- XNET


Privacidad,
Protección de Datos
vs
Abusos
Institucionalizados
Informe y Propuestas Legislativas

Xnet

- XNET

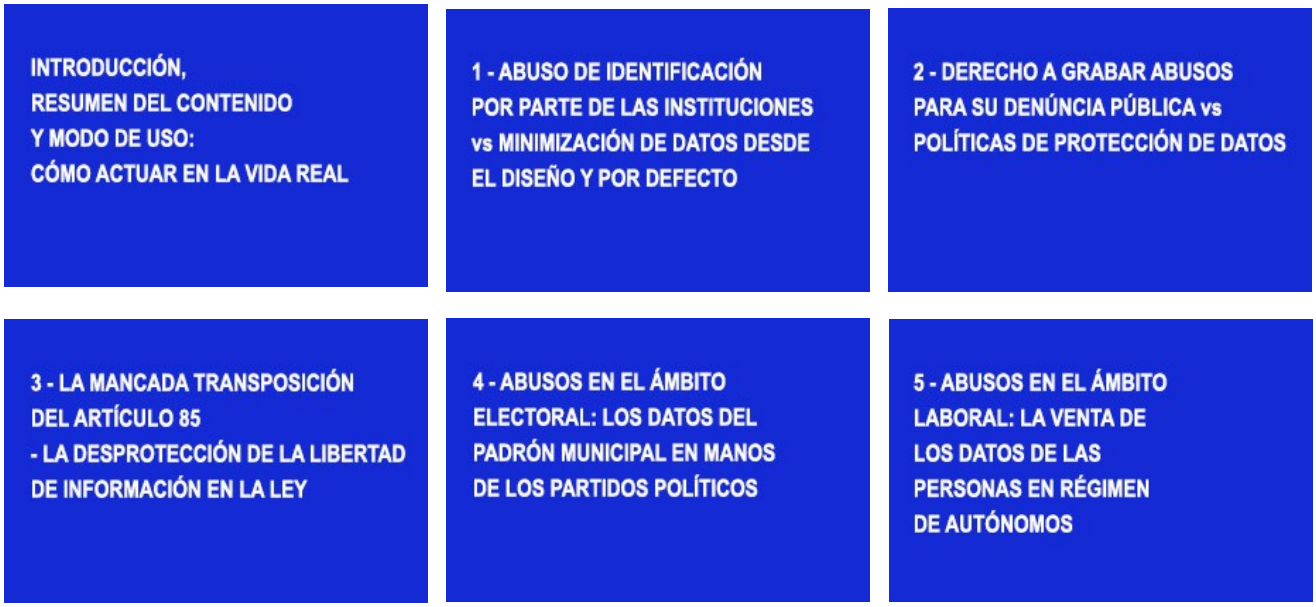
PRIVACIDAD, PROTECCIÓN DE DATOS Y ABUSOS INSTITUCIONALIZADOS

Por Xnet

Transparencia para las instituciones, privacidad para las personas

Reformas de las políticas de datos para corregir la asimetría y desprotección de las personas frente a las instituciones

- **XNET**



De cada apartado el presente informe aporta:

- RECOMENDACIONES
    - QUÉ PIDE **XNET** A LA Y EL LEGISLADOR
    - RECOMENDACIONES DE BUENAS PRÁCTICAS PARA LAS INSTITUCIONES Y EMPRESAS SISTÉMICAS ANTES Y DESPUÉS DE LA MODIFICACIÓN LEGISLATIVA
- ENMIENDAS DE LEY

En anexo por cada apartado:

- ANÁLISIS DEL DESARROLLO LEGISLATIVO (Excepción: en la parte 1 este apartado va en el cuerpo principal, no en anexo)
- ANÁLISIS DE LA JURISPRUDENCIA Y RESOLUCIONES RELEVANTES NACIONALES E INTERNACIONALES
- LISTADO DE LEGISLACIONES Y ARTÍCULOS RELEVANTES

INTRODUCCIÓN

El derecho a la protección de datos personales es un derecho fundamental relacionado con la privacidad que garantiza a la persona el control sobre sus datos, sobre su uso y destino. En pocas palabras, hablar de datos es hablar de control; es preguntarse sobre quién puede saber quiénes somos, dónde vivimos, qué hacemos durante el día y durante la noche; qué gustos, convicciones, vicios, placeres, dolores tenemos, etc. Es un derecho que debería ser respetado tanto por parte de organismos públicos como privados. Se ha hablado mucho de los abusos con los datos personales por parte de Facebook y otras compañías privadas, pero en cambio, se han comentado poco los incumplimientos por parte de Administraciones públicas o instituciones, las políticas que socavan la privacidad del conjunto de la ciudadanía, **los pequeños (o grandes) abusos cotidianos a los que se somete a las personas.**

En este contexto, en Xnet venimos denunciado desde hace tiempo un uso perverso de la "protección de datos"[1]: en muchas ocasiones se utiliza **la protección de datos como excusa tanto para esconder y proteger la corrupción como para tapar malas prácticas o inercias, incompetencias o abusos institucionales.**

El Reglamento Europeo de Protección de Datos (conocido por las siglas RGPD), cuya entrada en aplicación ha culminado en mayo de 2018, que todos recordamos por los infinitos mensajes de consentimiento que hemos empezado a recibir desde entonces, ha sido en realidad el resultado de más de una década de lucha de la sociedad civil organizada para que se garanticen los derechos a la privacidad de las personas y se actualicen al entorno digital[2]. La más beligerante ha sido la sociedad civil alemana que sabe lo que significa que los poderes establecidos tengan todos tus datos; sufrió a mano de la Stasi la más grande operación de vigilancia y recolección de datos personales jamás conocida en época predigital.

Con el RGPD conseguimos poner un primer freno -mejorable, pero firme- a los intereses corporativos o del Estado de control en la explotación del nuevo oro que son nuestros datos personales.

Pero es solo la primera piedra. Debemos seguir. Debemos utilizar esta primera e importante victoria para afianzar la lucha por nuestra privacidad y al mismo tiempo para que no sea **excusa ni refugio para malas prácticas** ni para impedir el derecho a la información y la denuncia de abusos.

Como herramienta para conseguirlo, Xnet presentamos el presente informe. Son más de 200 páginas que quieren explicar qué flancos están descubiertos y qué debemos hacer para protegerlos.

---

[1] https://blogs.publico.es/otrasmiradas/15834/proteccion-datos-obstaculo-lucha-corrupcion/
[2] https://xnet-x.net/breve-guia-nuevo-reglamento-europeo-proteccion-datos-batalla-de-cuatro-anos/

Se compone de 5 partes de las que ahora publicamos las primeras cuatro.

1 – ABUSO DE IDENTIFICACIÓN POR PARTE DE LAS INSTITUCIONES vs MINIMIZACIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

2 – DERECHO A GRABAR ABUSOS PARA SU DENÚNCIA PÚBLICA Y POLÍTICAS DE PROTECCIÓN DE DATOS

3 – LA MANCADA TRANSPOSICIÓN DEL ARTÍCULO 85 EN ESPAÑA – LA DESPROTECCIÓN DE LA LIBERTAD DE INFORMACIÓN EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

4 – ABUSOS EN EL ÁMBITO ELECTORAL: CÓMO HEMOS LLEGADO A QUE NOS PAREZCA NORMAL QUE LOS DATOS DEL PADRÓN MUNICIPAL ACABEN EN MANOS DE LOS PARTIDOS POLÍTICOS

5 – ABUSOS EN EL ÁMBITO LABORAL: LA VENTA DE LOS DATOS DE LAS PERSONAS EN RÉGIMEN DE AUTÓNOMOS

Cada una de estas partes va acompañada de **propuestas jurídico-legislativas para cambiar la situación**. Cada una de estas entregas implica pedir al o a los Gobiernos, al Congreso o a los Parlamentos y a los órganos competentes cambios en la legislación o en las políticas necesarios para que la ley de protección de datos sirva para proteger la privacidad de los ciudadanos y no para garantizar la impunidad de los poderosos.

Publicamos estas medidas abiertas a comentarios y enmiendas para que fueran mejoradas. Ahora están listas para ser reclamadas hasta conseguirlas.

En todo este trabajo hay **tres hilos conductores fundamentales**:

- El primero es una fuerza que nos da el RGPD. Es el **principio de minimización**. Nadie nos debe pedir o sonsacar más datos de los necesarios. Debemos saber que podemos ampararnos con fuerza en este principio. A día de hoy pedir a qué hora abre una ventanilla o llamar a una empresa de suministros para saber las tarifas requiere que te identifiques, por no hablar de cuando se pide información más compleja para destapar abusos o injusticias. Esto tiene que acabar.

- El segundo hilo conductor es una debilidad del RGPD. Permite que se nos pidan todo tipo de datos personales alegando “intereses legítimos”. Los países como el nuestro que no han delimitado cuáles son estos “intereses legítimos” ni piden que afloren y se detallen para poder ser puestos en discusión, abren la puerta a todo tipo de arbitrariedades y abusos. Esta fórmula se utiliza cuando no se dispone de base jurídica sólida o suficientemente justificada. Por respeto a los derechos, libertades e intereses de las personas no debería ser posible escudarse en extremos que sirven de cajón de sastre y que acaban invalidado el espíritu de la normativa. Los “intereses legítimos” que considere esta o aquella empresa o institución, no deben primar por encima de los derechos e intereses de las personas. Queremos que se garantice **el principio de privacidad desde el diseño y por defecto**.

- Por último, la protección de datos **no puede ser excusa para limitar el derecho a la información y la lucha contra la corrupción y los abusos**: desde los discos duros del PP que podían ser prueba de un posible caso de corrupción y que destruyeron alegando protección de datos[3], a la votación que se perdió para la publicación de hoja de servicio de Billy el Niño porque quien votó en contra lo hizo eximiendo protección de datos[4], nos encontramos esta "motivación" una y otra vez. Para los periodistas y los activistas contra la corrupción, estas escusas son los muros que nos encontramos a diario.

RESUMEN DEL CONTENIDO

Parte 1 - Abuso de identificación por parte de las instituciones vs minimización de datos desde el diseño y por defecto

En España existe una tendencia abusiva a pedir más datos de los necesarios cuando alguien lleva a cabo una simple petición a cualquier institución, algo que la aprobación en 2015 de la Ley de Procedimiento Administrativo e incluso la Ley de Transparencia agravan al establecer la verificación de la identidad de las y los interesados como obligatoria. Esto se debe a que, por defecto, toda relación entre ciudadanía y administración se considera "trámite administrativo", y eso incluye pedir información que por ley debería ser pública. Bien, por qué no. Si no fuera que "trámite administrativo" todavía significa poder, subordinación y jerarquía. El motivo de que esto ocurra no está en la lógica y menos en la lógica ágil de la era digital; tampoco en una idea de demo-cracia actualizada: es la sociedad civil que debe poder vigilar sus instituciones y no al revés.

Así **Xnet denuncia que nuestras leyes administrativas colisionan con un principio básico de una Ley superior**: el principio de **minimización** del Reglamento Europeo de Protección de Datos que establece que sólo deben recogerse los datos adecuados, pertinentes y no excesivos de acuerdo con los fines para los que son recogidos, y que se ha de explicar qué datos se recogen y por qué.

Se debe proteger al débil y controlar al fuerte ya que existe una clara asimetría entre los poderes establecidos, que nos pueden vigilar, y la ciudadanía de a pie que debe luchar y exponerse para acceder a información que debería ser suya por democracia (además de porque la pagamos entre todxs).

Parte de la lucha para una democracia real es la de acabar con esta asimetría. O sea: conquistar el acceso libre y sin amenazas a la información, sin el cual no podemos vigilar y decidir ni luchar contra la corrupción y los abusos, y ponerlo en equilibrio con el derecho a la privacidad, desenmascarando falsas ambigüedades.

Parte 2 - Derecho a grabar abusos para su denuncia pública y políticas de protección de datos

Y aquí la otra cara de la moneda. Si por un lado se nos piden muchos datos, por el otro a los poderes establecidos mucho les cuesta dar los suyos. Es otro clásico: apelar a la protección de datos para sancionar el uso (es decir, divulgación) de información como las grabaciones de funcionarios cometiendo excesos (policías, por ejemplo). Entre 2016 y 2018 se impusieron 113 sanciones en aplicación de la Ley Mordaza que supusieron un total de 70.522 euros contra los afectados. Este marco normativo ha ejercido un poderoso efecto disuasorio para la denuncia de abusos sistémicos. Pero, contrariamente a lo que se cree, el obstáculo más monolítico para grabar y sobre todo para difundir la comisión de abusos institucionales o sistémicos no es solo la Ley mordaza, sino

[3] https://www.elmundo.es/espana/2019/06/27/5d14b2a1fdddff95718b465f.html
[4] https://elpais.com/politica/2020/02/04/actualidad/1580834062_879620.html

la jurisprudencia de la Ley Orgánica de Protección de Datos.

Pero atención, el diablo está en los detalles: desde Xnet valoramos positivamente todo avance hacia agilizar las denuncias de personas víctimas de la difusión de contenido de carácter privado sin su consentimiento. Xnet apoya la campaña #PuedesPararlo de la Agencia Española de Protección de Datos que fortalece la interpretación de su homólogo europeo al no aplicar la excepción de uso doméstico en estos casos cuando hay viralización (o sea, la información circula de forma que trasciende el ámbito doméstico).

Dicho esto, hay un detalle importante: es necesario diferenciar estos casos de aquellos en los que las grabaciones de las personas se hayan captado en su desempeño de un servicio al público, en lugar público o en actos públicos. En ningún caso podemos equiparar esta situación a la violación de la intimidad. Se ha de recalcar con énfasis que **es muy pernicioso para cualquier democracia que se precie utilizar el primer caso – el de vulneración de derechos en la difusión de información íntima – para impedir lo segundo – la libertad de información en el interés público para divulgar abusos.**

Parte 3 - La desprotección de la libertad de información en la Ley Orgánica de Protección de Datos

Por todo ello es imprescindible por parte del legislador la correcta transposición del artículo 85 del RGPD que exige la armonización de la privacidad con la libertad de información y de expresión.
Cuando en 2018 se adaptó el ordenamiento jurídico español al RGPD con la Ley Orgánica Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), Xnet intentó sin éxito que se llevara a cabo. La LOPDGDD tiene algunas características embrionarias novedosas y loables respecto a los derechos digitales, pero también numerosas fragilidades, como veremos. Sobre la transposición del artículo 85, la negativa que recibió Xnet por parte del legislador fue que “esto lo resuelven los tribunales”. Los periodistas saben bien que no son pocas las veces que aquellos perjudicados por sus investigaciones pleitean para desgastar a los medios, aunque el caso acabe sobreseyéndose. Ante una querella, un medio se ve obligado a movilizar recursos para defenderse: y eso compromete la investigación periodística, algo de lo que no vamos precisamente sobrados. **Peor todavía es la situación de la o el alertador, persona corriente que desvela un abuso** (véase: LINK -> https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/).

La aproximación de “esto lo resuelven los tribunales” es una aproximación peligrosa y elitista ya que implica que la defensa de la libertad de expresión e información es garantizada solo para quién pueda permitirse pleitear. Preferimos que **se establezcan criterios claros para que todo el mundo pueda ejercer sus derechos con seguridad y sin temor a ser sancionado.**

La protección de datos es demasiadas veces un pretexto para invalidar pruebas. A parte de los ejemplos patrios anteriormente mencionados, el agravio democrático de no transponer la defensa de la libertad de información en ámbito de la protección de datos se ha hecho de manifiesto en toda su envergadura en la UE, en Rumanía, donde periodistas que investigaban corrupción gubernamental han sido amenazados con una sanción de 20 millones de euros por la Ley de protección de datos (los datos de los presuntos corruptos). Es por todo esto que la Association for Technology and Internet (ApTI) en colaboración con Privacy International y Xnet entre otras organizaciones europeas de defensa de derechos digitales, presentaron una queja ante la Comisión Europea hace un año. En aquella ocasión el portavoz de la Comisión Europea, Margaritis Schinas dijo: “Es sumamente importante que las autoridades de Rumanía implementen esta obligación [art.85] en el derecho nacional para (…) proteger las fuentes periodísticas (…) cuando sea necesario para respetar la libertad de información y expresión de los medios. (…) La protección de datos no puede utilizarse como una puerta trasera para forzar a los periodistas (…)”.

Una pena que la queja, un año después, todavía esté a la espera de respuesta.

Parte 4 - Cómo hemos llegado a que nos parezca normal que los datos del padrón municipal acaben en manos de los partidos políticos

Ya están muy extendidas las protestas para no recibir propaganda electoral a casa. No es suficiente.

Xnet niega la mayor.

El derecho a la protección de datos es un derecho fundamental que garantiza a las personas el control sobre sus datos, sobre su uso y su destino. Debe ser respetado tanto por parte de entidades públicas como privadas. Hay excepciones previstas por la normativa. Pero deberían ser las estrictamente necesarias para proteger algún bien superior.

Así que ¿cómo hemos llegado a que nos parezca normal que los datos del padrón municipal acaben en manos de los partidos políticos? Nombre y apellidos, provincia y municipio de residencia, distrito, sección y mesa electoral, domicilio, fecha de nacimiento y nacionalidad para los electores extranjeros. Increíble.

Al aprobar la nueva Ley Orgánica de Protección de Datos sólo se ha previsto la posibilidad de oponerse a que los datos sean enviados a los partidos (cosa que, por cierto, además no se cumple). Migajas de nuestros derechos legítimos.

Debería ser al revés si queremos ser fieles al principio de privacidad desde el diseño y por defecto: en el caso de querer ceder nuestros datos a los partidos para recibir la publicidad electoral, se debería tener que pedirlo.

Las **personas ni tan solo son informadas** cuando se inscriben al Padrón Municipal de habitantes. Esto vulnera otro de los principios esenciales del Reglamento Europeo de Protección de Datos, el principio de transparencia, que implica el conocimiento por parte de las personas, cuando proporcionan sus datos, de los usos a los que estos estarán destinados y a quienes serán comunicados en su caso, además de la obligación de **ofrecer la posibilidad de oponerse a ello.**

Xnet ofrece soluciones que pueden aplicarse de inmediato. Una pena que sean los únicos beneficiados de este atropello, los partidos, los que deben decidir si asumirlas.

Parte 5 – Abusos en el ámbito laboral: la venta de los datos de las personas en régimen de autónomos

Hemos hecho hincapié en nuestra vida cotidiana donde, tanto en el mundo físico como en el digital, utilizamos y permitimos que otros utilicen nuestros datos personales, y muchas veces no podemos escoger si queremos proporcionarlos. Estos casos deben ser motivados por el bien común, de lo contrario socavarían el derecho fundamental a nuestra privacidad.

Las y los autónomos, incluso antes de iniciar su actividad, se ven obligados a realizar declaraciones, inscripciones y registros ante diversas organizaciones para poder trabajar. La principal y coincidente en todo caso es la Agencia Tributaria; con las nuevas obligaciones de prevención de blanqueo de capitales, para quienes prestan ciertos servicios a empresas, también el Registro Mercantil.
Creemos que debe limitarse la posibilidad de difundir y vender los datos de los autónomos y más cuando estos datos no se han hecho manifiestamente públicos por los mismos, ni sean, en la mayoría de los casos, necesarios para comunicarse con ellos.
En cumplimiento del principio de minimización de datos, al no ser necesaria esta información, no debería estar disponible públicamente.

Existe un doble rasero en la aplicación de la protección de datos: mientras se oculta la propiedad de las empresas en paraísos fiscales, se venden los datos personales de los autónomos con menor poder adquisitivo.

La transparencia debe ser un instrumento para equilibrio de poderes y no está reñida con la preservación de la privacidad personal. Es absolutamente posible incluir las debidas salvaguardas para quiénes no tengan ingresos suficientes (3,5 veces el IPREM) para permitirse un domicilio profesional, mientras se permite conocer la titularidad de actividades profesionales.

Hemos propuesto modificaciones legales y recomendaciones para respetar la privacidad a la vez que la transparencia que debe guiar toda actuación empresarial por no ocultar posibles casos de corrupción o malas praxis.

En Xnet defendemos que la democracia sea entre otras cosas la vigilancia ciudadana sobre sus instituciones. Por esto se debe proteger al débil y controlar al fuerte ya que existe una clara asimetría entre los poderes establecidos y la ciudadanía.
Consideramos que parte de la lucha para una democracia real es la de acabar con esta asimetría.
Usando el nuevo Reglamento General de Protección de Datos, conquista de la sociedad civil organizada, vamos a empezar diversas acciones para seguir en el camino hacia una mayor y mejor democracia.

Manos a la obra.

