier organización, cuales son la salvaguarda de la seguridad y funcionalidad del sistema, en los parlamentos la necesidad de un equilibrio se hace evidente en el binomio protección de datos de carácter personal versus transparencia y publicidad que rigen sobre la actividad parlamentaria y de cada uno de los miembros de las Cámaras.

2.7.7 ¿Cómo se puede asegurar la privacidad en todo el ciclo de vida?

Para ello se deben implementar las medidas más adecuadas en cada una de las etapas del tratamiento, recogida, registro, clasificación, traslado, conservación, consulta, difusión,

supresión.

- La seudonimización temprana o técnicas de anonimización como la K-anonimicidad.
- Perfiles de acceso diferenciados según las funciones a realizar en relación con el tratamiento.
- El cifrado por defecto.
- La destrucción segura y garantizada de la información al final de su ciclo de vida.

La minimización es sin duda la mayor garantía de la privacidad, tanto limitando en lo posible su captación en origen como garantizando su supresión tan pronto ello sea posible.

2.7.8 En relación con la fase inicial de la recogida de datos en el Registro General de la Cámara como punto de entrada de escritos e iniciativas, presentados por los miembros de la Cámara y grupos parlamentarios en su mayoría, pero también, por otros órganos y entidades, así como por particulares, ¿tiene que adoptarse alguna cautela en materia de protección de datos personales?

En la medida en que, una vez registrados los escritos son públicos, a través de la intranet, para todos los usuarios habilitados para su consulta (personal de la Cámara, de los grupos parlamentarios, diputados y diputadas, gobierno…), no debieran ser públicos todos aquellos documentos que contengan datos personales cuya privacidad ha de ser garantizada, sino que sólo debieran aparecer visibles los campos: número de registro; tipo de expediente; fecha y hora del registro; el título del tipo de expediente; sus autores, sin que pueda consultarse, salvo por los perfiles de usuario predeterminados, el documento correspondiente.

2.7.9 ¿Qué sucede con la protección de datos personales en las solicitudes de autorización presentadas por los miembros de la Cámara para poder emitir su voto por procedimiento telemático?

En los casos de embarazo, maternidad, paternidad, enfermedad o situaciones excepcionales de especial gravedad, se ha de adjuntar justificante médico que motive su solicitud, documento que, dada la naturaleza de los datos personales que contiene, no debiera resultar visible al consultar el Registro ni ser objeto de publicidad en ningún momento posterior.

2.7.10 ¿Cómo se garantiza la privacidad de la documentación relativa a los trabajos de las Comisiones de Investigación?

En este caso, si bien la no publicidad se predica con carácter general de las sesiones de las Comisiones de Investigación en las que no se celebren comparecencias informativas, así como de los datos y documentos facilitados a las mismas, se trate o no de datos personales, la restricción de los perfiles de acceso a esta documentación garantiza la privacidad de los datos personales contenidos en la misma.

2.7.11 ¿Qué sucede con las peticiones presentadas por los ciudadanos al amparo del artículo 77 de la Constitución Española?

El texto de las iniciativas no es objeto de publicidad ni en la página web ni en el boletín oficial de la Cámara, estando su acceso restringido a aquellos perfiles de usuarios que deban conocerlos por razón de sus funciones.

2.7.12 ¿Cómo se garantiza la privacidad de los escritos procedentes de los órganos jurisdiccionales?

Desde su registro se debe velar por la no publicidad de la documentación que pudiera afectar a la condición procesal de los diputados/as, tanto en los suplicatorios como en otras solicitudes cursadas a la Cámara por los órganos judiciales (solicitudes de certificación de la condición de miembro de la Cámara, citaciones, embargos).

En el caso de los suplicatorios, la protección de la privacidad se debe mantener durante toda la tramitación, de forma que la documentación no es objeto de publicación ni en la página web ni en el boletín oficial de la Cámara, como tampoco se reflejan en el Diario de Sesiones los debates correspondientes, que no debieran si quiera mencionar el nombre de la diputada o diputado al que se refieran.

2.7.13 ¿Qué implicaciones tiene la protección de datos personales en los Registros Electrónicos?

En el planteamiento del diseño de un Registro totalmente electrónico han pues de considerarse estas cuestiones: la ocultación o no visibilidad de los escritos que se presenten bajo las categorías de expedientes que así se predetermine, y el permitir la no publicidad parcial de los escritos.

Por lo demás, los escritos no visibles para su consulta en el Registro sólo son accesibles para un número reducido de perfiles de usuarios.

2.7.14 ¿Cómo se puede hacer visible y transparente la política de protección de datos?