MODO DE USO: CÓMO ACTUAR EN LA VIDA REAL UTILIZANDO LO QUE EXPLICAMOS EN #DATOSPORLIEBRE

A.- EXIGE LA MINIMIZACIÓN DE DATOS QUE RECOGEN LAS INSTITUCIONES Y CORPORACIONES

- Cuando te pidan tus datos personales, tanto mediante un formulario en papel, por Internet o incluso telefónicamente, asegúrate de que los datos que te requieren y que proporcionas son los mínimos indispensables para llevar a cabo el servicio que van a prestarte o la tarea que van a realizar (art. 5.1.c) del Reglamento General de Protección de Datos).
- Si no es así, tienes derecho a negarte y no pueden no prestarte el servicio por no querer dar más datos de los necesarios (art. 6.3 de la Ley Orgánica 3/2018 de Protección de Datos y garantía de los derechos digitales[5]). Si piden datos que no parecen adecuados y pertinentes de acuerdo con lo anterior y consideras que por ello piden más datos de los necesarios, infórmales de que el principio de minimización del Reglamento Europeo de Protección de Datos dice que no pueden pedirte tantos datos.
- ATENCIÓN, en el caso de las entidades públicas, la Ley 39/2015 del Procedimiento Administrativo (LPAC), exige acreditar la identidad de quienes realicen cualquier actuación ante las mismas comprobando el DNI o documento equivalente, y en el ámbito digital mediante Cl@ve PIN, Cl@ve Permanente o DNI electrónico. Por lo tanto, ante estas entidades, y hasta que se modifique la ley, se considera "normal" solicitar nombre, apellidos y DNI para la realización de cualquier trámite. Pero nada más. Si te piden más tienes derecho a negarte y no pueden no prestarte el servicio por no querer dar más datos de los necesarios.

B.- NO DEJES QUE LA PROTECCIÓN DE DATOS SEA UNA EXCUSA PARA NO DAR INFORMACIÓN QUE DEBE SER PÚBLICA

En caso de que una entidad niegue el acceso a información pública alegando protección de datos, debe tenerse en cuenta que esto no es siempre un motivo válido por el que no deba proporcionarse.

Si la información solicitada contiene datos personales, aun así, la institución podrá proporcionar la información si se disocian o anonimizan los datos de carácter personal, es decir, se impida identificar a las personas que aparecen en la información solicitada.

[5] Considerando (43) del RGPD: "Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento."

C.- DENUNCIAR LAS MALAS PRÁCTICAS

Si te encuentras en uno de estos casos, avísales de que comunicaras su mal proceder / mala praxis a la AEPD (solo si es sector público, puedes también acudir a la Autoridad autonómica en Cataluña, País Vasco y Andalucía). Para interponer una reclamación puedes hacerlo en los siguientes enlaces y puedes decir que lo haces siguiendo las directrices de Xnet, así será más eficaz, podremos reagrupar consultas para crear precedentes generales y tendrán más claro de qué estás hablando:

- AEPD:
  https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/solicitudReclamacion.jsf;jsessionid=1DV+dWm411scPx45IvR43Ezm
- APDCAT (Cataluña):
  https://apdcat.gencat.cat/ca/seu_electronica/tramits/denuncia/
- AVPD (País Vasco):
  https://www.avpd.euskadi.eus/s04-5273/es/contenidos/informacion/contacto/es_9493/es_contacto.html
- CTPDA (Andalucía):
  https://www.ctpdandalucia.es/sites/default/files/inline-files/formulario_de_reclamacion_pd.pdf

Si puedes, envíanos la respuesta que recibes a contact@xnet-x.net

1 – ABUSO DE IDENTIFICACIÓN POR PARTE DE LAS INSTITUCIONES

vs

MINIMIZACIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

- **XNET**

ÍNDICE

- **XNET**

- Jurisprudencia y resoluciones internacionales
- Jurisprudencia y resoluciones nacionales

LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

ABUSO DE IDENTIFICACIÓN POR PARTE DE LAS INSTITUCIONES vs MINIMIZACIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

"***En general, un buen sistema de protección de datos se caracteriza por el hecho de que las organizaciones responsables del tratamiento de nuestra información personal conocen muy bien sus obligaciones normativas y los ciudadanos conocemos muy bien nuestros derechos y los medios para ejercerlos****. La máxima expresión de este axioma es un estadio en el que la intervención de las autoridades de control no sea necesaria. Sin embargo, la realidad presente dista mucho de contar con un sistema perfecto capaz de autorregularse por sí mismo. (…) No en vano,* ***el modelo europeo de protección de datos centra su enfoque en el refuerzo de los derechos de los ciudadanos****, así como de las obligaciones de las organizaciones en el marco de la denominada responsabilidad proactiva. El cambio de paradigma que tuvo lugar con la aprobación del Reglamento General de Protección de Datos (en adelante, RGPD), profundiza en el empoderamiento de las personas sobre su propia información, cimentado en la transparencia de las organizaciones sobre el uso que se hace de la misma.* ***Se pretende erradicar la asimetría, el desequilibrio de poder que genera la opacidad****,* ***el "poder ver sin ser visto****" sobre el que disertaba Foucault hace ya medio siglo*".[6]

El derecho de las personas a acceder a la información pública es un derecho reconocido. Además, la casi totalidad de los Estados Miembros de la Unión Europea, ya disponían de alguna regulación sobre la transparencia y el derecho de acceso a la información pública cuando en España se aprobó la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, desarrollando el artículo 105.b) de la Constitución Española. A esto se le ha de añadir la obligación de las y los servidores públicos responsables de una tarea de identificarse cuando prestan un servicio (art. 53 de la Ley 39/2015).

La transparencia de las instituciones y corporaciones es fundamental para la democracia, el derecho a proporcionar y recibir información veraz, el control de los poderes públicos, la protección del interés general, preservar la rendición de cuentas y la integridad en el sector público, inhibiendo la corrupción o simplemente garantizar una suficiente agilidad de las instituciones en sus relaciones con la ciudadanía y las y los usuarios.

Aun así, no toda la información que debería ser publicada por las Administraciones y corporaciones sistémicas lo es, y no siempre se publica correctamente. Además, el acceso a la información que debería ser pública y no se encuentra publicada, se desincentiva a través de los requisitos que se exigen para obtenerla. Se mantiene así una todavía considerable opacidad de las instituciones, mientras se exige a la ciudadanía exponerse demasiado si quiere ejercer su derecho de acceso a la información. No nos estamos refiriendo solo a información de una cierta complejidad, sino también a información trivial y de uso cotidiano como la información sobre servicios, tarifas o similares.

En el Estado español encontramos prácticas establecidas desde hace años según las cuales se recogen datos desproporcionados de la ciudadanía, sin motivo aparente alguno, lo que se ha incrementado desde 2015 cuando se aprobó la nueva Ley de Procedimiento Administrativo (e incluso con la Ley de Transparencia) con la obligación de identificación de todas las personas usuarias sistemática y por defecto.

La aplicación del nuevo Reglamento europeo de Protección de Datos y la adaptación del derecho nacional al mismo hubiera permitido al legislador español revertir la situación sobre esta recogida de datos. Sin embargo, no encontramos en la nueva (2018) Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales ninguna mejora sustancial relacionada con este aspecto, y aunque en algunas corporaciones y administraciones se ha reducido la cantidad de datos que se recogen de las y los consumidores y usuarios, esta no es una práctica habitual.

En este contexto se enmarca también la histórica crítica de Xnet a la demagogia con la que se está legislando la justa reivindicación de la sociedad civil para que haya registros de grupos de intereses. En este momento, estos registros desorganizados obligan

[6] Isidro Gómez-Juarez. Firma invitada "Apología de la privacidad en la era del Gran Hermano". El País - Retina. https://retina.elpais.com/retina/2019/09/18/tendencias/1568807812_129427.amp.html?__twitter_impression=true

mucho más a la ciudadanía que no a quienes realmente deberían hacer aflorar, perpetrando la asimetría de poder y desincentivando la participación activa de las personas en la gestión pública[7].

- **Colisión con el Reglamento Europeo de Protección de Datos (RGPD)**

En el transcurso del posgrado dirigido por Simona Levi y Cristina Ribas sobre Tecnopolítica y Derechos en la Era Digital, algunos de las y los participantes han realizado solicitudes de información a distintas administraciones públicas y corporaciones sobre la cantidad de datos requeridos para la realización de estos trámites,; preguntando sobre el motivo de cada uno de dichos requerimientos, en algunos casos obtuvieron que se eliminasen algunos. La Administración requiere identificación para la realización de cualquier actuación o trámite ante la misma, incluyendo las solicitudes realizadas vía la Ley de Transparencia, además de otras comunicaciones tan sencillas como quejas y sugerencias. Lo establece la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC)[8] o, en otros casos, como veremos, la Ley de transparencia.

Las Administraciones Públicas tienen la obligación de pedir un gran número de datos. Esto se deriva del hecho anacrónico de que toda relación entre ciudadanía e instituciones se considere un "trámite administrativo", incluso para poder conocer informaciones que, por ley, por políticas o simplemente por lógica, deben ser públicas. Como veremos en el siguiente apartado, la ley que impone estos procedimientos farragosos creemos que colide con la Ley europea superior.

De hecho, una de las reivindicaciones históricas de la sociedad civil que han dado origen al Reglamento General de Protección de Datos al que está subordinada la Ley Orgánica de Protección de Datos española, es la de no pedir a la ciudadanía más datos de los estrictamente necesarios para que su privacidad no se vea expuesta por una circulación excesiva de datos personales. A este principio se le llama **"minimización"** y surge especialmente de las reivindicaciones de la sociedad civil alemana que sufrió a mano de la Stasi la más grande operación de vigilancia y recolección de datos personales jamás conocida en la época predigital.

Cuanto a los procedimientos de las grandes empresas sistémicas que también piden más datos de los necesarios y a las que se les debería aplicar directamente la obligación de minimización, esto no ocurre en la mayoría de los casos[9]. Esto es agravado por el hecho de que cuando los consumidores detectan irregularidades en el tratamiento de sus datos deban reclamar ante la Agencia Española de Protección de Datos (AEPD) para alertar de ello con resultados que llegan a cuenta gotas y no implican un cambio general de la situación. Creemos que la AEPD que dispone de poderes de supervisión sobre las empresas españolas, podría actuar previa y proactivamente, como en algunos casos ya se ha empezado a hacer.

Las leyes administrativas no sólo exigen que la identificación de los ciudadanos se realice, sino que impone condiciones a dicha identificación. Además, en el ámbito digital, es habitual que se exija la identificación por medio de certificados electrónicos u otros medios que las Administraciones establezcan[10]. En el caso de uso de certificados electrónicos, cada Administración escoge la información que recopila de los mismos[11], sin que en general se informe al ciudadano de los datos efectivamente recogidos ni de la finalidad por la que van a ser utilizados ulteriormente (a parte de la identificación del ciudadano).

[7] Véase: Sobre Grupos de Interés, por Xnet: https://xnet-x.net/sobre-grupos-de-interes/
[8] En concreto, su artículo 11.
[9] https://www.elperiodico.com/es/economia/20190927/solo-una-de-cada-cinco-empresas-espanolas-cumple-la-ley-de-proteccion-de-datos-7654202
[10] En concreto, esta obligación se establece en el artículo 9 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC).
[11] Según consulta telefónica formulada ante la Fábrica Nacional de la Moneda y Timbre.

Los requisitos de comprobación de la identidad de la ciudadanía para todo trámite que quieran llevar a cabo ante las administraciones públicas colisionan directamente con el RGPD según el cual sólo deben recogerse los datos adecuados, pertinentes y no excesivos de acuerdo con los fines para los que son recogidos y antes de recogerlos debe establecerse qué datos serán recogidos por defecto y por qué.

Las leyes administrativas aprobadas en 2013 y 2015 exigen por defecto que las administraciones recojan más datos de los que son necesarios para decidir si permiten a los solicitantes acceder a la información pública o no.

En principio, los datos identificativos no son necesarios para resolver y responder a las solicitudes de acceso a información pública. Por lo tanto, **consideramos que deberían modificarse estas normas** para permitir la realización solicitudes y otros trámites sin necesidad de identificar las personas, lo que permitiría que la ciudadanía pudiese controlar las instituciones sin miedo a represalias además de reducir al mismo tiempo la burocracia por la que debe pasarse actualmente para acceder a la información. Quienes deberían identificar el expediente para su seguimiento, trazabilidad y demostrar que están respondiendo a las peticiones, deberían ser solamente las instituciones por medio de códigos identificativos para el usuario u otros sistemas parecidos.

- **Identificación prescindible de los solicitantes de información pública**

En las comparaciones de las leyes de transparencia de distintos países publicadas en la página del Consejo de Transparencia y Buen Gobierno[12,13], puede observarse que en la mayoría de países la solicitud de información pública puede realizarse sin identificarse o utilizando una palabra de reconocimiento que no debe coincidir con el nombre real de la persona, **siendo España uno de los pocos países en que se verifica obligatoriamente que la identidad del solicitante coincide con su identidad real mediante la comprobación del DNI, documento equivalente o certificado electrónico**. Además, en la mayoría de Estados que se analizan no se requieren la utilización de certificados o firmas electrónicas y es suficiente disponer de una dirección de correo electrónico para realizar la solicitud. Los sistemas en los distintos países son los siguientes:

Identificación requerida	Seguimiento de la solicitud por parte de la Autoridad pública
Sin identificación	Autoridad pública debe darle curso
	Autoridad pública puede o no darle curso
Puede indicarse la identidad (voluntad del solicitante)	Autoridad debe tratar las solicitudes haciendo abstracción de la identidad del solicitante, salvo que la solicitud se refiera a datos personales o concurran circunstancias concretas

[12] Estudio comparado sobre normativa internacional en materia de derecho de acceso a la información pública del Consejo de Transparencia y Buen Gobierno en colaboración con el Instituto Nacional de la Administración Pública (https://www.consejodetransparencia.es/ct_Home/dam/jcr:38363e0e-62b9-40db-b726-419e2bf3dbe2/Estudio%20comparado%20sobre%20normativa%20internacional.epub)

[13] Informe sobre los requisitos de identificación de los solicitantes de acceso a la información pública de Emilio Guichot Reina, realizado por encargo del Consejo de Transparencia y Buen Gobierno (https://www.consejodetransparencia.es/dam/jcr:977fc69c-b6a9-4df6-90d8-25d5b75993a9/Informe_requisitos_identificacion.pdf).

	No se verifica que la identidad sea efectivamente real, lo que posibilita el uso de nombres ficticios o palabras
Debe indicarse la identidad del solicitante	En general no se verifica que la identidad sea efectivamente real, lo que posibilita el uso de nombres ficticios
	En general no se verifica que la identidad sea efectivamente real, lo que posibilita el uso de nombres ficticios Se comprueba la identificación real o se deniega el acceso a la información por tratarse de nombres manifiestamente ficticios o burlescos
	Se verifica la identidad sólo en casos concretos, como cuando se solicita acceso a documentos secretos o clasificados
	Se verifica que la identidad sea real antes de cursar la solicitud, mediante la comprobación del DNI, documento equivalente o certificado electrónico

Xnet, teniendo en cuenta que las normas internacionales permiten que los Estados reconozcan el derecho a la privacidad de quien pide información pública, salvo cuando la identificación sea esencial para tramitar la solicitud de información, considera que **requerir la identificación de los solicitantes es excesivo cuando se solicita el acceso a información pública**, **pudiendo en ciertos casos incluso desincentivar las solicitudes de información por temor a posibles represalias.** Además, debemos ser conscientes que algunas de las solicitudes de información que se realizan se refieren a información que debería haber sido publicada por la Administración. Por lo tanto, **es ilógico requerir al solicitante que se identifique cuando debería poder acceder a dicha información libremente y no puede hacerlo a causa del incumplimiento de la Administración de su deber de publicar dicha información.**

La identificación no es necesaria para acceder a información pública, ya que para decidir sobre las solicitudes, las administraciones deben hacerlo de manera objetiva, es decir, **tomando sólo en consideración la información que se solicita y los límites de acceso establecidos** por ejemplo en la Ley de transparencia como son la protección de datos personales de las personas que pueden aparecer en la información y la protección de intereses generales como pueden ser la seguridad pública, la protección del medio ambiente, intereses económicos y comerciales, etc.

Finalmente, **ha sido admitido incluso por el Consejo de Transparencia y Buen Gobierno que los sistemas de identificación electrónica** (Cl@ve y otros certificados electrónicos) **pueden ser percibidos como una traba para el ejercicio del derecho de acceso a la información pública**[14] en la medida que pueden resultar de difícil uso para la ciudadanía porque son sistemas complejos en cualquiera de sus modalidades, además de discriminar tanto a las personas jurídicas (empresas, asociaciones, etc.) que no tienen DNI ni pueden obtener certificados electrónicos y también discrimina las personas extranjeras que carecen de DNI o certificados electrónicos, e incluso europeas porque el sistema pensado para ellos no funciona para muchos países. De este modo**,** el Consejo de Transparencia y Buen Gobierno admite que los sistemas de identificación suponen una traba, sin entrar a valorar si la identificación puede percibirse también como una traba al ejercicio del derecho de acceso a la información pública.

- **Prescindible identificación en el uso de servicios privados**

Tenemos derecho a utilizar un servicio sin revelar datos adicionales a los necesarios para su uso. Si una empresa u organización desea procesar datos personales que no son estrictamente necesarios para la prestación de un determinado servicio (por ejemplo,

[14] **Memoria Anual del Consejo de Transparencia y Buen Gobierno de 2015, páginas 103-104:** https://www.consejodetransparencia.es/dam/jcr:b4186ab2-141b-464f-99ac-156c2587ffeb/memoria_completa.pdf

una aplicación de transporte que desea acceder a la lista de contactos de su teléfono), debe obtener el consentimiento explícito para procesar dichos datos y no debería plantearse como un “chantaje”, o sea sin datos no hay servicio. Existen salvedades en la Ley (art. 6.3. “No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual”), pero las personas no lo saben. Que una empresa crea que ciertos datos son útiles para la prestación de su servicio, no siempre significa que sean necesarios. Eso permite también, por ejemplo, caminar hacia evitar el acoso y el atropello de la presunción de inocencia que practican muchas multinacionales de servicios como las de telefonía, luz y gas cuando persiguen clientes o supuestos deudores, aunque no se haya demostrado que lo sean.

RECOMENDACIONES

Fruto del análisis realizado, para garantizar y proteger el derecho de las personas a acceder a la información, en línea con la legislación internacional de derechos humanos, desde XNet recomendamos:

- **Modificar las leyes administrativas, en particular la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC), la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales, además de los protocolos de actuación internos a las instituciones y empresas para proteger la identidad de la ciudadanía cuando no es necesaria para acceder a los servicios prestados por la Administración o empresas.**

  El Ministerio de Presidencia señaló en 2017 su voluntad de simplificar el sistema de identificación de los solicitantes de información[15]. También hay expertos que se han postulado por una modificación de la Ley para revisar los criterios de identificación de los solicitantes de acceso a la información pública para que no disuadirlos del ejercicio de este derecho[16].

  En este sentido, Xnet considera necesario modificar las leyes administrativas y la Ley de Transparencia, para utilizar las facultades que las normas internacionales dan al Estado para que la identificación de la ciudadanía se requiera solo en casos imprescindibles y debidamente justificados.

  En la misma línea, es conveniente prever disposiciones similares para que no se requiera la identificación personal de quienes, desde la sociedad civil organizada y sin ánimo de lucro, se reúnan o interpelen instituciones para aportar exigencias y recomendaciones para las legislaciones y políticas públicas. La transparencia bien entendida debería poner la presión sobre la agenda de las instituciones haciendo de obligado cumplimiento real la publicación de todas las reuniones llevadas a cabo tanto con lobistas profesionales como con la sociedad civil, esto sin necesidad de exponer los datos personales de estos últimos.

- **Garantizar la minimización por defecto de los datos que se recogen**

  Revisar las leyes y normas de uso frecuente, tanto por parte de operadores públicos como privados, que exigen la recogida de datos personales de las personas para asegurar que el derecho interno no colisiona con el europeo y estos no requieran por defecto más datos de los necesarios escudándose en la ley que deben aplicar, recogiendo solo los datos estrictamente necesarios para el servicio o finalidad que debe cumplirse. En caso de detectar que una norma requiere más datos de los que serían necesarios, promover regulaciones y leyes para su enmienda y adaptación a la nueva regulación de protección de datos personales.