Hacer efectiva la transparencia en el tratamiento de datos por parte de la organización, a la que conmina el considerando 39 del RGPD, implica la adopción de medidas informativas que podrían sintetizarse en tres:

- Hacer públicas las políticas de privacidad y protección de datos de la Cámara, en el apartado apropiado de su página web.
- Desarrollar cláusulas claras de información para los interesados en cada uno de los tratamientos, de manera que puedan comprender con facilidad el alcance del tratamiento de sus datos, los riesgos y los derechos ejercitables.
- Publicar los tratamientos realizados y los datos de contacto de los responsables en materia de protección de datos.

2.7.15 ¿De qué manera se puede respetar la privacidad de los usuarios?

Para respetar la privacidad de los usuarios se puede:

- Adoptar medidas de privacidad por defecto sólidas y advertir a los usuarios de las consecuencias de alterar los parámetros preestablecidos.
- Facilitar información completa y adecuada para garantizar un consentimiento informado.
- Proporcionar a los interesados acceso a sus datos y a las finalidades del tratamiento, así como mecanismos eficientes para el ejercicio de sus derechos.

ANEXO I. CONSULTAS FRECUENTES

En el caso de la concesión de unos premios a menores de edad por una Consejería del Gobierno regional pero cuyo acto de entrega y organización se lleva a cabo en sede parlamentaria ¿sería suficiente recabar el consentimiento que legitima el tratamiento de los datos personales a través del formulario que pone la Consejería a disposición de los padres y tutores?

Sería suficiente siempre y cuando en dicho formulario se recogieran todos los aspectos del tratamiento que lleva a cabo el parlamento y que no coinciden necesariamente con los del tratamiento de la Administración. En caso contrario, la Cámara debe recabar el consentimiento informado de padres o tutores de los menores a través de su propio formulario.

¿Se pueden utilizar las imágenes de otros años de menores participantes en un programa de divulgación entre escolares de la Cámara Parlamentaria para hacer publicidad de la convocatoria de años posteriores cuando esta finalidad no estaba incluida en los formularios de consentimiento informado que firmaron los padres y tutores?

No, ya que la finalidad del tratamiento no coincide. Así, los datos -imagen- de años anteriores se recabaron y trataron con la finalidad de publicitar las visitas realizadas en un momento concreto y no para publicitar la propia existencia del Programa y la convocatoria anual en un momento posterior.

En el caso de separación de los progenitores de un menor de edad ¿es suficiente con que uno de ellos firme el formulario de consentimiento informado para poder tratar los datos del menor?

No, en este caso el formulario ha de estar firmado por los dos progenitores.

Un medio de comunicación, ¿puede utilizar el formulario de la Cámara para tratar datos de menores para un programa de televisión sobre la actividad parlamentaria?

No, ya que la finalidad del tratamiento del medio de comunicación no coincide con la finalidad para la que la Cámara recabó y trató los datos.

¿Pueden cancelarse los datos personales de un ciudadano que lo solicita y que ha estado en el Parlamento de visita, que ha comparecido como experto o bien que ha asistido como público asistente?

Los datos personales que se tratan son los estrictamente necesarios para la finalidad por la que se recogen y se conservan únicamente durante un período no superior al necesario según la finalidad y ello debe ser informado al ciudadano desde el primer momento. Los datos personales pueden conservarse durante períodos más largos siempre que se traten exclusivamente con finalidades de archivo en interés público, de investigación científica o

histórica o con finalidades estadísticas. En caso contrario deberán suprimirse una vez transcurrido el plazo de conservación estipulado según la finalidad del tratamiento.

¿Puede solicitar un aspirante a unas pruebas de selección de personal la supresión de sus datos personales que aparecen en el portal web del Parlamento relativos a una convocatoria pública de trabajo?

Si la convocatoria está finalizada y también los plazos para la interposición de los posibles recursos o alegaciones o la finalización del plazo para la interposición o presentación de los mismos podrán suprimirse dichos datos o, como mínimo, que no aparezcan publicados puesto que no es ya necesaria ni legítima la publicidad de los mismos. Ello, no obstante, podrán conservarse los datos personales de aquellos que fueron seleccionados o de todos si se cumplen los requerimientos de necesidad por archivo de interés público, investigación científica o histórica o estadística, aunque sin publicidad activa.

¿Puede solicitarse información sobre si el Parlamento tiene datos personales nuestros?

Si, puesto que el derecho de acceso consiste precisamente en el derecho de un ciudadano de conocer cuáles son los datos personales de qué dispone el Parlamento y con qué objeto o finalidad. En el supuesto de que no disponga de datos la respuesta será sencillamente negativa. Por el contrario, si la respuesta es afirmativa deberán indicarse exactamente los datos personales que posee el Parlamento y, además, la siguiente información:

a) Las finalidades del tratamiento de los datos personales, es decir, cuál es el uso que se da a dichos datos y con qué objetivo.

b) Las categorías de datos que posee (edad, DNI, domicilio, imagen etc.).

c) Si se efectúa una cesión de los datos a otras autoridades o personas.

d) El plazo de conservación de dichos datos.

e) El derecho del ciudadano de solicitar el acceso, la supresión, la rectificación, la limitación o la oposición, así como de solicitar la portabilidad de los datos.

f) El derecho a presentar una reclamación ante una autoridad de control.

g) El origen de los datos.

h) La existencia de decisiones automatizadas sobre los datos, incluida la elaboración de perfiles.