- **Exigir que la información de interés público sea puesta a disposición de la ciudadanía sin tener que solicitarla.**

  Como muchas organizaciones de la sociedad civil pedimos, poner más énfasis y sanciones en que se publique efectiva y

[15] III Plan de Acción de España 2017-2019 de la Alianza para el Gobierno Abierto, de 27 de junio de 2017, págs. 23, 29 y 59. (https://transparencia.gob.es/transparencia/dam/jcr:74d66aee-760c-4962-983e-0b250fb583b8/2017_Junio_Spain_III_Plan_GA_OGP_vf.pdf)

[16] Joaquín Meseguer Yebra, en su artículo “el acceso a la información pública y los requerimientos de identificación” publicado en la Revista Española de Transparencia nº3, de 2016, cree que es “el momento de promover decididamente las modificaciones precisas para que sea factible la identificación del solicitante en los términos menos restrictivos para el ejercicio del derecho de acceso”.
(https://drive.google.com/file/d/0BzZV66dM4HCTeVhGOVBfM1preUU/view)

debidamente la información que debe ser pública. Por otra parte, no hay impedimento para que las administraciones públicas y otras instituciones y organizaciones obligadas y no obligadas por la Ley publiquen voluntariamente más información de la exigida que pueda ser de interés público. Si las instituciones hacen pública la información, el acceso será directo por parte de la ciudadanía, sin necesidad de identificación alguna, garantizando así un acceso universal y gratuito. Son necesarias mejores sanciones cuando se incumplan las obligaciones de publicación de información en el ámbito de la Administración, las instituciones, los partidos políticos y de las empresas sistémicas. A este propósito recordamos otra reivindicación histórica cuanto a ampliar los sujetos y objetos de aplicación de la Ley de transparencia.

Las autoridades nos han manifestado su preocupación por el uso comercial que se hace de las informaciones que ellas ofrecen en la resolución a las consultas que se les plantean. Consideramos que se puede paliar este problema publicando las consultas de utilidad pública. Cobrar por información institucional que se puede conseguir públicamente es claramente una mala praxis.

- **Inspeccionar las medidas adoptadas por parte de instituciones y empresas para proteger los datos personales de las personas**

La Agencia Española de Protección de Datos puede ampliar y normalizar la actuación proactiva que está llevando a cabo, haciendo extensivas a otras instituciones y empresas del mismo sector de actividad las investigaciones que realice. Cuanto a las grandes empresas es necesario que las sanciones sean proporcionadas pero consistentes ya que ha quedado demostrado que las sanciones suelen ser inferiores a lo que las corporaciones ganan recopilando más datos de los necesarios[17]. Debe reconocerse la obligación de quienes tratan datos personales de cumplir con las resoluciones de las autoridades cuando se encuentren en situaciones similares a las que se aplique una resolución.

- **Reforzar el derecho de la ciudadanía a conocer el uso y destino de sus datos**

Exigir que se informe correctamente a la ciudadanía sobre las comunicaciones de datos que se llevaran a cabo y las finalidades de las mismas, también en los trámites voluntarios, para que esté bien informada y ejerza plenamente su derecho a la autodeterminación informativa reconocido por primera vez en Europa fue en la sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983 y en España por el Tribunal Constitucional (STC 254/1993) que la llamó "libertad informática".

- **Acortar mejor las definiciones de conceptos demasiado ambiguos, especialmente el de “intereses legítimos”.**

[17] https://www.genbeta.com/redes-sociales-y-comunidades/multa-5-000-millones-dolares-a-facebook-ha-hecho-rico-a-mark-zuckerberg-a-sus-accionistas

RECOMENDACIONES DE BUENAS PRÁCTICAS PARA LAS INSTITUCIONES Y EMPRESAS SISTÉMICAS

ANTERIORES A MODIFICACIONES DE LA LEY PARA CREAR UN MARCO MÁS FAVORABLE AL RESPETO DE LAS LIBERTADES FUNDAMENTALES

- Publicar proactivamente la información institucional, de planificación, jurídica, económica, presupuestaria, estadística o de otra índole, Incluso la que no esté expresamente requerida por Ley, para así reducir el número de solicitudes de acceso, mediante una interpretación amplia de la obligación de publicidad activa prevista por la Ley de Transparencia. Valorar la aplicación de los límites al derecho de acceso de forma objetiva, haciendo por defecto abstracción de la identidad del solicitante.

- En los casos de información o consultas que se realicen frecuentemente a la institución, publicar la información y respuestas en un lugar fácilmente accesible, por ejemplo, mediante una página de preguntas/consultas frecuentes para que no sea preciso contactarla para su obtención. Las autoridades nos han manifestado su preocupación por el uso comercial que se hace de las informaciones que ellas ofrecen en la resolución a las consultas que se les plantean. Consideramos que se puede paliar este problema publicando las consultas de utilidad pública. Cobrar por información institucional que se puede conseguir públicamente es claramente una mala praxis.

- Revisar las políticas existentes en las administraciones, instituciones y grandes empresas sobre la recogida de datos personales para que no recojan más datos de los estrictamente legales y necesarios para los distintos trámites que la ciudadanía puede llevar a cabo.

- Iniciar un mayor número de procedimientos de inspección en las instituciones y grandes empresas para detectar informaciones que deberían ser públicas, pero que sin embargo no han sido objeto de publicación activa así como las infracciones de protección de datos, además de aplicar con mayor agilidad las resoluciones a los actores análogos.

- Adoptar actos normativos, protocolos o procedimientos internos en los que no se requiera la identificación de los solicitantes en base a los estándares internacionales que lo permiten, para así facilitar el ejercicio del derecho de acceso por parte de la ciudadanía. Ejemplos que pueden tomarse en cuenta para este fin son el Protocolo del Consejo General del Poder Judicial[18], la Ordenanza de Transparencia del Ayuntamiento de Madrid[19] o el Buzón Ético del Ayuntamiento de Barcelona, comentados en el análisis del desarrollo legislativo del presente informe.

  En la misma línea, es conveniente prever disposiciones similares para que no se requiera la identificación personal de quienes, desde la sociedad civil organizada y sin ánimo de lucro, aporten exigencias y recomendaciones para las legislaciones y políticas públicas y sí hacer de obligado cumplimiento la publicación por parte de los cargos públicos de todas las reuniones llevadas a cabo tanto con lobistas profesionales como con la sociedad civil, esto sin necesidad de exponer los datos personales de estos últimos.

- Desincentivar los incumplimientos.

- Incentivar estas prácticas en el sector privado.

[18] www.poderjudicial.es/stfls/CGPJ/TRANSPARENCIA/FICHEROS/20141215%20Ac%20CP%2018%20nov%202014%20Protocolo%20acceso%20transparecia.pdf

[19] https://sede.madrid.es/FrameWork/generacionPDF/ANM2016_108.pdf?idNormativa=3eabe8e52c796510VgnVCM1000001d4a900aRCRD&nombreFichero=ANM2016_108&cacheKey=61

ENMIENDAS A LA LEY

Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

Para alcanzar el fin propuesto, debemos solicitar la enmienda de dos artículos de la Ley:

Con la modificación del apartado 1 del Artículo 9. *"Sistemas de identificación de los interesados en el procedimiento"*, que quedaría redactado como sigue:

> *1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, salvo en los casos previstos en el segundo párrafo del apartado 1 del artículo 11 de esta Ley, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.*

Asimismo, se debe introducir un nuevo párrafo en el apartado 1 del Artículo 11. *"Uso de medios de identificación y firma en el procedimiento administrativo"*, que quedaría redactado como sigue:

> *1. Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.*
>
> *Los interesados no deberán acreditar su identidad cuando realicen simples consultas, quejas y sugerencias, peticiones de acceso a información pública o información de interés público de acuerdo con la Ley 19/2013 de Transparencia, acceso a la información púbica y buen gobierno.*

Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Para alcanzar el fin propuesto, debemos solicitar la enmienda de un artículo de la Ley, eliminando el punto "a) La identidad del solicitante" del apartado 2 del artículo 17 "Solicitud de acceso a la información", que quedaría redactado como sigue:

> *2. La solicitud podrá presentarse por cualquier medio que permita tener constancia de:*
>
> *a) La información que se solicita.*
>
> *b) Una dirección de contacto, preferentemente electrónica, a efectos de comunicaciones.*
>
> *c) En su caso, la modalidad que se prefiera para acceder a la información solicitada.*

Además de la introducción de un nuevo apartado 3 del mismo artículo, que quedaría redactado como sigue:

> *3. El solicitante no está obligado a proporcionar su identidad real en su solicitud de acceso a la información. La ausencia de identificación no será por si sola causa de rechazo o inadmisión de la solicitud.*
>
> *La identificación del solicitante sólo podrá requerirse cuando sea esencial para valorar su solicitud, debiendo la institución justificar debidamente dicho requerimiento.*

Los apartados 3 y 4 actuales pasarán a ser, respectivamente los apartados 4 y 5.

Para incrementar las posibilidades de control, tanto del sector público como privado, es altamente recomendable ampliar las

posibilidades de publicación de información de forma proactiva y prever la inclusión de corporaciones sistémicas dentro del ámbito de aplicación de la Ley de Transparencia. De mismo modo, es necesaria la definición de sanciones sin las cuales la Ley es papel mojado.

Para incrementar las posibilidades de control de los procedimientos para la elaboración de leyes, reglamentos, políticas, planes y programas públicos, es también altamente recomendable que se exija la publicación de las agendas y reuniones llevadas a cabo por miembros y responsables de las instituciones tanto con lobistas profesionales como con la sociedad civil. En el primer caso, identificando de forma clara el grupo o entidad representada y en el segundo aplicando la siguiente enmienda al artículo 11.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas:

Tampoco deberían indicarse datos personales tales como domicilios o similares cuando, desde la sociedad civil se organicen agrupaciones adhoc y sin ánimo de lucro, se reúnan o interpelen instituciones para aportar exigencias y recomendaciones para las legislaciones y políticas públicas, sugerencias, exigencias o críticas para la elaboración de leyes, reglamentos, políticas, planes y programas públicos (función de grupo de presión para el bien común), pudiendo registrar y proporcionar un nombre, plataforma, grupo informal o colectivo, para que estas agrupaciones tengan una protección igual o superior a la de los lobistas profesiones. Estos - las consultoras y los grupos de presión profesionales - deberán inscribirse en el registro con sus datos profesionales de identificación completos.

Modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales.

Para alcanzar el fin propuesto, debemos solicitar la enmienda de la Ley para acotar las definiciones de conceptos genéricos existentes tanto en el Reglamento (UE) 2016/679 General de Protección de Datos como en la Ley, tales como "tratamientos a gran escala", y específicamente las relativas al "interés legítimo" como base jurídica de legitimación del tratamiento.

Además de la introducción de un nuevo párrafo en el artículo 50. "Publicidad", que quedaría redactado como sigue:

> *La Agencia Española de Protección de Datos publicará las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 77.1 de esta ley orgánica, las que impongan medidas cautelares y las demás que disponga su Estatuto.*
>
> *Las resoluciones y sus indicaciones serán de obligado cumplimiento para todo responsable y/o encargado del tratamiento que se encuentre en una situación análoga a las de los supuestos objeto de las mismas.*

Modificación del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

Para alcanzar el fin propuesto, debemos solicitar la enmienda de un artículo de la Ley:

Con la introducción de dos nuevos apartados, g) y h), en el Artículo 8. *"Derechos básicos de los consumidores y usuarios"*, que quedaría redactado como sigue:

> *Son derechos básicos de los consumidores y usuarios:*
>
> *a) La protección contra los riesgos que puedan afectar su salud o seguridad.*
>
> *b) La protección de sus legítimos intereses económicos y sociales; en particular frente a las prácticas comerciales desleales y la inclusión de cláusulas abusivas en los contratos.*

c) La indemnización de los daños y la reparación de los perjuicios sufridos.

d) La información correcta sobre los diferentes bienes o servicios y la educación y divulgación para facilitar el conocimiento sobre su adecuado uso, consumo o disfrute.

e) La audiencia en consulta, la participación en el procedimiento de elaboración de las disposiciones generales que les afectan directamente y la representación de sus intereses, a través de las asociaciones, agrupaciones, federaciones o confederaciones de consumidores y usuarios legalmente constituidas.

f) La protección de sus derechos mediante procedimientos eficaces, en especial ante situaciones de inferioridad, subordinación e indefensión.

g) El derecho de acceso a la información de interés público sobre las empresas sujetos a esta Ley.

h) El derecho a la protección de sus datos personales, conforme la legislación en vigor, y en especial a los principios relativos al tratamiento previstos en el artículo 5 del Reglamento (UE) 2016/679 General de Protección de Datos.

ANÁLISIS DEL DESARROLLO LEGISLATIVO

El derecho de las personas a acceder a la información pública se encuentra protegido tanto a nivel internacional, como europeo ya sea como parte del derecho a la libertad de expresión e información o como derecho autónomo:

Protección internacional	Protección en el Consejo de Europa	Protección en la Unión Europea
Artículo 19 de la Declaración Universal de los Derechos Humanos, adoptada y proclamada por la Asamblea General de las Naciones Unidas en su resolución 217 A (III), de 10 de diciembre de 1948	Artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Convenio de Roma del 4 de noviembre de 1950, del Consejo de Europa.	Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.
Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, Resolución 2200 A (XXI) de la Asamblea General de las Naciones Unidas, aprobada el 16 de diciembre de 1966.	Convenio núm. 205 del Consejo de Europa sobre acceso a los documentos públicos de 2009 / Council of Europe Convention No. 205 on Access to Official Documents	

Además, en España se aprobó la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno (en adelante, LTAIBG) que desarrolla el artículo 105.b) de la Constitución Española, según el cual la ley debe regular "el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas."

En este sentido, el derecho de acceso a la información pública se encuentra específicamente previsto en el artículo 12 de la LTAIBG tanto en el ámbito estatal como en el ámbito autonómico. Se configura como un **derecho universal disponible a "todas las personas"**, es decir, que debe poder ejercerse sin ser víctima de discriminación alguna. La ley en este sentido concuerda con las normas internacionales que no distinguen entre los solicitantes, el derecho aplicándose tanto a personas físicas como jurídicas[20], sin discriminación por motivo de nacionalidad o residencia, incluyendo a europeos y extranjeros[21], o por edad, formación, recursos, circunstancias personales o condición o situación social.

Además, de acuerdo con el artículo 17.3 LTAIBG, **no debe justificarse ningún interés del solicitante** en la solicitud de información, sin que la administración pueda denegar el acceso por ello. Indicar los motivos por los que se solicita la información es opcional. En caso de indicarlos, la administración podrá tenerlos en cuenta a la hora de decidir si concede el acceso o no.

El artículo 13 de la LTAIBG define el concepto de información pública del siguiente modo:

"Se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren

[20] Sentencia del Tribunal Supremo de 3 de junio de 2011.
[21] Sentencia de la Audiencia Nacional de 10 de febrero de 1999.

en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones."

Además de esta información, **la ciudadanía tiene derecho a conocer otra información que debe ser objeto de publicación activa por parte de las Administraciones públicas**, esta información incluye "información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública" según el artículo 5 de la LTAIBG, que viene concretada en los siguientes artículos que se refieren a "información institucional, organizativa y de planificación" (artículo 6 LTAIBG), el "registro de actividades de tratamiento" (artículo 6bis LTAIBG), "información de relevancia jurídica" (artículo 7 LTAIBG) e "información económica, presupuestaria y estadística" (artículo 8 LTAIBG).

Los "sujetos incluidos en el ámbito de aplicación de este título", es decir, a los que se les puede solicitar información elaborada o adquirida por ellos incluyen las instituciones previstas en los artículos 2 y 4 de la LTAIBG:

Artículo 2. *Ámbito subjetivo de aplicación.*

1. Las disposiciones de este título se aplicarán a:

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla y las entidades que integran la Administración Local.

b) Las entidades gestoras y los servicios comunes de la Seguridad Social, así como las mutuas de accidentes de trabajo y enfermedades profesionales colaboradoras de la Seguridad Social.

c) Los organismos autónomos, las Agencias Estatales, las entidades públicas empresariales y las entidades de Derecho Público que, con independencia funcional o con una especial autonomía reconocida por la Ley, tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad.

d) Las entidades de Derecho Público con personalidad jurídica propia, vinculadas a cualquiera de las Administraciones Públicas o dependientes de ellas, incluidas las Universidades públicas.

e) Las corporaciones de Derecho Público, en lo relativo a sus actividades sujetas a Derecho Administrativo.

f) La Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con sus actividades sujetas a Derecho Administrativo.

g) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100.

h) Las fundaciones del sector público previstas en la legislación en materia de fundaciones.

i) Las asociaciones constituidas por las Administraciones, organismos y entidades previstos en este artículo. Se incluyen los órganos de cooperación previstos en el artículo 5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en la medida en que, por su peculiar naturaleza y por carecer de una estructura administrativa propia, le resulten aplicables las disposiciones de este título. En estos casos, el cumplimiento de las obligaciones derivadas de la presente Ley serán llevadas a cabo por la Administración que ostente la Secretaría del órgano de cooperación.

Artículo 4. *Obligación de suministrar información.*

Las personas físicas y jurídicas distintas de las referidas en los artículos anteriores que presten servicios públicos o ejerzan potestades administrativas estarán obligadas a suministrar a la Administración, organismo o entidad de las

previstas en el artículo 2.1 a la que se encuentren vinculadas, previo requerimiento, toda la información necesaria para el cumplimiento por aquéllos de las obligaciones previstas en este título. Esta obligación se extenderá a los adjudicatarios de contratos del sector público en los términos previstos en el respectivo contrato.

Se excluyen entre los obligados a proporcionar información cuando les es solicitada mediante el derecho de acceso a muchos sectores sensibles como los **partidos políticos, sindicatos, organizaciones empresariales.** Desde siempre las organizaciones de la sociedad civil que luchamos por la transparencia de las instituciones pedimos que se eliminen un gran número de estas exclusiones. En lo que respecta a los **límites del derecho de acceso a información pública**, se encuentran previstos en los artículos 14 y 15 de la LTAIBG, a veces también mal empelados o discutibles. En todo caso se limita el acceso a la información cuando la difusión de la misma pueda suponer un perjuicio para: La seguridad nacional; La defensa; Las relaciones exteriores; La seguridad pública; La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios; La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva; Las funciones administrativas de vigilancia, inspección y control; Los intereses económicos y comerciales; La política económica y monetaria; El secreto profesional y la propiedad intelectual e industrial: La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión; La protección del medio ambiente.

Cuando la información contenga datos “que revelen la ideología, afiliación sindical, religión o creencias (…) el origen racial, la salud o la vida sexual” o “incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor”, solo podrá proporcionarse acceso a la misma cuando la persona cuyos datos contiene la información hubiese dado su consentimiento expreso o los hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso (por ejemplo, publicándolos en redes sociales), salvo disociación de los mismos para impedir la identificación de la persona afectada.

Sobre este límite, el mismo artículo 15 LTAIBG admite que los datos personales que aparezcan en la información solicitada sean disociados para que el solicitante no pueda identificar la persona o personas afectadas, es decir, la información podrá proporcionarse al solicitante cuando los datos personales que no sean pertinentes y proporcionados sean anonimizados.

Hay motivos de inadmisión de las solicitudes que se encuentran enumerados en el artículo 18 LTAIBG, el cual indica que podrán inadmitirse las solicitudes cuando:

- La información solicitada esté en curso de elaboración o de publicación general;
- La información tenga carácter auxiliar o de apoyo (borradores, notas, opiniones, resúmenes, comunicaciones e informes internos);
- La información deba reelaborarse antes de su divulgación;
- La solicitud se haya dirigido a un órgano que no es competente y se desconozca cual es el competente;
- Se trate de solicitudes manifiestamente repetitivas o abusivas.

Puede observarse que la falta de identificación del solicitante de información no constituye pues ni un límite ni una causa de inadmisión de la solicitud de acceso a información pública, pero es preciso examinar con más atención este requisito.

Apuntes sobre el requisito de identificación:

El artículo 17.2 LTAIBG establece que la solicitud de derecho de acceso deberá presentarse por cualquier medio que permita **tener constancia de la identidad del solicitante**, el acceso debiendo tener lugar preferentemente por vía electrónica (artículo 22.1

LTAIBG).

Si bien es cierto que la LTAIBG no establece que es necesario comprobar la identidad mediante la presentación del DNI o por medio de certificados electrónicos, en este aspecto se aplica de manera supletoria la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPAC).