El responsable del tratamiento, es decir, el Parlamento, deberá facilitar una copia de los datos personales que posee del ciudadano gratuitamente. Esta solicitud puede efectuarse también de forma electrónica y en dicho caso deberá responderse de la misma forma.

ANEXO II. FORMULARIOS

Mercè Arderiu Usart, Letrada-DPD del Parlamento de Cataluña

Solicitud de acceso a los datos personales

Datos del solicitante		
Nombre y apellidos		DNI
Domicilio [calle, avda.] Piso	Núm.	Bloque
Población		Código Postal
Provincia		Telf.
Correo electrónico:		

Responsable del tratamiento y Delegado de protección de datos		
Parlamento de		
Calle/Avda./Ctra.		Núm.
Población	Provincia	Código Postal
Portal web [indicar url]		
Correo de contacto DPD		

Asunto: solicitud de información sobre el tratamiento de los datos personales

Solicito que se me facilite el acceso a la siguiente información:

Asociación de delegados y delegadas de protección de datos de Parlamentos

- ☐ Acceso a los datos personales
- ☐ Categorías de datos personales
- ☐ Cesiones a terceros países u organizaciones Internacionales
- ☐ Plazo de conservación o criterios para determinarlo
- ☐ Derecho de rectificación, supresión, limitación u oposición
- ☐ Derecho a presentar una reclamación ante una autoridad de control
- ☐ Origen de los datos cuando no se han obtenido del interesado
- ☐ Existencia de decisiones automatizadas o elaboración de perfiles
- ☐ Fines del tratamiento
- ☐ Destinatarios o categorías de destinatarios

Fecha:

Firma solicitante:

:

Parlamento de ---

Se informa que se facilitará la información solicitada en el plazo máximo de un mes pero que dicho plazo puede prorrogarse según la complejidad y el número de solicitudes. No obstante, si transcurrido el plazo de un mes no se ha recibido información sobre la prórroga se podrá considerar la solicitud como desestimada y se podrá interponer la reclamación oportuna ante la autoridad de control de datos competente.

Asociación de delegados y delegadas de protección de datos de Parlamentos

Solicitud de rectificación de datos personales

Datos del solicitante			
Nombre y apellidos			
Domicilio [calle, avda.]		Núm.	Bloque
Piso	Puerta		
Población			Código Postal
Provincia			Telf.
Correo electrónico			
Responsable del tratamiento y Delegado de protección de datos			
Parlamento de			
Calle/Avda./Ctra.			Núm.
Población	Provincia	Código Postal	
Telf.			
Portal web [indicar url]			
Correo de contacto DPD			
Asunto: solicitud de rectificación de datos personales			
Se solicita que (...)			
Firma solicitante		Fecha:	
Parlamento de			
Se informa que se facilitará la información solicitada en el plazo máximo de un mes pero que dicho plazo puede prorrogarse según la complejidad y el número de solicitudes. No obstante, si transcurrido el plazo de un mes no se ha recibido información sobre la prórroga se podrá considerar la solicitud como desestimada y se podrá interponer la reclamación oportuna ante la autoridad de control de datos competente.			

Asociación de delegados y delegadas de protección de datos de Parlamentos

Solicitud de supresión de datos personales

Datos del solicitante

Nombre y apellidos

Domicilio [calle, avda.] Núm.
Bloque Piso Puerta

Población Código Postal
Provincia Telf.

Correo electrónico

Responsable del tratamiento y Delegado de protección de datos

Parlamento de

Calle/Avda./Ctra. Núm.

Población Código Postal
Provincia Telf.

Portal web [indicar url]

Correo de contacto DPD

Asunto: solicitud de supresión de datos personales

Se solicita que

Firma solicitante Fecha

Parlamento de

Se informa que se facilitará la información solicitada en el plazo máximo de un mes pero que dicho plazo puede prorrogarse según la complejidad y el número de solicitudes. No obstante, si transcurrido el plazo de un mes no se ha recibido información sobre la prórroga se podrá considerar la solicitud como desestimada y se podrá interponer la reclamación oportuna ante la autoridad de control de datos competente.

Asociación de delegados y delegadas de protección de datos de Parlamentos

Solicitud de derecho de oposición a los datos personales

Datos del solicitante		
Nombre y apellidos		
Domicilio [calle, avda.] Bloque	Piso	Núm. Puerta
Población		Código Postal
Provincia		Telf.
Correo electrónico		
Responsable del tratamiento y Delegado de protección de datos		
Parlamento de		
Calle/Avda./Ctra.	Núm.	
Población		Código Postal
Provincia		Telf.
Portal web [indicar url]		
Correo de contacto DPD		
Asunto: solicitud de oposición al tratamiento de datos personales		
Se solicita que (concretar los datos personales a los que se opone)		
Firma solicitante	Fecha:	
Parlamento de-----		
Se informa que se facilitará la información solicitada en el plazo máximo de un mes pero que dicho plazo puede prorrogarse según la complejidad y el número de solicitudes. No obstante, si transcurrido el plazo de un mes no se ha recibido información sobre la prórroga se podrá considerar la solicitud como desestimada y se podrá interponer la reclamación oportuna ante la autoridad de control de datos competente		

Asociación de delegados y delegadas de protección de datos de Parlamentos

Solicitud de derecho de limitación

Datos de la persona solicitante			
Nombre y Apellidos			DNI
Domicilio			
Núm.	Bloque	Piso	Puerta
Población			Código Postal
Provincia			Telf.
Correo electrónico			

☐ **Deseo recibir la solicitud de información por correo postal certificado (personas no obligadas a relacionarse de forma electrónica con la administración)**

Datos relativos a la persona responsable del tratamiento y Delegado de protección de datos	
Parlamento de	
Calle	Núm.
Población	Código Postal
Provincia	Telf.
Portal web [indicar url]	
Correo de contacto DPD	

Asunto: solicitud de limitación del tratamiento de los datos personales

Se solicita que (....)

Firma Localidad y fecha:

Parlamento de

Se informa que se facilitará la información solicitada en el plazo máximo de un mes pero que dicho plazo puede prorrogarse según la complejidad y el número de solicitudes. No obstante, si transcurrido el plazo de un mes no se ha recibido información sobre la prórroga se podrá considerar la solicitud como desestimada y se podrá interponer la reclamación oportuna ante la autoridad de control de datos competente.

ANEXO III. ESQUEMAS DE PROCEDIMIENTO

INVENTARIO DE ACTIVOS

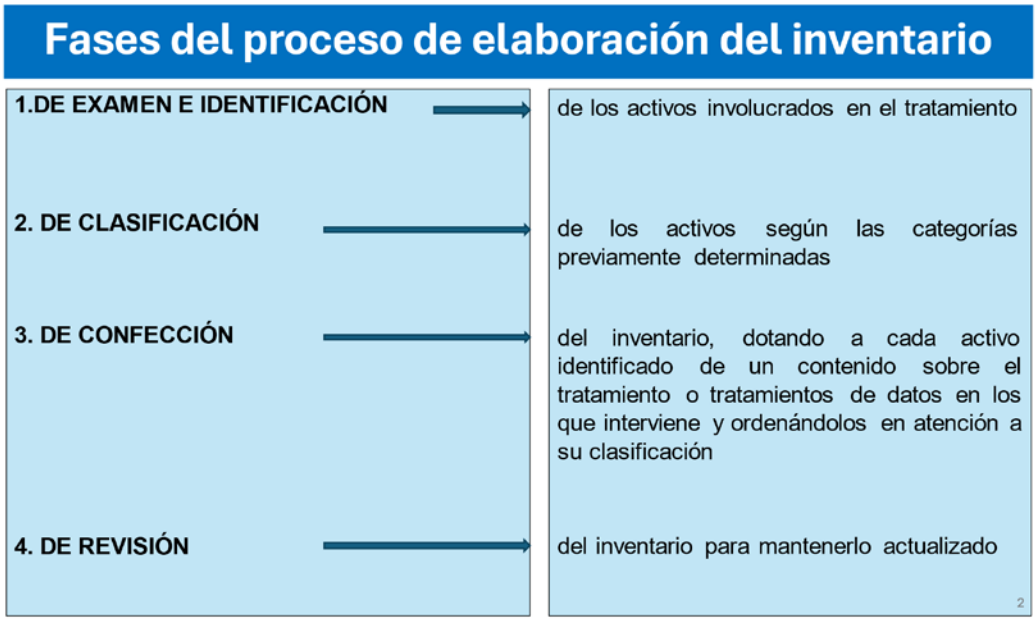
Ana Francisca Martínez Conesa, Letrada-DPD de la Asamblea Regional de Murcia