Encontramos en la LPAC el artículo 11.1 que requiere acreditar la identidad de la ciudadanía "con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo", incluyendo en el campo de aplicación de este articulo cualquier actuación o trámite ante la Administración Pública, como serían las solicitudes realizadas vía la Ley de Transparencia, además de otras comunicaciones, quejas y sugerencias. Un ejemplo de la aplicación de este artículo puede encontrarse en el Portal de Transparencia de la Administración General del Estado dónde se justifica solicitar la identificación de la ciudadanía que ejerce el derecho de acceso a información pública del modo siguiente:

> "¿Por qué debo identificarme?
>
> El ejercicio del Derecho de Acceso inicia con la administración un procedimiento administrativo que exige la identificación del solicitante."[22]

La LPAC no sólo exige comprobar la identidad de los solicitantes de información o personas que realizan algún trámite ante la Administración[23], sino que además impone condiciones a dicha comprobación en su artículo 9, debiendo proporcionarse el DNI o documento equivalente, y en el ámbito digital, es habitual que se exija la identificación por medio de certificados electrónicos u otros medios que las Administraciones establezcan (generalmente mediante: Cl@ve PIN, Cl@ve Permanente y DNI electrónico), como el mismo artículo indica.

Ha sido admitido incluso por el Consejo de Transparencia y Buen Gobierno en su memoria anual de 2015[24] que los sistemas de identificación electrónica (Cl@ve y otros certificados electrónicos) pueden ser una traba para el ejercicio del derecho de acceso a la información pública en la medida que pueden resultar de difícil uso para la ciudadanía porque son sistemas complejos en cualquiera de sus modalidades.

Además, de acuerdo con la misma memoria del Consejo de Transparencia y Buen Gobierno, estos sistemas de identificación electrónica resultan discriminatorios con:

- la ciudadanía española que reside en el extranjero y no dispone de identificación por medio del sistema Cl@ve, DNI electrónico o código PIN, porque dichos métodos de identificación sólo están disponibles para los residentes en España[25];
- las personas jurídicas, porque no tienen DNI ni pueden obtener certificados electrónicos desde la entrada en vigor del Reglamento Europeo de firma electrónica en julio de 2016;

---

[22] https://transparencia.gob.es/transparencia/transparencia_Home/index/Derecho-de-acceso-a-la-informacion-publica/Solicite-informacion.html#

[23] La ley anterior a la 39/2015, la Ley 30/1992 de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, no exigía la comprobación de la identidad de las personas que actuaban ante la Administración, sino que, como la LTAIBG exigía que indicasen sólo su nombre y apellidos, y en su caso de la persona que los representase (artículo 70.1.ª)).

[24] Memoria Anual del Consejo de Transparencia y Buen Gobierno de 2015, páginas 103-104: https://www.consejodetransparencia.es/dam/jcr:b4186ab2-141b-464f-99ac-156c2587ffeb/memoria_completa.pdf

[25] Informe sobre los requisitos de identificación de los solicitantes de acceso a la información pública de Emilio Guichot Reina, realizado por encargo del Consejo de Transparencia y Buen Gobierno, p. 24.

- la ciudadanía de la Unión Europea, porque aún poder verificar su identidad a través de la plataforma STORK de validación de firmas e identidades establecidas por los distintos Estados, no todos los países de la UE o del EEE están adheridos a dicha plataforma.

- las personas extranjeras de terceros países no pueden obtener acceso a información alguna al no poder ser comprobada su identidad, debiendo acudir en persona a las Embajadas españolas en caso de querer realizar una solicitud[26].

Suprimir el requisito de la identificación no solo serviría para ser coherentes con la regulación internacional del derecho de acceso a la información pública, sino que facilitaría su ejercicio, garantizaría que se trata efectivamente de un derecho universal, y reduciría la burocracia que debe cumplirse actualmente para ejercerlo.

Apuntes sobre la normativa de protección de datos personales:

De la localización de la regulación del derecho a la protección de datos personales en la Constitución Española (artículo 18.4CE), bajo el Título dedicado a "los derechos y deberes fundamentales" puede fácilmente deducirse que el mismo constituye un derecho fundamental cuya regulación prima sobre la regulación del derecho de acceso de los ciudadanos a la información pública (artículo 105.b) CE) y la legislación administrativa.

Siendo así, durante la adaptación del ordenamiento jurídico español al 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 o Reglamento General de Protección de Datos (en adelante, RGPD), consideramos que el legislador español, cuando fue adoptada la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), no tuvo suficientemente en cuenta dos principios para evitar que se recojan datos excesivos de la ciudadanía:

- **El principio de minimización de datos**: **no es un concepto nuevo en el ordenamiento jurídico español.**

El artículo 5.1.c) del RGPD establece que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados", a lo que el Considerando 39 del mismo RGPD añade que "los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios".

No sería un principio nuevo en el ordenamiento jurídico español[27]. Quizás inspirada de la doctrina del Tribunal Constitucional que ya

[26] Informe sobre los requisitos de identificación de los solicitantes de acceso a la información pública de Emilio Guichot Reina, realizado por encargo del Consejo de Transparencia y Buen Gobierno, p. 24.

[27] La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), preveía en cierto modo un principio de minimización al anunciar el principio de calidad de los datos en su artículo 4, según el cual "Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas

lo había establecido, la Federación Española de Municipios y Provincias aprobó una "Ordenanza tipo de transparencia, acceso a la información y reutilización"[28] la cual, en su artículo 26.1 indica que "Los órganos competentes para resolver las solicitudes de acceso a la información pública no requerirán a los solicitantes más datos sobre su identidad que los imprescindibles para poder resolver y notificar aquellas".

El **artículo 25 del RGPD** remitiendo y precisando el principio anterior, establece:

> "1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
>
> 2.El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
>
> 3.Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo. "

Así, el RGPD dice que cuando se diseña un tratamiento de datos personales, debe garantizarse que por defecto sólo sean objeto de tratamiento los datos necesarios.

En este caso, el legislador es quien diseñó el tratamiento consistente en la recogida y comprobación de los datos identificativos de los solicitantes de acceso a la información pública por ley, en concreto la LTAIBG de 2013 y la LPAC de 2015. El RGPD se aprobó en 2016 y la LOPDGDD en 2018. **En el proceso de elaboración de la LOPDGDD el legislador debió revisar normas de uso tan frecuente como las mencionadas para asegurar que el derecho interno no colisionaba con el europeo, pero no lo hizo. Así, nos encontramos que las administraciones públicas requieren por defecto más datos de los necesarios escudándose en la ley que deben aplicar, que no fue modificada para ser coherente con los estándares europeos.**

Confirmando nuestra posición, encontramos:

- El **RGPD**
- El **artículo 11 del RGPD, dedicado a los tratamientos que no requieren identificación**, que indica que "si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al

para las que se hayan obtenido."

[28] http://femp.femp.es/files/11-5133-fichero/Ordenanza%20Transparencia,%20Acceso%20y%20Reutilizaci%C3%B3n%20de%20la%20informaci%C3%B3n.pdf

interesado con la única finalidad de cumplir el presente Reglamento."

- La inclusión por parte del RGPD de la seudononimización como medida aplicable para garantizar el cumplimiento del mismo.

- El Reglamento (UE) 910/2014 sobre servicios de identificación electrónica y servicios fiduciarios para transacciones electrónicas en el mercado interior que además de recordar que la autenticación debe implicar exclusivamente el tratamiento de los datos identificativos adecuados, pertinentes y no excesivos para la concesión del acceso al servicio en línea de que se trate (considerando 11), establece la posibilidad de utilizar seudónimos (artículo 5) o de establecer niveles más bajos de identificación para ciertos servicios (considerando 15), incluidas las transacciones electrónicas que se llevan a cabo en los Estados miembros de la UE.

- **El Buzón Ético de Xnet[29] y el Ayuntamiento de Barcelona[30] y sus réplicas**

  Xnet ha sido pionera en España reivindicando la importancia de proteger a las personas frente a la asimetría con los poderes establecidos y en particular cuando las personas revelan abusos sistémicos para el interés general (whistleblowers/alertadores). En esta labor ha instalado por primera vez en una institución – el Ayuntamiento de Barcelona- un buzón de alerta contra abusos sistémico completamente anónimo. A través de este buzón, la ciudadanía puede enviar denuncias, pistas o indicios de irregularidades para que sean investigados por el Ayuntamiento, quien también puede remitirlas a la institución pertinente al efecto. Este buzón conserva el poder de la ciudadanía de decidir si revela o no su identidad, permitiendo comunicar la información tanto de forma confidencial, es decir, proporcionando la propia identidad, como de forma anónima.

  Este prototipo se ha replicado y continua replicándose en otras instituciones como las Oficina Antifraude de Catalunya y de la Comunidad Valenciana, entre otras y es recogido en la Proposición de Ley de Protección Integral de los Alertadores de Xnet, primera transposición europea de la Directiva (UE) 2019/1937, de 23 de octubre de 2019, del Parlamento Europeo y del Consejo sobre la Protección de las Personas que informen sobre infracciones, registrada en el Congreso de los Diputados: https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/.

- Ya dentro del marco de la inminente aprobación de la mencionada Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión[31], **la LOPDGDD permitió la presentación de denuncias anónimas a través de los sistemas de denuncias internas en su artículo 24.1**, según el cual:

  > "Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información."

  Siguiendo este precepto y el camino abierto por Xnet, la Agencia Española de Protección de Datos, con la aprobación de su Código Ético en enero de 2020[32], incorporó un canal de consulta y alerta[33] en los que no es preciso indicar la identidad de quién consulta o alerta sobre la comisión de incumplimientos del código ético, irregularidades o actos contrarios a la legalidad.

[29] https://xnet-x.net/buzon-xnet/
[30] https://xnet-x.net/buzon-denuncias-anonimas-ciudad-barcelona-bustia-etica/
[31] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019L1937&from=EN
[32] https://www.aepd.es/sites/default/files/2020-01/codigo-etico.pdf
[33] https://www.aepd.es/es/la-agencia/sostenibilidad/canal-etico-de-la-aepd

- **Consejo General del Poder Judicial**

Antes de la entrada en vigor de la LTAIBG el Consejo General del Poder Judicial (en adelante, CGPJ) puso en marcha su Portal de Transparencia y lo hizo sujetándose a los estándares internacionales fijados en el Convenio n.º 205 del Consejo de Europa sobre el Acceso a Documentos Públicos.

El 18 de noviembre de 2014 CGPJ adoptó un "Protocolo de Integración de la gestión de solicitudes de información de los ciudadanos en el funcionamiento de la organización interna del Consejo General del Poder Judicial"[34] donde se establece en su punto 1.1.1 lo siguiente:

> "**El CGPJ tramitará todas las solicitudes de información con independencia de los datos de identificación proporcionados.**
>
> Sólo cuando se requiera un acceso cualificado (por ejemplo, si se solicita el acceso presencial a una gran cantidad de documentación) se exigirá una identificación."

Justifica que no se requiera identificación del siguiente modo:

> "Aunque la Ley 19/2013 exige la identificación del solicitante, **la falta de necesidad de identificación del solicitante es un estándar internacionalmente fijado, al entenderse que el acceso a la información pública es un derecho fundamental de carácter universal en cuya garantía priman las obligaciones de transparencia de los poderes públicos frente a cualquier requisito impuesto al ciudadano que solicita el acceso**".

- **El Ayuntamiento de Madrid**:

En la Ordenanza de Transparencia del Ayuntamiento de Madrid[35], a parte de prever el régimen general aplicable de acuerdo con la LTAIBG, se estableció la posibilidad de solicitar el acceso a información pública sin identificación del solicitante, el cual sólo debe facilitar una dirección de correo electrónico para que el Ayuntamiento pueda comunicarle su decisión y, en su caso, la información solicitada. En todo caso, la Ordenanza indica que de no ser concedido el acceso a la información el solicitante no podrá impugnar la resolución, pero podrá volver a solicitarlo mediante la aplicación de la Ley de Transparencia, esta vez haciendo constar su identidad.

[34] www.poderjudicial.es/stfls/CGPJ/TRANSPARENCIA/FICHEROS/20141215%20Ac%20CP%2018%20nov%202014%20Protocolo%20acceso%20transparecia.pdf

[35] https://sede.madrid.es/FrameWork/generacionPDF/ANM2016_108.pdf?idNormativa=3eabe8e52c796510VgnVCM1000001d4a900aRCRD&nombreFichero=ANM2016_108&cacheKey=61

En anexo:

- ANÁLISIS DE LA JURISPRUDENCIA Y RESOLUCIONES RELEVANTES
  - Jurisprudencia y resoluciones internacionales
  - Jurisprudencia y resoluciones nacionales

- LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

2 - DERECHO A GRABAR ABUSOS PARA SU DENÚNCIA PÚBLICA Y POLÍTICAS DE PROTECCIÓN DE DATOS

ÍNDICE

b) Interpretación de la excepción doméstica

LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

DERECHO A GRABAR ABUSOS PARA SU DENÚNCIA PÚBLICA Y POLÍTICAS DE PROTECCIÓN DE DATOS

XNet, a propuesta de la Organización Internacional Witness y en el marco de la investigación del Relator Especial de Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, ha investigado el marco jurídico, la jurisprudencia y la práctica respecto al "Right to Record" en el Estado español: el derecho de las personas a grabar y hacer públicas las actuaciones de funcionarios públicos (policías u otros) u otros actores sistémicos que operan de cara al público o en el cumplimiento de sus funciones (corporaciones de servicios básicos) en el caso de posibles abusos o ilícitos.

La conclusión es que existe una gran inseguridad jurídica y desprotección de las personas que intentan monitorear y documentar la actuación de los poderes públicos o fácticos.

En síntesis, la situación es la siguiente:

- **Un derecho no amparado por la ley**

En España, la seguridad jurídica para, en caso de abusos o mala praxis, poder grabar o difundir las grabaciones de las actuaciones de funcionarios públicos u otros actores sistémicos que operan de cara al público mientras realizan sus funciones, es prácticamente nula.

La libertad de información está relativamente amparada para que no colida con otros derechos fundamentales reconocidos en el artículo 18 de la Constitución Española como el derecho al honor, a la privacidad y a la propia imagen cuando se trata de cargos públicos:

Artículo 8.2 de la Ley Orgánica 1/1982: *"No se reputará, con carácter general, intromisiones ilegítimas (…) cuando predomine un interés histórico, científico o cultural relevante. En particular, el derecho a la propia imagen no impedirá (…) su captación, reproducción o publicación (…) 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*".

Desde una perspectiva más general, no existe una seguridad jurídica estructurada en la legislación y depende en gran medida de la casuística y la jurisprudencia generada. Del análisis de la jurisprudencia existente se puede concluir que pueden considerarse lícitas las grabaciones cuando:

- Se realicen fuera del ámbito íntimo o privado.
- Se tenga el consentimiento o quien lo grabe sea parte de la conversación.
- Se realicen para un fin legítimo. Esto es básicamente para ser utilizadas como prueba en un proceso judicial, denunciar un delito, o en el ámbito de una relación negocial, pero no se contempla, por ejemplo, la denuncia de abusos.

En general, las salvedades jurisprudenciales resultan ser muy frágiles y la difusión de las grabaciones se encuentra fácilmente penalizada, con excepciones en el caso de los medios de comunicación.

En el momento de la publicación inicial de este informe, criticamos el tratamiento particular que se hacía en el caso de los cuerpos de seguridad, desde la Ley de Protección de la Seguridad Ciudadana aprobada en 2015, más conocida como «Ley Mordaza», donde si bien no se mencionaba el acto de grabar específicamente, se introducía el enfoque al menos "narrativo" de sancionar el uso no autorizado de grabaciones de imágenes de servidores públicos – policía en este caso -, penalizando hasta con multas de

30.000 euros el uso de grabaciones en casos en los que se considerase que podían poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación. Entre los años 2016 y 2018 se impusieron un total de 113 sanciones por una cuantía total de 70.552 Euros por este concepto[36]. Nótese que se habla del uso, pero muy fácilmente esto hace que se extrapole *de facto* a la misma grabación.

Tanto fue así que el 17 de Octubre de 2018 el Ministerio del Interior emitió una instrucción en la que recalcaba que la mera toma de imágenes o el tratamiento de los datos de los agentes no constituía infracción si no representaba un riesgo o peligro para ellos, su familia, las instalaciones o las operaciones policiales (Instrucción 13/2018, de 17 de octubre, de la Secretaría de Estado de Seguridad, sobre la práctica de los registros corporales externos, la interpretación de determinadas infracciones y cuestiones procedimentales en relación con la Ley Orgánica 4/2015, de 30 de marzo, de protección de la *seguridad ciudadana*)[37].

Por otra parte, la Instrucción reconocía "la posibilidad de identificar a la persona que haya tomado las imágenes, al objeto de proceder, en su caso, al ejercicio de las actuaciones oportunas para salvaguardar los derechos de los actuantes, o a su sanción administrativa o penal si se hiciese un ulterior uso irregular de los datos o imágenes en el sentido expuesto", lo cual era contradictorio, porque si la toma de imágenes antes mencionada no constituía una infracción administrativa, era difícil justificar la identificación por la hipotética comisión de una infracción por el uso del contenido grabado en un futuro hipotético[38].

Todo esto a pesar de que la ONU ha abordado esta cuestión en numerosas ocasiones[39], incluso en la reciente Resolución del Consejo de Derechos Humanos de junio de 2018 que reconoce el derecho a grabar y utilizar las grabaciones de forma explícita en el marco de "*La promoción y protección de los derechos humanos en el contexto de las protestas pacíficas*".

En general, el marco internacional de lucha contra la corrupción, los abusos y de protección de los llamados "alertadores" (*whistleblowers*) donde Xnet ha sido pionera[40] promueve la necesidad de que la ciudadanía pueda recoger y hacer públicas, incluso sin intermediarios, pruebas sin sufrir represalias, pero, como se puede comprobar, la praxis y marco jurídico españoles son fuertemente disuasorios, ya no solo para el uso de grabaciones sino también para su mera grabación.

Actualizamos este informe el 19 de noviembre de 2020 tras el dictamen del Tribunal Constitucional (https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2020_108/NOTA%20INFORMATIVA%20N%C2%BA%20108-2020.pdf) según el cual – en línea justamente con lo que estamos defendiendo -declara como inconstitucional el inciso de la Ley Mordaza que permitía sancionar el uso no autorizado de las imágenes de servidores públicos – policía en ese caso -.

---

[36] Según los datos estadísticos publicados por el Ministerio del Interior de España. Disponibles en: www.interior.gob.es/documents/642317/9256481/Seguridad+ciudadana+%28Ley+Org%C3%A1nica+4-2015%29%202017.zip/bb3f95d4-fc3b-4fe0-934e-519ac4eec9ca
y en: www.interior.gob.es/documents/642317/11039771/Seguridad+ciudadana+%28Ley+Org%C3%A1nica+4-2015%29%202018/c7e8abc1-b819-4b96-843b-4711b2aed777.
En 2016 se impusieron 32 sanciones por un valor de 19.377€, en 2017 41 sanciones por un valor de 25.695€ y en 2018 40 sanciones por un valor de 25.480€.

[37] Texto de la instrucción disponible en: https://www.eldiario.es/politica/Interior-ofensas-policia-respetuoso-adecuado_0_826268470.html

[38] En este mismo sentido lo expresa Francisco Miguel Fernández Caparrós, citando a Melero Alonso en: https://www.elsaltodiario.com/conquista-derecho/amordazar-ley-mordaza#

[39] Especialmente relevantes en este caso son: los artículos 6, 9 y 12 de la Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos, aprobados en la Resolución de la Asamblea General de la ONU (A/RES/53/144) del 8 de marzo de 1999; El Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Christof Heyns sobre el uso de la tecnología de la información y las comunicaciones para garantizar el derecho a la vida presentado en el 29° período de sesiones el Consejo de Derechos Humanos el 24 de Abril de 2015 (A/HRC/29/37); y el Informe conjunto del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación y el Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias acerca de la gestión adecuada de las manifestaciones presentado en el 31er período de sesiones del Consejo de Derechos Humanos el 4 de febrero de 2016 (A/HRC/31/66).

[40] Nos remitimos en este punto a la Proposición de Ley de Protección Integral de los Alertadores de Xnet, primera transposición europea de la Directiva (UE) 2019/1937, de 23 de octubre de 2019, del Parlamento Europeo y del Consejo sobre la Protección de las Personas que informen sobre infracciones, registrada en el Congreso de los Diputados: https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/

Por otra parte, se añade ulterior complejidad respecto al secreto de las comunicaciones, donde no se autoriza la grabación y/o difusión de conversaciones de terceros, penadas incluso con prisión (hasta 5 años en caso de difusión).

- **Las políticas de protección de datos como principal obstáculo para el uso de grabaciones de abusos**

Todo y así, contrariamente a lo que se suele creer, ni la "Ley Mordaza", ni los derechos al honor o a la propia imagen son o han sido los obstáculos más monolíticos para poder grabar y hacer públicos abusos por parte de servidores públicos o servicios sistémicos.

Las políticas de protección de datos son el principal obstáculo al derecho a grabar para poder difundir abusos, como parte del derecho a la libertad de información.