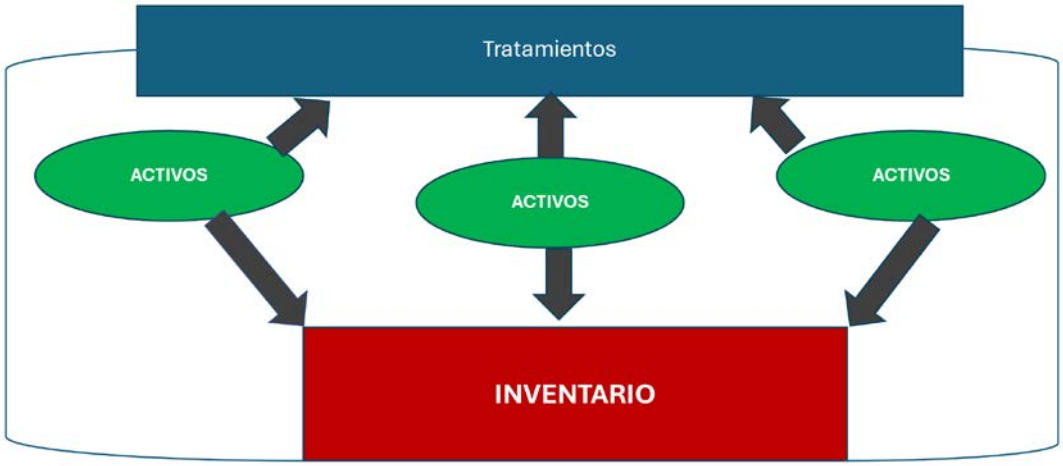
DESCRIPCIÓN DEL CONTENIDO DE LA TABLA DENOMINADA DE "DESCRIPCIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL TRATAMIENTO"

Activo	Bien o recurso empleado en el tratamiento. Identificado con una denominación e incluso con un código
Tecnologías involucradas:	Tecnologías de la información y comunicación, que se ven involucradas en el tratamiento de datos que se realiza a través del activo. Se pretende identificar el uso de tecnologías disruptivas, poco maduras o emergentes en el tratamiento. Como: - Cookies y tecnologías de seguimiento. - Redes sociales. - Cloud computing. - Big Data. - Inteligencia Artificial. - Blockchain y Tecnologías de Registro Distribuido. - Smart Cities.
Tratamientos y fases en las que se emplean: (Puede utilizarse el mismo activo en distintos tratamientos)	Tratamiento o los tratamientos -de entre los recogidos en el registro de actividades de tratamiento de la Institución- en los que se emplea el activo, así como las fases del tratamiento en las que se emplean: - Captura. - Clasificación/almacenamiento. - Uso y explotación. - Cesión y transferencias a terceros - Bloqueo y/o supresión. Resulta esencial para que la información sea la adecuada y para identificar correctamente lo anterior que el registro de actividades se encuentre actualizado y que en él figuren adecuadamente identificadas todas las actividades de tratamiento de datos que realiza la Institución.

Operaciones de tratamiento en las que es necesario:	Las operaciones de tratamiento se recogen en el artículo 4.2) del RGPD: - Recogida. - Registro. - Organización. - Estructuración. - Conservación. - Adaptación o modificación. - Extracción. - Consulta. - Utilización. - Comunicación por transmisión. - Difusión. - Otra forma de habilitación de acceso. - Cotejo o interconexión. - Limitación. - Supresión. - Destrucción.
Datos que son tratados:	Datos tratados por el activo y que se pueden clasificar en una de las tres categorías que recoge el RGPD: de carácter general, categorías especiales y de naturaleza penal. Son datos de carácter personal: los identificativos, los de características personales, circunstancias familiares y sociales, información laboral, académicos y profesionales, financieros, actividades y negocios. Son categorías especiales los del artículo 9 del Reglamento: origen étnico o racial, opiniones políticas, convicciones filosóficas o religiosas, afiliación sindical, genéticos, biométricos dirigidos a identificar inequívocamente a una persona, relativos a la salud, relativos a la vida sexual o a la orientación sexual. Los datos personales de naturaleza penal hacen referencia a denuncias, procedimientos judiciales o sentencias condenatorias.
Datos que son generados:	Aquellos que se originan por la utilización en el tratamiento de aplicaciones, por los sistemas de información, por el uso de sistemas de comunicación. Se trata de datos que se generan en la actividad o en las relaciones de la organización.
Roles con acceso al activo:	Para cada interviniente hay que definir sus roles con relación a las operaciones de tratamiento identificadas.
Vulnerabilidades (Inherentes al activo):	Derivadas de elementos técnicos, humanos u organizativos, que pueden provocar accesos no autorizados o la pérdida de calidad de datos, exactitud, disponibilidad, resiliencia…Una vulnerabilidad en uno de los activos identificados pudiera dar lugar a una brecha con consecuencias no deseadas sobre los derechos y libertades de los interesados.

Amenazas (internas y externas) asociadas al activo:	Las amenazas o factores de riesgos -en términos del RGPD que lo utiliza como sinónimos- denominadas por la Agencia "factores de riesgo", son las derivadas de los elementos técnicos, humanos u organizativos, así como de situaciones o contextos sociales determinados (crisis económica, pandemia, inestabilidad política y social, etc.) que aprovechando la vulnerabilidad de uno de los activos identificados pudieran dar lugar a brechas con consecuencias no deseadas para los derechos y libertades de los ciudadanos. Se denominan amenazas o factores de riesgo. Algunas amenazas, sin ánimo de exhaustividad, serían: los accesos no autorizados; las causas naturales; los accidentes; los errores humanos; los errores en el funcionamiento de tratamientos automatizados.