En ese marco, la difusión de las grabaciones siempre vulnera el derecho de Protección de datos si se interpreta la legislación considerando todas las grabaciones y su difusión como tratamientos y cesiones de datos personales.

La Agencia Española de Protección de Datos (AEPD), como parte de sus competencias, ha desarrollado criterios en sus decisiones, resoluciones e informes legales (específicamente el informe jurídico 0077/2013) en los que dicta que la grabación de imágenes o conversaciones de empleados públicos que desarrollan su trabajo y su difusión por Internet sin su consentimiento es ilegal, ya que se considera una cesión de datos personales.

En este sentido, la AEPD aplica la normativa de protección de datos a particulares, aunque en principio está pensada para ser aplicada a empresas ya que a los particulares se aplica la excepción de uso doméstico. Se les aplica la normativa fundamentándose en la doctrina jurídica prevista a nivel europeo desde 2003 que tiende a hacer responsables a los particulares[41] en situaciones en las que la divulgación de información se hace por medios en los que pierden el control de a quiénes alcanza la información, como las redes sociales. En este sentido no se aplica la excepción de uso doméstico; de un cierto modo se considera este tipo de difusión casi como una comunicación pública.

Xnet entiende y apoya que sea sancionable el particular que haga comunicación pública de información personal de terceros captada en el ámbito privado e íntimo, sin informarles ni obtener su consentimiento. Así se ha hecho en ocasiones por parte de la AEPD siguiendo esta doctrina (p. ej. fotografías íntimas o conversaciones privadas[42]). El canal prioritario establecido por la AEPD[43] a este efecto y la campaña #PuedesPararlo son una loable iniciativa al agilizar y hacer sostenible económicamente la preservación de la intimidad de las personas.

Por otra parte, pero, Xnet considera necesario diferenciar los casos en los que las grabaciones de las personas se hayan captado en su desempeño de un servicio al público, en lugar público o en actos públicos, para ampararse en la libertad de información y permitir denunciar y difundir grabaciones de abusos o irregularidades y de interés público.

Por ello es imprescindible por parte del legislador la correcta transposición del artículo 85 del RGPD, tal y como comentaremos en capítulos sucesivos.

Queremos recalcar con énfasis que sería muy pernicioso para cualquier democracia que se precie utilizar el primer caso – el de vulneración de derechos en la difusión de información íntima – para impedir lo segundo – la libertad de información en el interés

[41] En la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, asunto C-101/01 Lindqvist, se sancionó por protección de datos a una catequista que incluyó en una página web que ella misma creó información sobre sus compañeros de parroquia (nombre, descripción de las funciones que desempeñaban e indicó que una de sus compañeras estaba de baja parcial por enfermedad), sin informarles ni solicitar su consentimiento.

[42] https://elpais.com/economia/2020/02/06/mis_derechos/1580977149_547064.html

[43] https://www.aepd.es/canalprioritario/

público para divulgar abusos.

- **Presunción de veracidad**

Finalmente, resulta relevante señalar que en el Estado español existe la presunción de veracidad sobre la información emitida por parte de aquellos funcionarios públicos que son considerados como autoridad (artículo 77.5 de la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas), además de la ley "mordaza" en su artículo 52 (Ley Orgánica de protección de la seguridad ciudadana 4/2015, de 30 de marzo), respecto al valor probatorio de las declaraciones de los agentes de la autoridad.

Xnet no quiere cuestionar aquí la pertinencia de este hecho, pero sí señalar que en contrapartida se hace más necesario, si cabe, permitir las grabaciones por parte de las personas para poder disponer de pruebas ante posibles abusos e irregularidades.

Consideramos importante que para evitar agresiones físicas y verbales de trabajadores de cara al público se permitan las grabaciones del ambiente o sonido y las y los usuarios en estos ámbitos de trabajo. Del mismo modo y por reciprocidad, es necesario que exista la posibilidad de hacer uso de la posibilidad de grabar por parte de la ciudadanía y consumidores que son atendidos para poder denunciar posibles agresiones, abusos, mala praxis e irregularidades cometidos por parte de los trabajadores o instituciones y corporaciones que les prestan servicio. En ambos casos y para preservar la presunción de inocencia, en caso de difusión se deben tomar las medidas necesarias para que no se pueda reconocer la persona grabada ni difundir partes de la grabación que sean inherentes a hechos privados que no tengan utilidad en el esclarecimiento del posible abuso.

RECOMENDACIONES

Fruto del análisis realizado, para garantizar y proteger el derecho de las personas a grabar las actuaciones de personal al servicio de las Administraciones Públicas o de corporaciones sistémicas, en línea con las normas internacionales de derechos humanos, desde XNet recomendamos:

- **Equilibrar la balanza sobre el consentimiento y garantizar la seguridad jurídica de la ciudadanía.**

Promover regulaciones y leyes, como por ejemplo enmendando la recientemente aprobada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, para que no se requiera el consentimiento de los funcionarios en servicio o trabajadores de corporaciones para captar abiertamente su imagen y voz durante el desempeño de sus funciones cuando la finalidad de dichas grabaciones sea la de controlar el buen funcionamiento de las instituciones públicas, denunciar abusos de poder, mala praxis, abusos de la situación de inferioridad de los usuarios o irregularidades cometidas por quienes les prestan servicio. Puede legitimarse este tratamiento de datos personales mediante otras bases jurídicas del tratamiento previstas tanto por la Ley de Protección de Datos (artículo 8) como por el Reglamento Europeo General de Protección de Datos (artículo 6.1, letras c, e y f): cumplimiento de obligaciones legales aplicables a la ciudadanía, el cumplimiento de misiones realizadas en interés público y la satisfacción de intereses legítimos.
Debe complementarse esta medida mediante la enmienda de la misma Ley Orgánica en el sentido que la misma garantice, y no solo anuncie, las libertades de expresión e información para la población en general. En este sentido, dedicaremos un capítulo aparte a la correcta transposición del artículo 85 del RGPD.

Normalizar la posibilidad de grabar de forma recíproca y no unidireccional, (o sea, ahora solo graban las instituciones y corporaciones y no se facilita a la ciudadanía y consumidores esta posibilidad), en los espacios donde se presten servicios abiertos al público y llamadas telefónicas a instituciones y servicios, como medida preventiva de la comisión de agresiones e irregularidades, las grabaciones y su difusión encontrándose solo justificadas en caso de comisión de abusos, irregularidades y malas praxis por parte de los prestadores de servicio o de las y los usuarios.

• Proteger el interés público y las libertades de expresión e información respecto a la difusión de las grabaciones. Armonizarlos con la presunción de inocencia.

Derogar el artículo 36.23 de la Ley 4/2015 de Seguridad Ciudadana.

Promover regulaciones que garanticen la posibilidad de difundir grabaciones de cargos públicos o profesionales de notoriedad o proyección pública, servidores y cargos públicos, así como trabajadores de corporaciones que actúen de cara al público o de usuarios de esos servicios para denunciar situaciones de mala praxis, irregularidades, abusos o agresiones, respetando otros derechos fundamentales. Es decir, preservando los datos personales de la persona grabada y ocultando/camuflando su voz e imagen, u otros datos personales que puedan identificarle en la difusión. En ambos casos y para preservar la presunción de inocencia, en caso de difusión se deben tomar las medidas necesarias para que no se pueda reconocer la persona grabada ni difundir partes de la grabación que sean inherentes a hechos privados que no tengan utilidad en el esclarecimiento del posible abuso, sobre todo cuando el ilícito que se quiere exponer no haya sido demostrado o hecho público por las autoridades y medios competentes.

Actualización a 20/11/2020: el 19/11/2020 el Tribunal Constitucional declara inconstitucional el inciso “no autorizado” del artículo 36.23 de la Ley de Seguridad Ciudadana (Ley Mordaza). Nota de prensa: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2020_108/NOTA%20INFORMATIVA%20N%C2%BA%20108-2020.pdf

- **XNET**

  - **Aprobación de la Proposición de Ley de Protección Integral de los Alertadores de Xnet**, primera transposición europea de la Directiva (UE) 2019/1937, de 23 de octubre de 2019, del Parlamento Europeo y del Consejo sobre la Protección de las Personas que informen sobre infracciones, registrada en el Congreso de los Diputados: https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/

Creemos en el efecto disuasorio y preventivo de estas medidas.

RECOMENDACIONES DE BUENAS PRÁCTICAS PARA LAS INSTITUCIONES Y EMPRESAS SISTÉMICAS

ANTERIORES A LAS MODIFICACIONES DE LA LEY PARA CREAR UN MARCO MÁS FAVORABLE AL RESPETO DE LAS LIBERTADES FUNDAMENTALES

- Establecer criterios interpretativos claros e informar a la ciudadanía sobre los mismos para que pueda conocer los límites existentes entre la libertad de expresión e información y el derecho a la protección de los datos personales y así facilitar el ejercicio de estas libertades en los casos en que sea de interés público protegiendo al mismo tiempo el derecho fundamental a la protección de datos personales y el derecho de defensa en su caso.

- Tanto para su protección como para proteger la presunción de inocencia, informar a la ciudadanía de que en caso de grabar y querer difundir grabaciones en las que aparezca personal al servicio de las Administraciones Públicas o de corporaciones sistémicas o usuarios, cuando no se disponga del consentimiento explícito de los mismos, es necesario difundir sólo las partes que contengan información de relevancia para el interés general; no difundir conversaciones o partes de las mismas que contengan información que pertenece clara y únicamente al ámbito personal de la persona grabada y que no es de relevancia para el hecho/abuso que quiere darse a conocer; editar las imágenes y la voz, así como otros datos personales que incluya, para que la persona grabada no pueda reconocerse (camuflar la voz, pixelar el rostro, etc.) y la difusión no pueda resultar vejatoria. Lo importante son los hechos a denunciar. Muchas veces los abusos no son causados por la persona que es un simple trabajador, sino por la estructura dónde trabaja.

- Concienciar a los cargos públicos, profesionales de notoriedad y al personal al servicio de las Administraciones Públicas o corporaciones sistémicas, que dar a conocer hechos que suceden cuando atienden al público, puede ser muy beneficioso para la salud democrática y la mejora del funcionamiento de las entidades.

- Impulsar un entorno en el que haya consentimiento para la captación de grabaciones del funcionamiento general tanto de los prestadores de servicios como de los usuarios.

- Las autoridades competentes de cada Comunidad Autónoma pueden contribuir a la normalización de estas buenas prácticas mediante la emisión de informes, órdenes y actos vinculantes favorables a las mismas, dentro de sus competencias.

ENMIENDAS A LA LEY

Derogación del artículo 36.23 de la Ley 4/2015 de Seguridad Ciudadana.

Artículo 36. Se considera infracción grave:

(...) 23. El uso no autorizado de imágenes o datos personales o profesionales de autoridades o miembros de las Fuerzas y Cuerpos de Seguridad que pueda poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, con respeto al derecho fundamental a la información.

Actualización a 20/11/2020: el 19/11/2020 el Tribunal Constitucional declara inconstitucional el inciso "no autorizado" del artículo 36.23 de la Ley de Seguridad Ciudadana (Ley Mordaza). Nota de prensa:

https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2020_108/NOTA%20INFORMATIVA%20N%C2%BA%20108-2020.pdf

Modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Para alcanzar el fin propuesto debemos solicitar la enmienda de un único artículo de la Ley, con la introducción de un nuevo punto en el *Artículo 8 "Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos"* de la misma, que pasaría a denominarse *"Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos, interés legítimo"*.

3. La captación de la voz y la imagen, conforme los términos del artículo 8.2.a) de la Ley Orgánica 1/1982, de cargos públicos o profesionales de notoriedad o proyección pública, del personal al servicio de las Administraciones Públicas o trabajadores de corporaciones, durante el ejercicio de sus funciones o usuarios, podrá realizarse para la denuncia o información sobre conductas irregulares, abusivas, de mala praxis o agresiones, que afecten:

a) a la prestación de servicios;

b) al ciudadano o consumidor concreto que realiza la grabación;

c) y/o al interés público.

No obstante, dichos datos de carácter personal no podrán ser difundidos públicamente salvo que, en las imágenes, grabaciones o cualquier otro tipo de soporte o medio utilizado para la difusión, se incluyan modificaciones, tanto de la imagen, de la voz, como de los datos personales que incluya, que impidan reconocer la identidad del afectado, cuando el ilícito que se quiere exponer no haya sido demostrado o hecho público por las autoridades y medios competentes.

No deberá informarse sobre la grabación y captación de imágenes, así como de su posible difusión a los afectados y ambos tratamientos de datos personales se presumirán fundados:

a) en el interés legítimo del ciudadano que realiza la grabación, en los términos previstos en el artículo 6.1.f) del Reglamento (UE) 2016/679;

b) en el cumplimiento de una misión realizada en interés público, en los términos previstos en el artículo 6.1.e) del Reglamento (UE) 2016/679;

En todo caso podrán utilizarse las imágenes y grabaciones captadas, sin modificación alguna, como pruebas en procedimientos disciplinarios, administrativos y judiciales.

Además de la introducción de un nuevo artículo (tal y como indicaremos más adelante en relación con la transposición del art. 85 del GDPR) que establezca lo siguiente:

1. Todo ciudadano puede poner a disposición del público información de interés general en ejercicio de las libertades de expresión e información, independientemente del origen de la misma.

Para respetar el derecho a la protección de datos personales de las personas cuyos datos puedan ser revelados del hecho de esta información, el ciudadano o consumidor, deberá tomar en consideración los siguientes aspectos:

a) Aplicar las modificaciones previstas en el artículo 8.3 cuando la información que se quiere divulgar consista en grabaciones.

b) Si la persona está actuando en un contexto público o hizo pública la información, se trata de una figura o personaje público o bien si se trata de personas individuales, debiendo respetar en todo caso el ámbito íntimo y personal de la persona afectada, teniendo en cuenta las consecuencias previsibles de la difusión. Sólo podrá ser objeto de divulgación la información relevante para el interés general.

2. Se entiende por tratamiento de datos personales:

a) con fines periodísticos el realizado durante el ejercicio de la profesión periodística para la preparación de una publicación, incluyendo, entre otros, la recogida, redacción, producción, difusión o archivo de información para informar al público, por cualquier medio, en ejercicio de las libertades de información y de expresión entendidas en sentido amplio para permitir el ejercicio de la profesión. Deberán respetarse en todo caso las normas deontológicas del periodismo aplicable.

Siguiendo una interpretación amplia de las actividades incluidas dentro del ámbito de las libertades de información y de expresión, podrá considerarse como tratamiento de datos personales con fines periodísticos también aquél realizado por parte de la ciudadanía y alertadores para poner información de interés general a disposición del público por cualquier medio.

(…)

3. No serán aplicables a los tratamientos del apartado 2 las disposiciones del Reglamento (UE) 2016/679 previstas a continuación y sus concordantes previstas en la presente Ley Orgánica:

a) Del capítulo II: El artículo 5.1 a y e y artículos 6 a 11 del Reglamento (UE) 2016/679.

b) Del capítulo III: Los artículos 12 a 14, 15 y 18 a 23 del Reglamento (UE) 2016/679.

c) Del capítulo IV: Los artículos 30, 31 y 35 a 39 del Reglamento (UE) 2016/679.

d) Del capítulo VI: El apartado 1 del artículo 58 del Reglamento (UE) 2016/679. En concreto, la Autoridad de Control no podrá solicitar en ningún caso el acceso a las fuentes de la información.

El resto de disposiciones previstas por el artículo 85 del Reglamento (UE) 2016/679 y sus concordantes previstas en la presente Ley Orgánica, deberán respetarse, salvo cuando su aplicación pudiese comprometer la publicación proyectada o pudiese constituir una medida de control o censura previa a la publicación que limite y sea incompatible con las libertades de expresión e información.

- **XNET**

En anexo:

- ANÁLISIS DEL DESARROLLO LEGISLATIVO
- ANÁLISIS DE LA JURISPRUDENCIA Y RESOLUCIONES RELEVANTES
- LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

3 - LA MANCADA TRANSPOSICIÓN DEL ARTÍCULO 85 EN ESPAÑA – LA DESPROTECCIÓN DE LA LIBERTAD DE INFORMACIÓN EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

ÍNDICE

LA MANCADA TRANSPOSICIÓN DEL ARTÍCULO 85 EN ESPAÑA – LA DESPROTECCIÓN DE LA LIBERTAD DE INFORMACIÓN EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

El Reglamento Europeo de Protección de Datos obliga a los Estados a conciliar el derecho a la protección de datos con otros derechos fundamentales, tales como las libertades de expresión e información.

Xnet durante la elaboración de la Ley Orgánica de Protección de Datos y garantía de los derechos digitales, aprobada en diciembre de 2018, hizo propuestas en varias reuniones con el legislador, para conciliar los límites entre estos derechos. Ninguna de las propuestas fue aceptada con una motivación que no podemos compartir: "esto lo resuelven los tribunales". Nosotros consideramos que esta aproximación es peligrosa ya que implica que la defensa de la libertad de expresión e información es garantizada solo para quién pueda permitirse pleitear. Preferimos que **se establezca un marco donde sea posible ejercer estos derechos con mayor seguridad jurídica.**

En España todavía no se ha producido un caso que evidencie masivamente esta asimetría y negativo impacto sobre los derechos fundamentales, pero sí aportamos algunos ejemplos sintomáticos.

Primer ejemplo: Xnet, en sus actividades entorno a la lucha contra la corrupción, tiene constancia de la frecuencia con la que, en los casos de corrupción, los corruptos alegan el derecho a la protección de sus datos para invalidar pruebas[44,45,46]. Conocido por todos es el caso del Partido Popular que justificó la destrucción de los discos duros posiblemente relacionados con el caso Bárcenas alegando protección de datos[47]. En este sentido véase también el capítulo sobre "Derecho a grabar abusos" de este informe.

Otro ejemplo. Las consecuencias de esta omisión ya se han hecho visibles en el ámbito académico cuando la Universidad de Alicante decidió eliminar de los resultados de búsqueda de buscadores como Google, tras una petición vía la Ley de Protección de Datos, el nombre de Antonio Luis Baena Tocón, alférez del Ejército franquista que ejerció de secretario judicial en uno de los consejos militares que condenaron a muerte al poeta Miguel Hernández, de varios textos firmados por el catedrático Juan Antonio Ríos Carratalá. Finalmente, la Universidad rectificó y decidió no eliminar los resultados de búsqueda al considerar que el nombre y actuación del alférez era información de interés público, hecha con fines de investigación histórica[48].

Pero el ejemplo claro de las consecuencias de no plasmar el espíritu del artículo 85 del Reglamento General de Protección de Datos Europeo han podido observarse en **Rumania**, donde **la Autoridad de Protección de Datos Rumana investigó los periodistas de RISE Project** por un reportaje sobre un escándalo de corrupción. Se les acusó de haber violado la protección de datos de las personas (políticos, etc.) que mencionaban en su investigación al haberla publicado. Se les pidió, entre otras cosas, las fuentes de la información que habían publicado. En un primer momento se les amenazó con una multa de 600€ por cada día de retraso en proporcionar la información, además de una sanción de 20 millones de euros[49].

"Tanto el Tribunal de Justicia de la Unión Europea como el Tribunal Europeo de Derechos Humanos han señalado en numerosas sentencias la importancia de proteger el debate sobre asuntos de interés público y que la protección de las fuentes periodísticas es uno de los pilares de la libertad de información de la prensa. El Relator Especial de la ONU sobre la protección del derecho a la

[44] https://blogs.publico.es/otrasmiradas/15834/proteccion-datos-obstaculo-lucha-corrupcion/
[45] https://twitter.com/adsuara/status/1108116611314143233
[46] https://civio.es/novedades/2019/12/17/el-supremo-da-la-razon-a-civio-y-obliga-al-tribunal-de-cuentas-a-darnos-los-nombres-de-todos-sus-eventuales/
[47] https://www.elespanol.com/espana/tribunales/20190620/pp-destruyo-ordenadores-barcenas-ley-proteccion-datos/407709807_0.html
[48] https://web.ua.es/es/actualidad-universitaria/2019/julio19/29-31/la-universidad-de-alicante-mantendra-el-nombre-de-baena-tocon-en-su-repositorio.html
[49] Traducción al inglés de la carta de la Autoridad de Protección de Datos de Rumanía enviada a RISE Project: https://www.occrp.org/en/16-other/other-articles/8876-english-translation-of-the-letter-from-the-romanian-data-protection-authority-to-rise-project

libertad de opinión y de expresión también ha subrayado la necesidad de proteger las fuentes periodísticas[50].”[51]

Con la regulación europea e internacional en mente, la Association for Technology and Internet (ApTI) con la colaboración de Privacy International y Xnet entre otras organizaciones europeas de defensa de derechos digitales[52] presentó una queja ante la Comisión Europea[53] considerando que el Reglamento europeo no podía servir de herramienta para limitar las libertades de expresión e información y que en el caso de Rumanía las tres excepciones previstas por la Ley eran demasiado limitadas, las actividades periodísticas yendo más allá de lo previsto. Además, también cuestionó los poderes de investigación de la Autoridad de Protección de Datos cuando la libertad de información está en juego.

El portavoz de la Comisión Europea, Margaitis Schinas, hizo las siguientes declaraciones al respecto:

https://audiovisual.ec.europa.eu/en/video/I-163519

“El derecho a la protección de datos personales no es un derecho absoluto. El artículo 85 del Reglamento General de Protección de Datos indica claramente que el derecho a la protección de datos debe equilibrarse con las libertades de expresión e información. Utilizar el Reglamento General de Protección de Datos contra estos dos otros derechos fundamentales sería un abuso claro de la regulación. Por lo tanto, es sumamente importante que las autoridades de Rumanía implementen esta obligación en el derecho nacional para proveer excepciones y derogaciones para proteger las fuentes periodísticas en particular de los poderes de la Autoridad de protección de datos cuando sea necesario para respetar la libertad de información y expresión de los medios. (…) La protección de datos no puede utilizarse como una puerta trasera para forzar a los periodistas a decir o hacer cosas que tienen derecho a no decir o no hacer bajo la libertad de expresión e información y protección de las fuentes”.

Lamentamos que tras las declaraciones no se emprendiera ningún tipo de acción por parte de los organismos europeos.

Tras el caso de Rumanía, el **Presidente de Bulgaria ejerció su derecho de veto sobre la Ley búlgara de protección de datos** porque consideró que las previsiones de la ley relativas a las condiciones para que la misma no se aplicase cuando la protección de datos colisionase con las libertades de expresión e información conllevarían el control del trabajo de los periodistas, académicos y artistas, perjudicando sus libertades de expresión e información además de su independencia[54]. Aun así, la Ley se aprobó sin modificación alguna sobre este punto con el voto a favor de más de la mitad de todos los miembros del Parlamento y entró en vigor el pasado marzo de 2019.

Por todo ello es necesario remediar estas lagunas también en el ordenamiento jurídico español.

[50] Informe del Relator Especial de la ONU sobre la protección del derecho a la libertad de opinión y de expresión. https://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361

[51] https://www.apti.ro/sites/default/files/ApTI%20and%20PI%20letter%20to%20EDPB%20-%20RISE%20Project.pdf

[52] https://www.apti.ro/sites/default/files/ApTI%20and%20PI%20letter%20to%20EDPB%20-%20RISE%20Project.pdf

[53] https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf

[54] http://www.mondaq.com/x/781214/Data+Protection+Privacy/The+President+Vetoes+Local+Law+Implementing+The+GDPR

RECOMENDACIONES

Fruto del análisis realizado, para garantizar y proteger el derecho de las personas a informar y recibir información de interés general, según los estándares internacionales de derechos humanos, desde XNet recomendamos:

- **Proteger el interés público y las libertades de expresión e información**

  Enmendar la recientemente aprobada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, para que garantice, y no solo anuncie, las libertades de expresión e información para la población en general.

  Para al mismo tiempo proteger la presunción de inocencia, nos remitimos a nuestras recomendaciones para el derecho a grabar[55] y aplicamos los mismos parámetros: los datos personales de las personas que aparezcan en información que se hace pública para el interés general deben ser ocultados a menos que sean hechos públicos y notorios o hayan sido revelados ya por parte de la justicia o medios de comunicación. Así mismo, se deben tomar las necesarias medidas para no difundir partes de la información que sean inherentes a hechos privados y que no tengan utilidad pública. Por otra parte, se debe respetar la función social de ciertos profesionales en un sistema democrático y establecer criterios específicos para ellos (periodistas, académicos, investigadores, artistas...) preservando sus prerrogativas y función para el interés general y protegiendo sus fuentes como prioridad.

- **Aprobar la Ley de Protección Integral de Alertadores de Xnet (primera transposición de la Directiva Europea).**

  Con la tramitación de la Ley de Secretos Comerciales se consiguió un avance en este sentido incluyendo una excepción a la aplicación de la misma para garantizar que no sea delito revelar un secreto comercial para proteger interés público, garantizando así la libertad de expresión e información[56].

  Siguiendo este camino, Xnet creó la Ley de Protección Integral de Alertadores[57] e integró la primera transposición de la

---

[55] Recomendaciones del informe sobre el Derecho a Grabar:

- **Equilibrar la balanza sobre el consentimiento y garantizar la seguridad jurídica de la ciudadanía.**
  Promover regulaciones y leyes, como por ejemplo enmendando la recientemente aprobada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, para que no se requiera el consentimiento de los funcionarios en servicio o trabajadores de corporaciones para captar su imagen y voz cuando la finalidad de dichas grabaciones sea la de controlar el buen funcionamiento de las instituciones públicas, denunciar abusos de poder, mala praxis, abusos de la situación de inferioridad de los usuarios o irregularidades cometidas por quienes les prestan servicio. Puede legitimarse este tratamiento de datos personales mediante otras bases jurídicas del tratamiento previstas tanto por la Ley de Protección de Datos (artículo 8) como por el Reglamento Europeo General de Protección de Datos (artículo 6.1, letras c, e y f): cumplimiento de obligaciones legales aplicables a la ciudadanía, el cumplimiento de misiones realizadas en interés público y la satisfacción de intereses legítimos.
  Normalizar el uso de cámaras y sistemas de grabación en los espacios donde se presten servicios abiertos al público, tanto por parte de las instituciones y corporaciones como de la ciudadanía y consumidores, como medida preventiva de la comisión de agresiones e irregularidades.
- **Proteger el interés público y las libertades de expresión e información respecto a la difusión de las grabaciones. Armonizarlos con la presunción de inocencia.**
  Derogar el artículo 36.23 de la Ley 4/2015 de Seguridad Ciudadana.
  Promover regulaciones que garanticen la posibilidad de difundir grabaciones de servidores y cargos públicos, así como trabajadores de corporaciones que actúen de cara al público o de usuarios de esos servicios para denunciar situaciones de mala praxis, irregularidades, abusos o agresiones, respetando otros derechos fundamentales. Es decir, preservando los datos personales de la persona grabada y ocultando/camuflando su voz e imagen en la difusión. En ambos casos y para preservar la presunción de inocencia, en caso de difusión se deben tomar las necesarias medidas para que no se pueda reconocer la persona grabada ni difundir partes de la grabación que sean inherentes a hechos privados que no tengan utilidad en el esclarecimiento del posible abuso.

[56] https://xnet-x.net/victoria-acceso-informacion-abusos-whistleblowers-transposicion-directiva-secretos-comerciales/

[57] https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/

Directiva europea en la que también participó. Esta ley ya tiene tres tramitaciones, a nivel estatal[58], catalán[59] y vasco[60], aunque ninguna todavía ha culminado en una aprobación. Esta ley garantiza la protección contra cualquier tipo de represalia de quienes saquen a la luz abusos sistémicos que afectan el interés general.

[58] https://xnet-x.net/xnet-registra-primera-ley-alertadores-ue/
[59] https://xnet-x.net/xnet-parlament-catalunya-proposicion-ley-proteccion-alertadores/
[60] https://xnet-x.net/ley-proteccion-alertadores-plantilla-xnet-alertas-ciudadanas-elkarrekin-parlamento-vasco/

- **XNET**

RECOMENDACIONES DE BUENAS PRÁCTICAS PARA LAS INSTITUCIONES Y EMPRESAS SISTÉMICAS

ANTERIORES A MODIFICACIONES DE LA LEY PARA CREAR UN MARCO MÁS FAVORABLE AL RESPETO DE LAS LIBERTADES FUNDAMENTALES

- Establecer criterios interpretativos claros e informar a la ciudadanía sobre los mismos para que pueda conocer los límites existentes entre la libertad de expresión e información y el derecho a la protección de los datos personales y así facilitar el ejercicio de estas libertades en los casos en que sea de interés público protegiendo al mismo tiempo el derecho fundamental a la protección de datos personales y el derecho de defensa en su caso.
- Implementar canales de alerta anónimos y seguros, internos y/o externos como los de Globaleaks que Xnet ha adaptado a la legislación española e implementado en instituciones por primera vez en España[61], que permitan la revelación de información de interés público sobre irregularidades cometidas tanto en el ámbito público como empresarial. Normalizar el uso de dichos canales sin criminalizar su utilización[62].

[61] https://xnet-x.net/buzon-denuncias-anonimas-ciudad-barcelona-bustia-etica/
[62] https://xnet-x.net/proliferacion-buzones-anonimos-no-lo-son/

ENMIENDAS A LA LEY

Modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Para alcanzar el fin propuesto, debemos solicitar la introducción de un nuevo artículo en la Ley que establezca lo siguiente:

1. Todo ciudadano puede poner a disposición del público información de interés general en ejercicio de las libertades de expresión e información, independientemente del origen de la misma.

Para respetar el derecho a la protección de datos personales de las personas cuyos datos puedan ser revelados del hecho de esta información, el ciudadano o consumidor, deberá tomar en consideración los siguientes aspectos:

a) Aplicar las modificaciones previstas en el artículo 8.3 cuando la información que se quiere divulgar consista en grabaciones.

b) Si la persona está actuando en un contexto público o hizo pública la información, se trata de una figura o personaje público o bien si se trata de personas individuales, debiendo respetar en todo caso el ámbito íntimo y personal de la persona afectada, teniendo en cuenta las consecuencias previsibles de la difusión. Sólo podrá ser objeto de divulgación la información relevante para el interés general.

2. Se entiende por tratamiento de datos personales:

a) con fines periodísticos el realizado durante el ejercicio de la profesión periodística para la preparación de una publicación, incluyendo, entre otros, la recogida, redacción, producción, difusión o archivo de información para informar al público, por cualquier medio, en ejercicio de las libertades de información y de expresión entendidas en sentido amplio para permitir el ejercicio de la profesión. Deberán respetarse en todo caso las normas deontológicas del periodismo aplicable.

Siguiendo una interpretación amplia de las actividades incluidas dentro del ámbito de las libertades de información y de expresión, podrá considerarse como tratamiento de datos personales con fines periodísticos también aquél realizado por parte de la ciudadanía y alertadores para poner información de interés general a disposición del público por cualquier medio.

b) con fines de expresión académica el realizado en todos los niveles educativos, públicos o privados, por parte de profesores, investigadores y alumnos en sentido amplio, para llevar a cabo actividades de docencia, investigación, publicación y difusión.

c) con fines de expresión artística o literaria el realizado para crear, distribuir y participar en expresiones culturales diversas.

3. No serán aplicables a los tratamientos del apartado 2 las disposiciones del Reglamento (UE) 2016/679 previstas a continuación y sus concordantes previstas en la presente Ley Orgánica:

a) Del capítulo II: El artículo 5.1 a y e y artículos 6 a 11 del Reglamento (UE) 2016/679.

b) Del capítulo III: Los artículos 12 a 14, 15 y 18 a 23 del Reglamento (UE) 2016/679.

c) Del capítulo IV: Los artículos 30, 31 y 35 a 39 del Reglamento (UE) 2016/679.

d) Del capítulo VI: El apartado 1 del artículo 58 del Reglamento (UE) 2016/679. En concreto, la Autoridad de Control no podrá solicitar en ningún caso el acceso a las fuentes de la información.

El resto de disposiciones previstas por el artículo 85 del Reglamento (UE) 2016/679 y sus concordantes previstas en la presente Ley Orgánica, deberán respetarse, salvo cuando su aplicación pudiese comprometer la publicación proyectada o pudiese constituir una medida de control o censura previa a la publicación que limite y sea incompatible con las libertades de expresión e información.

- **XNET**

Aprobación de la Ley de Protección Integral de Alertadores de Xnet[63] para transponer la Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas que informen sobre infracciones del derecho de la Unión.

[63] **h**ttps://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/

- **XNET**

En anexo:

- ANÁLISIS DEL DESARROLLO LEGISLATIVO
- ANÁLISIS DE LA JURISPRUDENCIA Y RESOLUCIONES RELEVANTES
- LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

4 – ABUSOS EN EL ÁMBITO ELECTORAL: CÓMO HEMOS LLEGADO A QUE NOS PAREZCA NORMAL QUE LOS DATOS DEL PADRÓN MUNICIPAL ACABEN EN MANOS DE LOS PARTIDOS POLÍTICOS

ÍNDICE

ANÁLISIS DE LA JURISPRUDENCIA RELEVANTE

LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

[Para que cesen los abusos que aquí exponemos, hemos enviado sendas peticiones al Chair of the Petitions Committee European Parliament; European Commission Commissioner Mr. Didier Reynders; Directorate General of Democracy of the Council of Europe (DGII); OSCE Office for Democratic Institutions and Human Rights (ODIHR).

https://xnet-x.net/fin-abuso-datos-privacidad-ciudadania-ue-elecciones *]*

CÓMO HEMOS LLEGADO A QUE NOS PAREZCA NORMAL QUE LOS DATOS DEL PADRÓN MUNICIPAL ACABEN EN MANOS DE LOS PARTIDOS POLÍTICOS

El derecho a la protección de datos es un derecho fundamental que garantiza a las personas el control sobre sus datos, sobre su uso y su destino. Debe ser respetado tanto por parte de entidades públicas como privadas. Aún así, hay excepciones previstas por la normativa a la aplicación de determinadas obligaciones que deberían cumplir, cuya consecuencia principal es que las personas pierdan el control efectivo sobre sus datos. Para que esto sea admisible desde el punto de vista de las libertades fundamentales, debe de haber muy buenos motivos para dichas excepciones.

En la normativa, existen excepciones en el caso de los datos que las personas inscriben en el Padrón de su Ayuntamiento, es decir, toda la población empadronada. Estos datos pasan a constituir el censo electoral. Existe una tradición decimonónica consentida por la ley que consiste en ceder esta base de datos exhaustiva de la población (incluyendo las direcciones privadas de víctimas, activistas, periodistas, abogados, etc.) a los partidos políticos, de toda índole política, incluso los más extremistas. Esta tradición que quizás pudo tener sentido cuando no existía otro modo de que las personas conocieran los programas electorales, ha perdurado con la televisión y ahora perdura con internet.

Tras examinar las Leyes que regulan tanto el padrón municipal de habitantes como el censo electoral, se puede deducir **el flujo de los datos, desde que la persona se inscribe en el padrón de habitantes hasta la comunicación de estos datos a los partidos políticos. Es el siguiente**:

CIUDADANO → AYUNTAMIENTO (Padrón) → INSTITUTO NACIONAL DE ESTADÍSTICA → AYUNTAMIENTO + REGISTRO CIVIL (para la actualización de los datos del Padrón) → OFICINA DEL CENSO ELECTORAL (Censo) → PARTIDOS POLÍTICOS.

Los datos que se proporcionan a los partidos políticos de cada elector son los siguientes: Nombre y apellidos, provincia y municipio de residencia, distrito, sección y mesa electoral, domicilio, fecha de nacimiento y nacionalidad para los electores extranjeros. Y en caso de los electores que viven en el extranjero, se incluye si se ha solicitado el voto, dónde se está inscrito a efectos electorales, domicilio, país de residencia y fecha de nacimiento.

Claro está que **sería conveniente modificar la Ley del Régimen Electoral General para derogar esta comunicación y no permitir más la cesión masiva de datos que viene produciéndose desde 1985**.
Así debería ser si **queremos una democracia en la que sea la ciudadanía la que tenga el control sobre sus instituciones y no al revés**.

La ley que rige los tratamientos de datos personales en período electoral es la Ley Orgánica del Régimen Electoral General, aplicándose la Ley Orgánica de Protección de Datos y garantía de los derechos digitales y el Reglamento Europeo de Protección de Datos de forma subsidiaria, es decir, sólo en lo que la primera no ha previsto[64], pero incluso aquí el Tribunal Constitucional dictaminó que lo previsto en la LOREG no era suficiente para proteger debidamente los datos de la ciudadanía en la Sentencia 76/2019, de 22 de mayo, que declaró inconstitucional la recogida de datos ideológicos por los partidos y agrupaciones políticas. Pero el constitucional no entró a valorar la comunicación de datos del censo a los partidos, al no ser considerados "datos de categorías especiales", es decir, datos sensibles.

Así, se perpetúa la comunicación a los partidos políticos por la LOREG, sin que la influencia del nuevo Reglamento europeo General de Protección de Datos haya servido para reflexionar sobre prácticas abusivas de los poderes públicos que se perpetúan en el tiempo. Al aprobar la nueva Ley Orgánica de Protección de Datos sólo se ha previsto la posibilidad de oponerse a que los datos sean enviados a los partidos, cuando creemos que debería ser al revés si queremos ser fieles al principio de privacidad desde el diseño y por defecto: se debería poder pedir ceder estos datos a los partidos para recibir la publicidad electoral y no haber de oponerse para no recibirla. Además el modo de ejercer este derecho de oposición (mediante certificado electrónico) puede dificultar que gran parte de la ciudadanía lo ejerza efectivamente.

El RGPD tampoco no protege en este caso, dejando esta circunstancia en mano de los Estados y debilitando el principio de la privacidad desde el diseño y por defecto que es uno de sus principios básicos.

Además de producirse dicha comunicación, en la mayoría de los casos **las personas no son informadas** cuando se inscriben al Padrón Municipal de habitantes de las futuras comunicaciones de sus datos personales a otras administraciones ni a los partidos políticos ni tampoco para qué van a utilizar sus datos estas entidades. Esto vulnera uno de los principios esenciales del Reglamento Europeo de Protección de Datos, el principio de transparencia, que implica el conocimiento por parte de las personas, cuando proporcionan sus datos, de los usos a los que estos estarán destinados y a quienes serán comunicados en su caso, además de la obligación de **ofrecer la posibilidad de oponerse a ello.**

En base a todas estas consideraciones, pedimos un cambio en la ley para una democracia actualizada y mejor.

[64] *Artículo 2.3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

RECOMENDACIONES

Fruto del análisis realizado, para garantizar y proteger el derecho de las personas a conocer y controlar el destino y uso de sus datos, en línea con la legislación europea sobre la protección de datos personales, desde XNet recomendamos:

• **Derogar la comunicación a los partidos políticos de los datos recogidos en el Censo electoral**

Los datos personales no deberían ser objeto de cesión masiva a los partidos políticos por parte de las autoridades públicas. Debe eliminarse dicha comunicación que se lleva a cabo por defecto y a la que actualmente uno debe oponerse de forma expresa.

Podría preverse la fórmula contraria a la existente actualmente: quien quiera recibir propaganda electoral que así lo indique, sin que los datos del resto de la ciudadanía pasen a manos de los partidos políticos.

RECOMENDACIONES DE BUENAS PRÁCTICAS PARA LAS ADMINISTRACIONES PÚBLICAS

ANTERIORES A LA MODIFICACIÓN DE LA LEY PARA IMPULSAR SU APLICACIÓN

• En el momento de la recogida de datos de empadronamiento, informar correctamente a la ciudadanía sobre las distintas finalidades para las que se van a utilizar sus datos ulteriormente así como las comunicaciones de datos que se llevaran a cabo de forma previsible y las finalidades de las mismas, indicando, si es necesario la Ley en que están previstas. **Estudiar fórmulas que permitan la opción de oposición en el acto**.

ENMIENDAS A LA LEY

Derogación de los apartados 5 y 6 del artículo 41 de la Ley Orgánica del Régimen Electoral General.

> *"(…) 5. Los representantes de cada candidatura podrán obtener dentro de los dos días siguientes a la proclamación de su candidatura una copia del censo del distrito correspondiente, ordenado por mesas, en soporte apto para su tratamiento informático, que podrá ser utilizado exclusivamente para los fines previstos en la presente Ley. Alternativamente los representantes generales podrán obtener en las mismas condiciones una copia del censo vigente de los distritos donde su partido, federación o coalición presente candidaturas. Asimismo, las Juntas Electorales de Zona dispondrán de una copia del censo electoral utilizable, correspondiente a su ámbito.*
> *Las Juntas Electorales, mediante resolución motivada, podrán suspender cautelarmente la entrega de las copias del censo a los representantes antes citados cuando la proclamación de sus candidaturas haya sido objeto de recurso o cuando se considere que podrían estar incursas en alguna de las circunstancias previstas en el artículo 44.4 de esta Ley.*
> *6. Excepcionalmente y por razones debidamente justificadas, podrá excluirse a las personas que pudieran ser objeto de amenazas o coacciones que pongan en peligro su vida, su integridad física o su libertad, de las copias del censo electoral a que se refiere el apartado 5 del presente artículo."*

Para alcanzar el fin propuesto debemos solicitar, además, la enmienda o derogación, según los casos, de las disposiciones reglamentarias que desarrollan el artículo 41.5 de la LOREG.