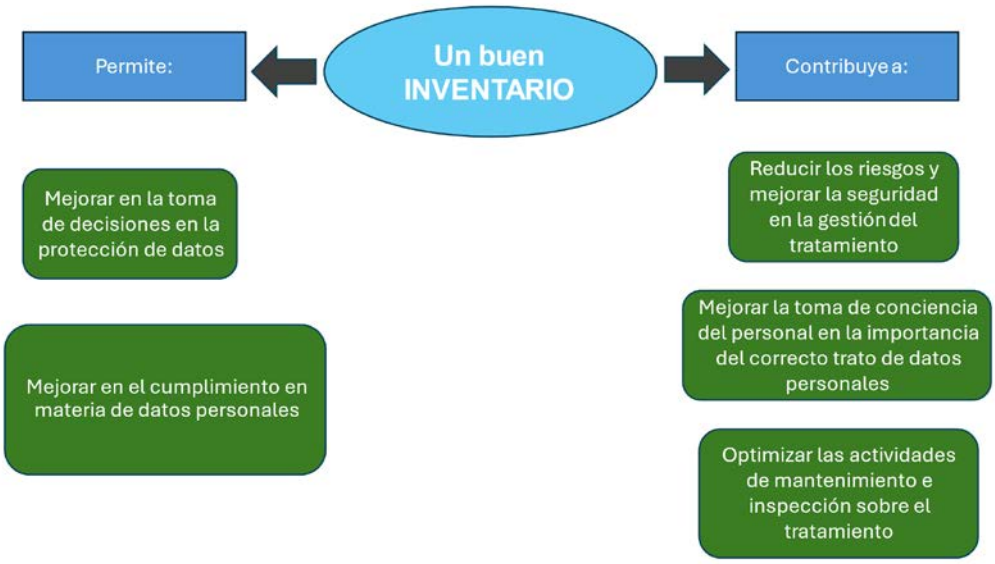
REGISTRO ACTIVIDADES -INVENTARIO ACTIVOS

REGISTRO	INVENTARIO
• **Obligatorio** para algunos sujetos (art. 30 RGPD)	• **No** es en ningún caso obligatorio
• Tiene un **contenido** mínimo (art. 30 RGPD)	• **No** tiene un contenido mínimo fijado normativamente
• Se confecciona sobre la base de las **actividades** de tratamiento atendiendo a la finalidad que se persigue con el mismo	• Se confecciona sobre la base de los **activos** implicados en los tratamientos

Ambos

Son instrumentos para la gestión de riesgos en materia de protección de datos personales desde enfoques diferentes: desde la actividad del tratamiento atendiendo a la finalidad que persigue o desde el activo implicado en el mismo.

Y contribuyen a cumplir con el principio de responsabilidad proactiva que impone el Reglamento (EU) 2016/679, Reglamento General de Protección de Datos.


Un buen INVENTARIO
Permite:
Mejorar en la toma de decisiones en la protección de datos
Mejorar en el cumplimiento en materia de datos personales
Contribuye a:
Reducir los riesgos y mejorar la seguridad en la gestión del tratamiento
Mejorar la toma de conciencia del personal en la importancia del correcto trato de datos personales
Optimizar las actividades de mantenimiento e inspección sobre el tratamiento

PROCEDIMIENTO PARA EL EJERCICIO DE DERECHOS

Mercè Arderiu Usart, Letrada-DPD del Parlamento de Cataluña

El procedimiento para el ejercicio de cualquiera de los derechos en protección de datos personales requiere seguir los pasos que se detallan a continuación:

1º Rellenar el formulario correspondiente al derecho de acceso, rectificación, cancelación, oposición, limitación o portabilidad que se ejerce. El nombre del derecho que se quiere ejercer parece indicado en el encabezamiento del formulario.

2º Enviar el formulario completado al Delegado de protección de datos [DPD] del Parlamento [dpd@parlamento] o bien al responsable del tratamiento [Secretaria General o Mesa del Parlamento].

3º A continuación se abren tres posibilidades:

a) El responsable responde facilitando el ejercicio del derecho (conformidad)

b) El responsable no admite el ejercicio del derecho (disconformidad)

c) No se recibe ninguna respuesta (silencio)

4º En el supuesto de disconformidad (b) o de que no se responda a la petición formulada (c) se plantean tres posibilidades:

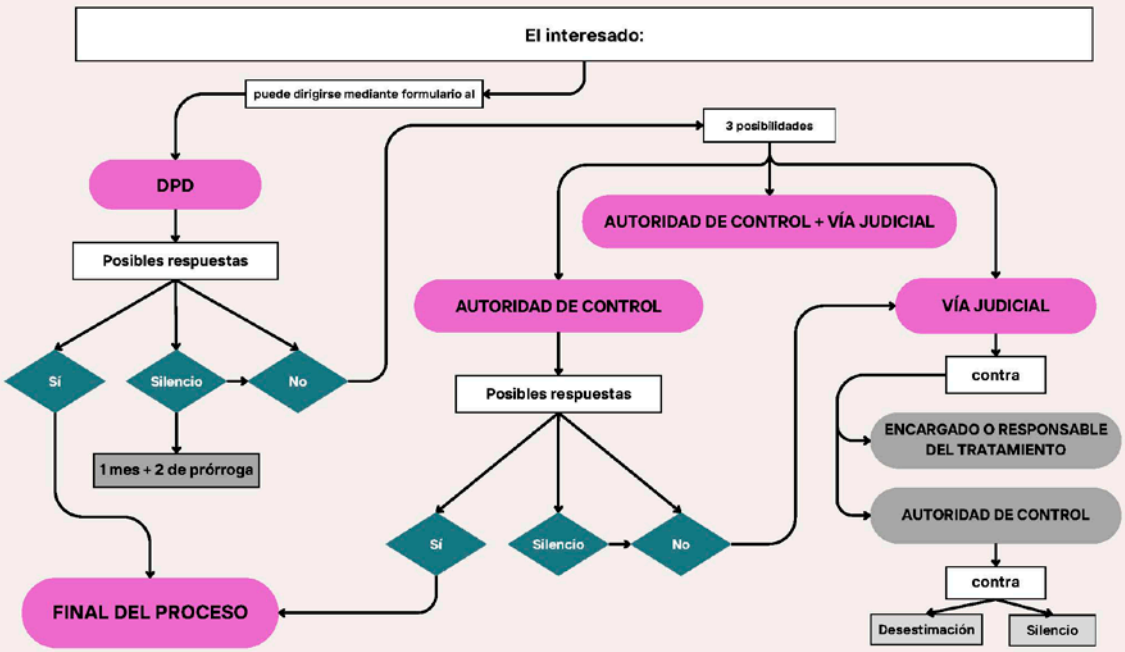
1ª Se puede presentar una reclamación ante la autoridad de control competente.

2ª Se puede plantear una reclamación judicial contra el responsable o contra la autoridad de control si ésta no responde durante tres meses o no se está de acuerdo con su decisión.

3º Se puede plantear el ejercicio concurrente de las dos posibilidades, es decir, la reclamación ante la autoridad de control y la reclamación judicial.

Esquema de procedimientos

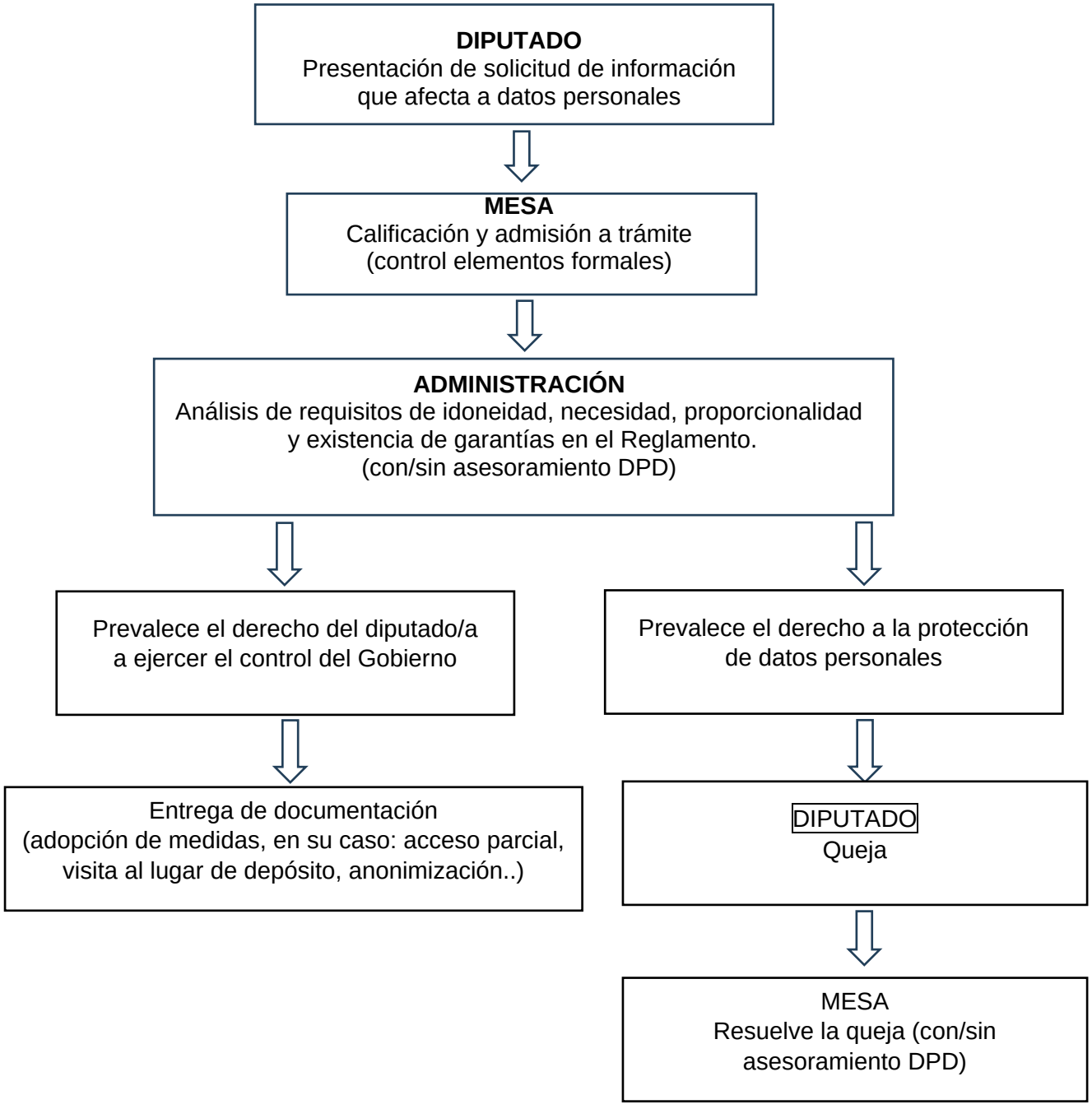
PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS



SOLICITUDES DE INFORMACIÓN

Blanca Belmonte Peláez, Letrada-DPD de la Junta General del Principado de Asturias

ESQUEMA DEL PROCEDIMIENTO DE LAS SOLICITUDES DE INFORMACIÓN



ANEXO IV. REDES SOCIALES

María Aneiros Gónzalez, Letrada-DPD del Parlamento de Galicia

Parlamento de Andalucía	facebook.com/parlamentodeandalucia.es	@parlamentoand	@parlamentoand	@ParlamentoAndalucia	https://www.flickr.com/photos/parlamentodeandalucia/	https://t.me/ParlamentodeAhttps://t.me/ParlamentodeAndalucia
Cortes de Aragón	facebook.com/cortesdearagon	@cortes_aragon	@cortes.aragon	@CortesAragon	https://www.flickr.com/photos/CortesAragon	
Junta General del Principado de Asturias	https://www.facebook.com/people/Junta-General-del-Principado-de-Asturias/100064652442697/	@JuntaAsturias		@JuntaGeneralPrincipadoAsturias		https://www.linkedin.com/company/junta-general-del-principado-de-asturias
Parlamento de las Islas Baleares		@ParlamentIB	@parlamentib	@canalparlamentdelesillesba5117		
Parlamento de Canarias	facebook.com/parlamentodecanarias	@parcan	@parlamentocanarias	@ParcanEs	https://www.flickr.com/photos/parlamentodecanarias/	
Parlamento de Cantabria	facebook.com/parlamentodecantabria	@parlacan	@parlacan	@parlamentodecantabria	https://www.flickr.com/photos/parlamentodecantabria/	
Cortes de Castilla-La Mancha	facebook.com/cortesclm	@cortesclm	@cortesclm	@CortesdeCastillaLaMancha	https://www.flickr.com/photos/cortesclm/	
Cortes de Castilla y León	facebook.com/cortesdecastillayleon	@cortes_CYL	@cortescastillayleon	@cortesdecastillayleon1694		
Parlamento de Cataluña	facebook.com/parlament.cat	@parlamentcat	@parlamentcat	@ParlamentCatalunya		
Asamblea de Extramadura	facebook.com/AsambleaExtremadura	@Asamblea_Ex	@asamblea_ex	@ParlamentodeExtremadura	https://www.flickr.com/photos/asambleaextremadura/	
Parlamento de Galicia	facebook.com/parlamentodegalicia	@Par_Gal				

Asamblea de Madrid	facebook.com/asambleamadrid/	@asambleamadrid	@asambleamadrid	@asambleademadrid336		
Asamblea Regional de Murcia	facebook.com/asambleamurcia/		@asambleregionalmurcia	@AsambleamurciaEs		
Parlamento de Navarra		@parlamentoNA		@parlamentodenavarra-nafarr2667		
Parlamento Vasco	facebook.com/legebiltzarra	@PVasco_EuskoL			http://www.flickr.com/photos/parlamentovasco/	
Parlamento de la Rioja	facebook.com/ParlamentodeLaRioja	@ParlamentoRioja	@parlamento_larioja	@parlamentodelarioja3400		
Cortes Valencianas	facebook.com/cortsval	@cortsval	@corts_valencianes	@LesCortsValencianes	https://www.flickr.com/photos/cortsval	