Derogación de los puntos primero a sexto relativos a la solicitud de copias del Censo Electoral de la Orden de 3 de febrero de 1987 por la que se regula la distribución de copias del Censo Electoral en soporte magnético y la expedición de certificados de inscripción en el Censo Electoral

> *"Primero.*
> *Una vez terminada la revisión anual del Censo Electoral, cada Comunidad Autónoma podrá obtener, en cinta magnética, una sola copia del referido censo, a petición del Órgano competente de la Comunidad Autónoma. La petición habrá de ser dirigida al Director de la Oficina del Censo Electoral.*

> *Segundo.*
> *1. En la convocatoria de elecciones, los representantes generales de cada partido, federación o coalición podrán obtener, a partir del día de la proclamación de candidatos, una copia en cinta magnética del Censo Electoral de los distritos donde la respectiva entidad política haya presentado candidatos.*
> *2. En el caso de que, dentro del período anual de revisión del Censo Electoral, se convoquen varios procesos electorales aquellos partidos, federaciones o coaliciones que hayan obtenido ya copia del Censo Electoral en soporte magnético, no podrán volver a solicitar nueva copia, salvo que se justifique el deterioro de la copia anterior.*

> *Tercero.*
> *Si un partido o coalición no hubiera solicitado a través de su representante general el Censo Electoral de la totalidad de los distritos en que se presenta, el representante de la candidatura de cada distrito podrá obtener una copia en cinta magnética del censo de su correspondiente distrito, en las condiciones indicadas en el punto precedente.*

Cuarto.
1. El plazo para solicitar las copias del Censo Electoral en soporte magnético por los partidos políticos, federaciones, coaliciones o agrupaciones de electores, será el que medie entre el día de la designación de representante y el de la proclamación de candidatos, quedando condicionada la solicitud a la confirmación de la referida proclamación.
2. La entrega de la copia solicitada se efectuará en la Sede Central de la Oficina del Censo Electoral si se trata de una petición que abarque más de una distrito electoral o en la correspondiente Delegación Provincial de la misma, cuando la petición sea uniprovincial y será realizada al representante de la entidad política solicitante, o a persona suficientemente autorizada por éste.

Quinto.
Los derechos reconocidos en los dos puntos anteriores corresponden, en materia de referéndum, a los grupos políticos comprendidos en el artículo 11. 2 de la Ley Orgánica de las distintas modalidades de referéndum.

Sexto.
Quienes hayan obtenido copias del Censo Electoral en soporte magnético, quedan sometidos a la prohibición de facilitar cualquier tipo de información particularizada sobre datos personales incluidos en el censo, conforme a lo dispuesto en el artículo 41. 2 de la Ley 5/1985."

Enmienda del artículo 5 del Real Decreto 1799/2003, de 26 de diciembre, por el que se regula el contenido de las listas electorales y de las copias del censo electoral, que quedaría redactado como sigue:

"Artículo 5. Copias del censo electoral.
*1. Las copias del censo electoral que se faciliten en virtud de lo dispuesto en el artículo 41, **apartado 4**, de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, contendrán a los electores ordenados de igual forma que en las listas de votación, con las exclusiones que correspondan por la aplicación del artículo 6 de este real decreto.*
***2**. Los datos de cada elector serán los siguientes:*
***2**.1 Electores residentes en España (españoles y nacionales de otros Estados con derecho de voto en España).*
a) Número de orden.
b) Apellidos y nombre.
c) Provincia y municipio de residencia.
d) Distrito, sección y mesa electoral.
e) Domicilio.
f) Fecha de nacimiento: día, mes y año.
g) País de nacionalidad, para los electores nacionales de otros Estados.
***2**.2 Electores residentes-ausentes que viven en el extranjero:*
a) Número de orden.
b) Indicador de haber solicitado el voto.
c) Apellidos y nombre.
d) Provincia y municipio de inscripción a efectos electorales.
e) Domicilio.
f) País de residencia.
g) Fecha de nacimiento: día, mes y año.
***3**. En las copias para las Juntas Electorales de Zona se incluirá el número del identificador personal: Documento Nacional de Identidad, pasaporte o inscripción en el Registro Central de Extranjeros."*

En anexo:

- ANÁLISIS DEL DESARROLLO LEGISLATIVO

Apuntes sobre los tratamientos llevados a cabo por parte de los Ayuntamientos

a. Recogida de los datos: Inscripción al Padrón Municipal de habitantes
b. Comunicación de los datos: al Instituto Nacional de Estadística. Actualización de los datos del Padrón Municipal de Habitantes

Apuntes sobre los tratamientos llevados a cabo por parte de la Oficina del Censo Electoral

a. Comunicación de los datos: Inscripción al Censo Electoral y comunicación recibida de Ayuntamientos y Registros Civiles
b. Comunicación de los datos: Distribución de Copias del Censo a los partidos políticos y tratamiento por parte de los partidos

Apuntes sobre el ejercicio de derechos por parte de la ciudadanía

a. Derechos que pueden ejercerse en cualquier momento
b. Derechos cuyo ejercicio se limita al período electoral

- ANÁLISIS DE LA JURISPRUDENCIA RELEVANTE

- LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

5 – ABUSOS EN EL ÁMBITO LABORAL:

LA VENTA DE LOS DATOS DE LAS PERSONAS EN RÉGIMEN DE AUTÓNOMOS

ÍNDICE

2. LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

LA VENTA DE LOS DATOS DE LAS PERSONAS EN RÉGIMEN DE AUTÓNOMOS

En nuestra vida cotidiana, tanto en el mundo físico como en el digital, utilizamos y permitimos que otros utilicen nuestros datos personales. Hay veces que podemos escoger si queremos proporcionar nuestros datos y hay muchas veces que no. Estos casos deben ser motivados en aras del bien común, de lo contrario socavarían el derecho fundamental a nuestra privacidad.

Este informe se publica en un momento muy crítico para la interpretación de qué es este bien común.

En el activismo pro-transparencia y anticorrupción estamos todavía en shock por la sentencia del TJUE que impide el acceso público a los registros de titularidad de las empresas considerándolo una injerencia en la vida privada.

El procedimiento judicial ante el TJUE lo activaron dos demandas presentadas por la compañía Sovim SA y su dueño real, propietario de una sociedad de cartera en las Islas Vírgenes Británicas con con actividades en Luxemburgo, Chipre y Rusia y activos valorados en más de tres millones de dólares y copropietario de una empresa registrada en el paraíso fiscal centroamericano de Belice, tal y como revela una investigación periodística del ICIJ posterior a la resolución judicial.

Una vez más, leyes surgidas de la sociedad civil para proteger sus derechos frente a abusos de los más poderosos, como son las leyes de protección de datos, ven tergiversada su razón de ser para ser utilizadas en favor de estos últimos y perpetrar la asimetría de poder que se quería corregir.

Y no solo. Hay un doble rasero que hace que mientras se cuida que los poderosos no sufran grandes cambios por la afirmación de derechos colectivos, la gran mayoría de la población sufre años y años de déficit en la implementación que afectan a la salvaguarda de sus intereses.

Las y los autónomos, incluso antes de iniciar su actividad, se ven obligados a realizar declaraciones, inscripciones y registros ante distintas organizaciones para poder trabajar. La principal y coincidente en todo caso es la Agencia Tributaria; con las nuevas obligaciones de prevención de blanqueo de capitales, para quienes prestan ciertos servicios a empresas, también el Registro Mercantil.

Desde el momento en que alguien se registra como autónomo dándose de alta en el censo de actividades económicas de la Agencia Tributaria, el nombre, DNI, teléfono, correo electrónico y dirección que notifiquen son tratados como información de interés profesional. Como consecuencia de este tratamiento, si los datos coinciden con los datos privados y personales, en algunos epígrafes los datos de trabajadores autoempleados quedan expuestos en internet, fácilmente accesibles a un solo clic desde los buscadores. Además, acaban ofertados a un precio muy asequible: actualmente entre 9 y 40€.

Estos hallazgos en ningún caso deben justificar el cierre al público del registro mercantil. La transparencia debe ser un instrumento para equilibrio de poderes y no está reñida con la preservación de la privacidad personal. Es absolutamente posible incluir las debidas salvaguardas para quiénes no tengan ingresos suficientes para permitirse un domicilio profesional, mientras se permita conocer la titularidad de actividades profesionales.

Creemos que debemos distinguir entre dos tipos de autónomos: aquellos que pueden pagar una oficina, coworking u oficina virtual dónde trabajar o tener una dirección profesional, distinguiéndola así de su domicilio particular, y aquellos que trabajan desde casa y

no tienen medios para tener otro domicilio fiscal y legal para la actividad y cuyo domicilio profesional, por lo tanto, coincide con su domicilio personal. En el caso de estos últimos, dependiendo de su epígrafe, la dirección que queda expuesta a través de los buscadores es la de su domicilio personal.

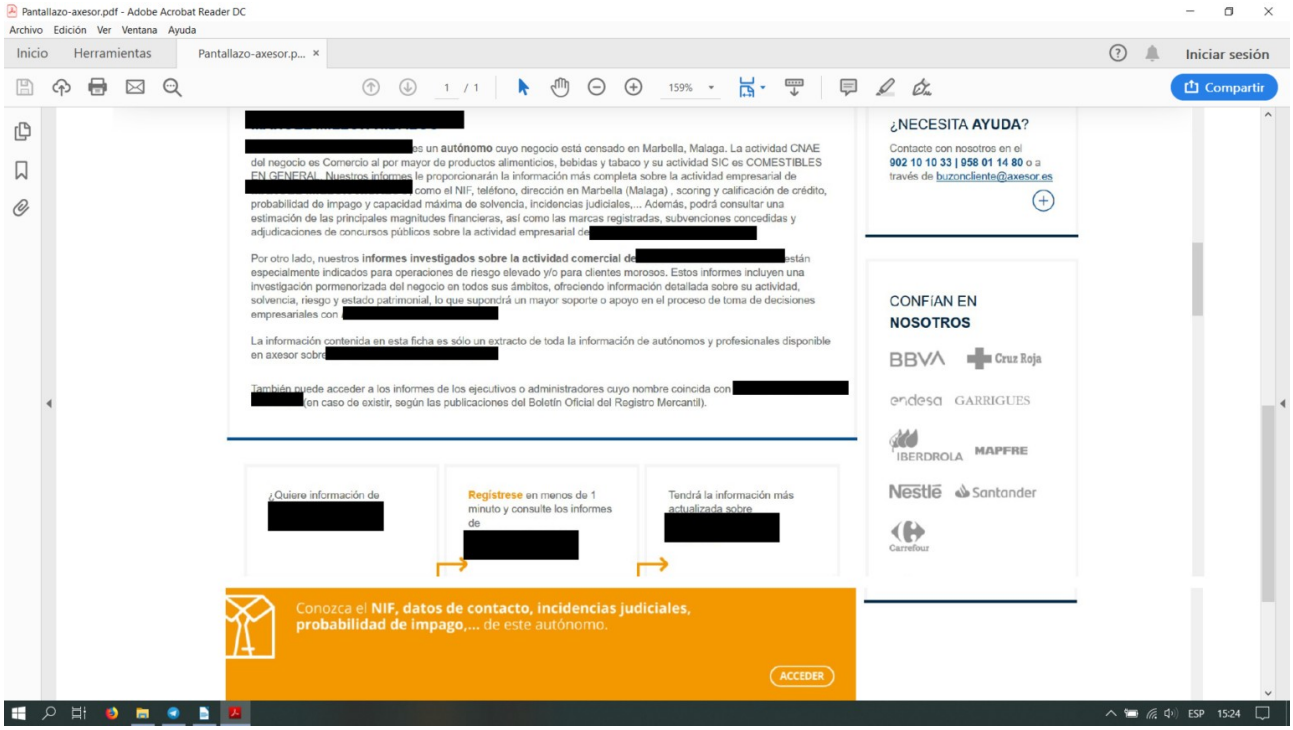
Teniendo en cuenta este hecho, creemos que debería limitarse la posibilidad de difundir y vender los datos de las y los autónomos, en particular los de rentas bajas, para proteger quienes trabajan desde su domicilio personal porque no pueden permitirse un domicilio profesional diferente, para evitar posibles vulneraciones de su intimidad, y más cuando estos datos no se han hecho manifiestamente públicos por los mismos ni sean, en la mayoría de los casos, necesarios para comunicarse con ellos, existiendo medios electrónicos por los que hacerlo sin necesidad de conocer el domicilio de los profesionales. En cumplimiento del principio de minimización de datos, al no ser necesaria esta información, no debería estar disponible públicamente. Por esto proponemos modificaciones legales y recomendaciones para respetar la privacidad a la vez que defendemos la transparencia que debe guiar toda actuación empresarial para no ocultar posibles casos de corrupción o malas praxis.

• Recorrido de los datos: de la Agencia Tributaria **a su venta por internet**

A raíz de una investigación llevada a cabo por algunas de las participantes del Posgrado de Tecnopolítica y Derechos en la Era Digital, dirigido por Simona Levi, Cristina Ribas y David Bondia, se ha descubierto un proceder con indicios de ser lesivo lesivo para la privacidad de las personas que trabajan como autónomas en España, pudiendo afectar directamente en torno al millón de personas con ingresos inferiores a 1000 euros al mes, según datos de Hacienda de 2021.

Presumiblemente, dependiendo del epígrafe, un elevado número de autónomos que incluyan su nombre y apellidos en un buscador como Google, verán que en los resultados datos sobre ellos que no han proporcionado nunca abiertamente en internet, como su dirección de domicilio.

Resultados de búsqueda en Google tras introducir el nombre y apellidos de una o un autónomo.



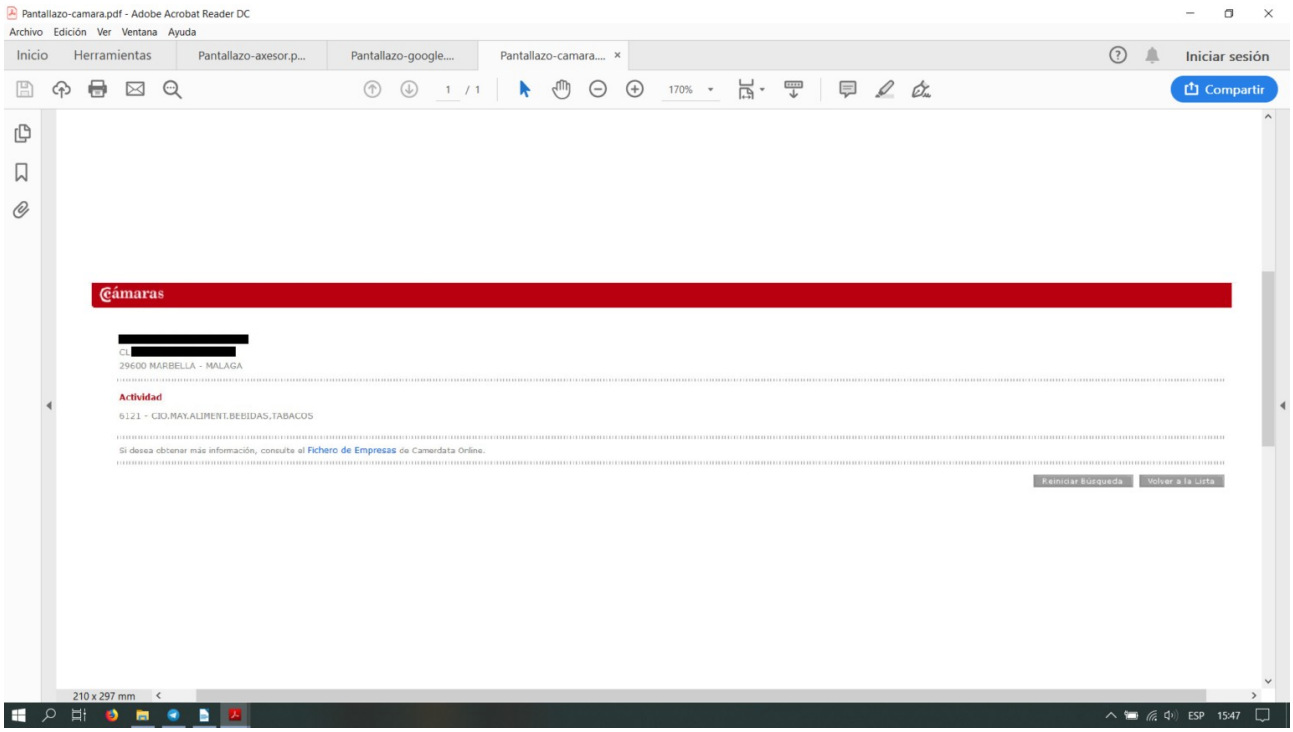
Al entrar en alguno de los enlaces, los datos que aparecen suelen ser, además del nombre y apellidos, su DNI, dirección, correo electrónico, teléfono y actividad comercial, e incluso en ciertos casos información financiera, o incidencias judiciales y probabilidades de impago, y se venden por módicos precios por parte de empresas cuyo negocio consiste en recogerlos y ponerlos a disposición de quien esté dispuesto a pagar por ello.

Información que se ofrece de la misma persona en una página de rating que aparecía como resultado de la búsqueda.

Si nos preguntamos de dónde proceden estos datos vemos que se menciona el Registro Mercantil (donde desde 2018 también deben inscribirse los autónomos que presten ciertos servicios a empresas y asociaciones, entre otros[65]), el Boletín Oficial del Estado, “registros públicos”, etc.
La propia Cámara de Comercio, que en parte también es una institución pública, en el Censo Público de Empresas de su página web, proporciona a cualquiera que haga una búsqueda por apellido, no solo la actividad que ejerce la o el autónomo sino también la dirección, dirigiendo, para conseguir más información a la página web de una entidad privada, CAMERDATA ONLINE[66]:

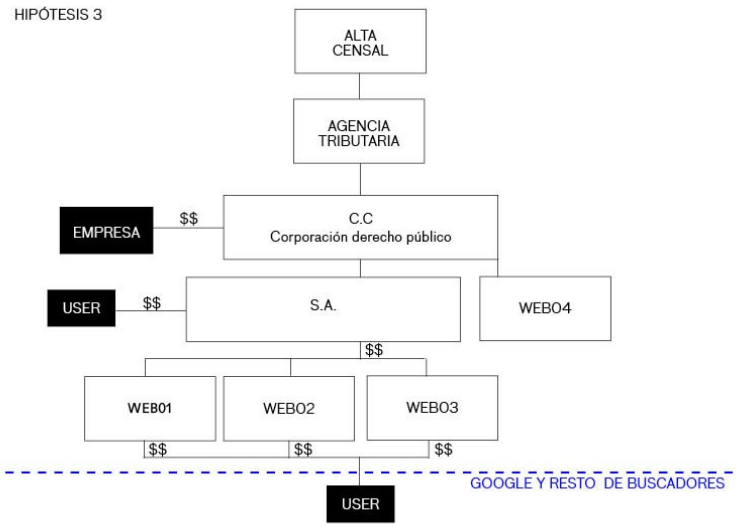
[65] El Real Decreto-Ley 11/2018, de 31 de agosto, estableció la obligación de inscribirse en el Registro de Prestadores de Servicios, además de otras obligaciones según cada caso concreto, a los Empresarios personas físicas y a los Profesionales personas físicas que presten los servicios señalados en el artículo 2.1.o) de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

[66] Incluye un botón de acceso directo al Fichero de Empresas Camerdata Online (https://www.camerdata.es), una empresa privada que parece gestionar estos datos y que también ofrece más información, previo pago.



Información sobre la misma persona que aparece en el Censo Público de Empresas de la Cámara de Comercio de España, que dirige, para obtener más información sobre ella, a la página web de una empresa privada.

Los participantes en el Posgrado de Tecnopolítica y Derechos en la Era Digital y Xnet han trazado el recorrido de estos datos, pasando por las Cámaras de Comercio, hasta llegar a su fuente inicial, la Agencia Tributaria:
AGENCIA TRIBUTARIA → CÁMARAS DE COMERCIO (Censo público de empresas) / BOE / BORME / REGISTRO MERCANTIL → CAMERDATA / EMPRESAS → BUSCADORES



Recorrido de los datos

Xnet pide que se corrijan estas prácticas tanto en las Administraciones Públicas como en entidades privadas.

El nuevo Reglamento Europeo General de Protección de Datos (RGPD) de 2016, supuso un cambio respecto a la legislación española anterior que preveía que los datos profesionales no estuviesen protegidos por las normas de protección de datos.

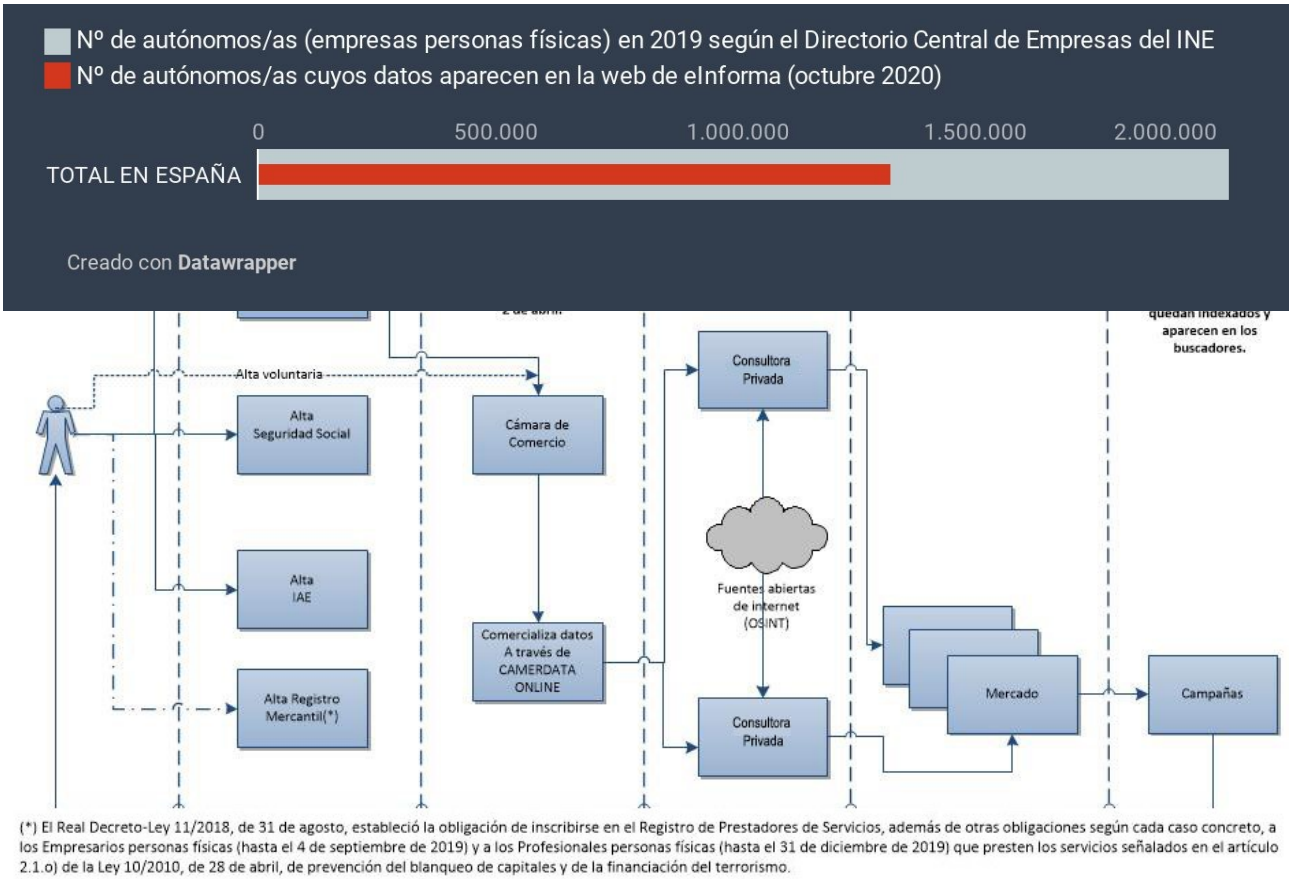
La Ley Orgánica de Protección de Datos española de 2018, con ánimo de querer facilitar el trabajo a las empresas, presupone el «interés legítimo» para el tratamiento de los datos de las y los autónomos, creando de facto una excepción que permite que no sea necesario su consentimiento para tratar sus datos de contacto (Art.19.2 LOPDGDD). Aún así, se indica que esto ha de ser únicamente para mantener relaciones de carácter profesional con ellos, pero en realidad, esto es lo que ahora es utilizado por CAMERDATA, empresas terceras que obtienen los datos y, presumible aunque no explícitamente porque no proporciona información al respecto, por la Cámara de Comercio para justificar el uso de los datos de las y los autónomos para publicarlos, indexarlos, venderlos y realizar campañas de marketing y comunicaciones comerciales. El "interés legítimo" no está pensado para que prevalezca por defecto sino de forma ponderada. Admitir la situación anteriormente descrita, equivale a considerar que estas actividades económicas particulares son de mayor importancia que los derechos y libertades fundamentales a la privacidad e intimidad de autónomos y profesionales. Este es un claro ejemplo del uso que hemos reiteradamente criticado de la “satisfacción de intereses legítimos” del RGPD como “cajón de sastre” por parte de multitud de entidades para justificar y legalizar el tratamiento de datos personales cuando no disponen de otra base jurídica para amparar actividades que necesitan más justificación y análisis porque podrían vulnerar los derechos, libertades e intereses de las personas.

No podemos estar de acuerdo con este hecho. Además, los datos de las y los autónomos están siendo utilizados para cumplir con finalidades de las que no se ha recibido información en el momento de proporcionarlos a la Agencia Tributaria, quien no les informa, en el momento de la recogida de los mismos sobre este uso comercial.

Algo similar ocurre con las Cámaras de Comercio y toda la cadena de empresas que se benefician del uso y cesión de los datos de las y los autónomos, quienes no informan correctamente a las y los autónomos de las comunicaciones de datos que se están llevando a cabo, ni para qué son tratados, y retuercen así el espíritu de las exclusiones previstas por las normas de protección de datos que en principio deben utilizarse solo excepcionalmente.

La falta de información al respecto conlleva que gran parte de las y los autónomos no conozca los derechos que tiene en relación con los tratamientos que se llevan a cabo por estas entidades (como el derecho a oponerse a que se realicen o el derecho a que sus datos se supriman, aunque, hemos verificado, a cada remesa, reaparecen) ni cómo deben ejercerlos ante estas. Debemos recordar además que el Reglamento europeo se basa en el principio rector de que la privacidad debe ser desde el diseño y por defecto o sea que el esfuerzo para mantener a salvo los datos y el cumplimiento de las obligaciones como asegurarse de la legalidad del tratamiento o cesión de datos o el deber de información no debería depender de las personas sino que debería tener lugar desde el diseño del protocolo institucional para recoger y almacenar estos datos.

Lo que vemos aquí es que autónomos y profesionales pierden el control sobre sus datos sin saberlo, descubriendo, quizás por la publicación de este informe, quizás por buscar su propio nombre en un buscador, que hay quien se lucra con sus datos.



Ciclo por el que se exponen y ponen a la venta los datos de las personas en régimen de autónomos

• Sesgo por poder adquisitivo y contractual

Existe otro hecho a tomar en consideración: no todas las y los autónomos encuentran su información publicada y a disposición en los buscadores y páginas web. A primera vista resultaba incomprensible entender según qué criterio los datos de algunos se encontraban, mientras los de otros no. Con un análisis más pormenorizado realizado por Alba Soler, Carmelo Ordóñez, Jose Luis Ribés como investigadores participantes en el Posgrado de Tecnopolítica y Derechos en la Era Digital, utilizando como caso de estudio los datos tratados por EInforma en 2019, se detectó un posible sesgo relacionado con el tipo de actividad económica llevada a cabo.

Según datos del 2019, existen unos 2.047.779 autónomos/as en España (autónomos/as no socios en sociedades mercantiles o cooperativas) según el directorio (DIRCE) del Instituto Nacional de Estadística (y Seguridad Social para el sector primario) y 1.336.408 cuyos datos aparecen y se comercializan en la web eInforma.com.

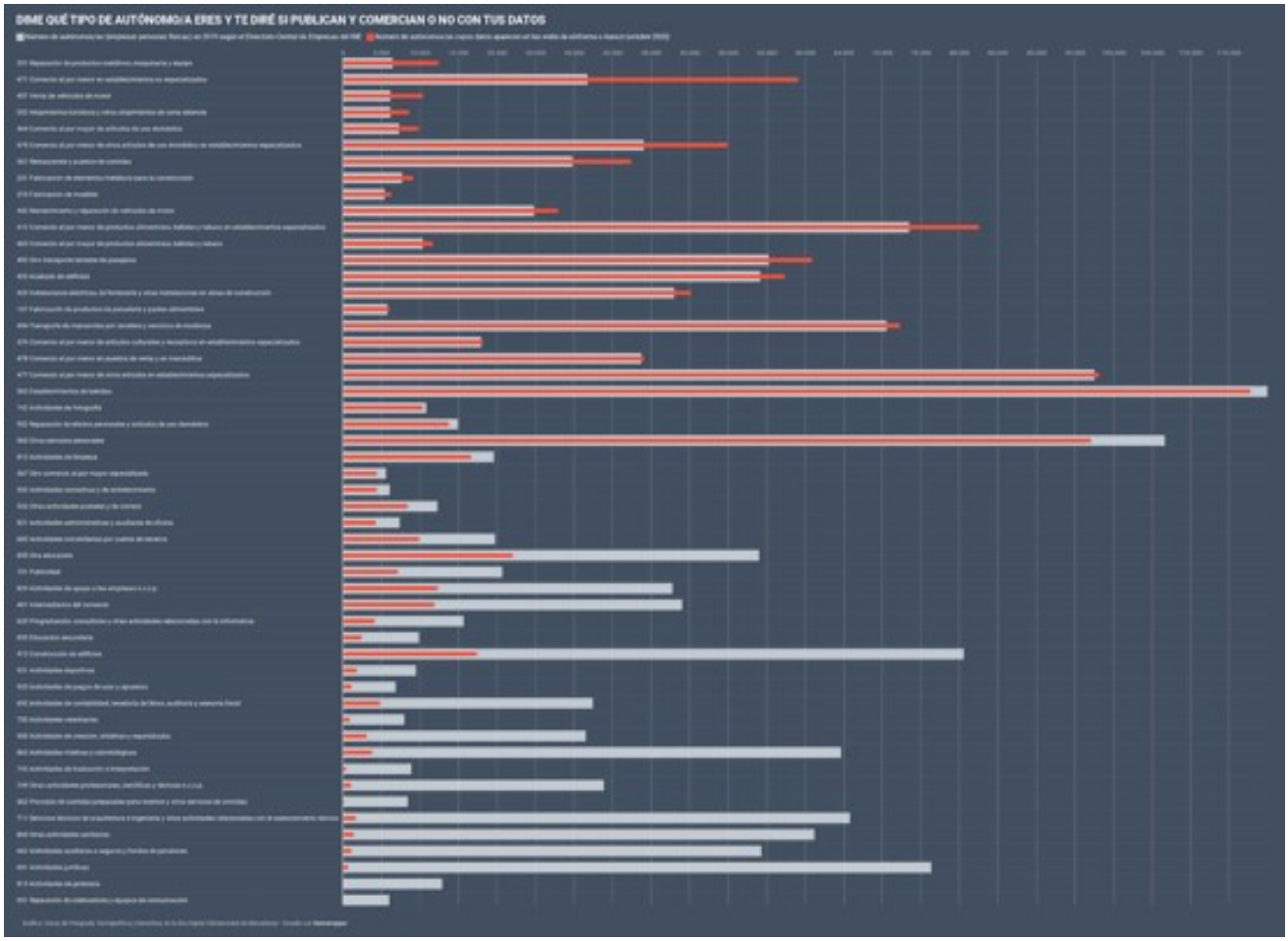
Comparativa entre el número de autónomos y aquellos cuyos datos aparecen en eInforma

Desagregando por tipo de actividad económica desarrollada, la investigación ha aflorado que la situación cambia dependiendo de qué actividad se desempeña:

1) En mayor medida son actividades cuyos colectivos están en total o considerable medida englobados en colegios profesionales oficiales las que cuentan con una reducida o despreciable presencia en estas webs (con alguna que otra excepción a esta regla). Cabe destacar que los datos personales de estos profesionales suelen estar publicados por sus respectivos colegios, pero no se hace un tratamiento comercial de los mismos.

2) Por contra, las actividades del pequeño comercio, limpieza, transporte, de cuidados, tratamientos y servicios personales, aparecen sobredimensionadas, o sea, encuentran que sus datos están más expuestos. Además, aparecen datos de decenas de miles de aquellas personas que estuvieron, pero ya no, dadas de alta en el Régimen Especial de Trabajadores Autónomos.

Apreciamos, pues, un sesgo relacionado con el poder adquisitivo y con el poder de negociación de las y los trabajadores, donde en general los más vulnerables son más expuestos.



RECOMENDACIONES

Fruto del análisis realizado, para garantizar y proteger el derecho de las personas de controlar el uso y destino de sus datos, en línea con la legislación internacional de derechos humanos, desde XNet recomendamos:

• Proteger los datos personales de las y los autónomos cuando puedan coincidir con los profesionales por motivos de poder adquisitivo.
Enmendar la ley para hacer que la protección de datos personales de las y los autónomos y profesionales prime por defecto cuando sus datos profesionales y personales coincidan por no poderse permitir alternativas. Entre la normativa a modificar, a parte las pormenorizadas más adelante, se podría considerar incluso la LSSI y legislaciones análogas que obliguen a publicar los datos de domicilio del prestador de servicios, por ejemplo en el aviso legal de las páginas web. Esto evitaría además casos de chantaje y de suplantación de identidad.

Nosotros defendemos la importancia de la transparencia de los datos profesionales para evitar la corrupción, por esto dichas enmiendas deben aplicarse solo hasta un cierto nivel de ingresos anuales (3,5 veces el Indicador Público de Renta de Efectos Múltiples (IPREM)) y cuando el domicilio personal (de empadronamiento o residencia) coincide con el profesional.

Desde la defensa de que los Registros deben ser, cuanto antes, públicos y de acceso gratuito, al mismo tiempo consideramos necesario que el censo público de empresas y profesionales elaborado por la Cámara de Comercio y el Registro Mercantil recojan, pero no publique o anonimice, la dirección de las y los autónomos cuando esta coincida con la dirección de empadronamiento o residencia si, por su cifra de negocio (inferior a la aquí propuesta), no pueden permitirse otra dirección alternativa para uso profesional. Esta información sólo debería entregarse bajo petición con el consentimiento de la persona afectada o por mandato judicial. Recomendamos explorar la misma posibilidad en la LSSi, siendo un email válido la mejor manera de comunicarse con el responsable de una web.

Así, la información no debe ser cedida a Camerdata para su venta a empresas privadas que explotan la información económicamente.

Además, deben establecerse sanciones más rigurosas en caso de explotación económica por medio de venta o publicación de información recabada de forma masiva de bases de datos que puedan afectar derechos fundamentales, sin que esto afecte al uso del open data para el interés general. Para más inri cuando se trata de bases de datos públicas, pero cuyo acceso completo es mediado por pagos, se crea un sesgo de acceso relacionado con el poder adquisitivo.

• Reforzar el derecho de la ciudadanía a conocer y poder oponerse por defecto al uso y destino de sus datos.
Informar correctamente a la ciudadanía sobre las comunicaciones de datos que se llevaran a cabo y las finalidades de las mismas, indicando con claridad la Ley en que están previstas, para asegurarse de que la aceptación sea voluntaria y bien informada, como exige el RGPD, y que se ejerza plenamente el derecho a la autodeterminación informativa. Esto sobre todo en los casos en que los datos no sean recogidos directamente del afectado o sean objeto de cesión, incluso cuando procedan o se cedan desde instituciones públicas y/o de “fuentes de acceso público”.

• Concretar la definición de “intereses legítimos” y de otra terminología ambigua.
Es necesario para evitar que se justifique y legalice el tratamiento de datos personales cuando no se dispone de ninguna base jurídica sólida y justificada. Respeto a los derechos, libertades e intereses de las personas no debe ser posible escudarse en extremos que sirvan de cajón de sastre y que acaben invalidado el espíritu de la normativa para que prime el principio de privacidad desde el diseño y por defecto, que debe tenerse en cuenta, tanto en la concepción de un tratamiento de datos personales como en

su desarrollo.

Creemos en el efecto disuasorio y preventivo de estas medidas.

Por todo ello, requerimos las siguientes modificaciones legales:Modificación del art.8 de la Ley 4/2014, de 1 de abril, Básica de las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación.

Modificación del art. 421 del Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil.

Y posiblemente, modificación de los artículos 3, 8, 11, 12 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

RECOMENDACIONES DE BUENAS PRÁCTICAS PARA LAS ADMINISTRACIONES PÚBLICAS

ANTERIORES A LA MODIFICACIÓN DE LA LEY PARA IMPULSAR SU APLICACIÓN

• Reforzar la obligación de informar sobre las cesiones de datos proporcionando a las y los afectados información completa sobre el tratamiento de sus datos personales y permitir que indiquen que los datos proporcionados a las Administraciones Públicas NO pueden tratarse con objetivos comerciales ni por parte de la Administración ni por parte de terceros. Cuando sus ingresos son inferiores a 3,5 veces el IPREM y los datos de domicilio profesional se corresponden a los datos de empadronamiento o residencia, permitir que indiquen que NO pueden publicarse los datos y que solo se puedan acceder tras un requerimiento.

Incluir cláusulas en los contratos que obliguen a las terceras entidades, tanto públicas como privadas, a las que se comunican los datos a informar a las y los afectados de la comunicación y de los usos de los datos por su parte para que no se escuden en las exclusiones previstas por la Ley o Reglamento de forma abusiva.

• No fundamentar las comunicaciones de datos a terceras entidades privadas en el interés legítimo de las mismas para evitar recoger el consentimiento de la ciudadanía afectada. Se ha de requerir que los intereses se pormenoricen y justifiquen.

• Cuando la o el afectado ejerza sus derechos de protección de datos, comunicarlo a las entidades a quienes se hayan cedido sus datos personales para que también rectifiquen, supriman o limiten el tratamiento de los mismos y no lo vuelvan a publicar en «remesas» posteriores.

ENMIENDAS A LA LEY

Modificación de la Ley 4/2014, de 1 de abril, Básica de las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación.

Para alcanzar el fin propuesto, debemos solicitar la enmienda del artículo 8 de la Ley “Censo público”, que quedaría redactado como sigue:

Las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación elaborarán un censo público de empresas del que formarán parte las personas físicas o jurídicas, nacionales o extranjeras, que ejerzan las actividades comerciales, industriales, de servicios y navieras en territorio nacional, para cuya elaboración contarán con la colaboración de la administración tributaria competente así

como de otras administraciones que aporten la información necesaria, garantizando, en todo caso, la confidencialidad en el tratamiento y el uso exclusivo de dicha información.
En ningún caso será objeto de publicación y divulgación ***pública la dirección profesional cuando esta coincida con sus datos personales de residencia, siempre y cuando sus ingresos*** anuales sean inferiores a 3,5 veces el IPREM. Esta información sólo se entregará bajo petición con el consentimiento de la persona afectada o por mandato judicial.
En aplicación del principio de minimización de datos, solo serán publicados los datos mínimos imprescindibles como nombre, apellidos, actividad y número identificativo siguiendo las normas específicas existentes sobre su difusión.
Para la elaboración del censo público de empresas las administraciones tributarias facilitarán a la Cámara Oficial de Comercio, Industria, Servicios y Navegación de España y a las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación los datos del Impuesto sobre Actividades Económicas y los censales de las empresas que sean necesarios. Únicamente tendrán acceso a la información facilitada por la administración tributaria los empleados de cada Cámara que determine el pleno.
Esta información se empleará para la elaboración del censo público de empresas, para el cumplimiento de las funciones público-administrativas que la presente Ley atribuye a las Cámaras así como para la elaboración del censo electoral a que se hace referencia en el artículo 17 de la misma.
Dicho personal tendrá, con referencia a los indicados datos, el mismo deber de sigilo que los funcionarios de la administración tributaria. El incumplimiento de este deber constituirá, en todo caso, infracción muy grave de conformidad con su régimen disciplinario.

Modificación del Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil.

Para alcanzar el fin propuesto, debemos solicitar la enmienda del apartado primero del artículo 421 del Real Decreto “Sección 1.ª: Empresarios”, que quedaría redactado como sigue:

1. El Registrador Mercantil Central determinará el contenido de la sección 1.ª del boletín, e incluirá en ella los datos remitidos por los Registradores Mercantiles.
En el apartado «actos inscritos» se recogerán los datos a que se refieren los artículos 386 a 391.En el apartado «otros actos publicados en el Registro Mercantil» se recogerán los datos a que se refiere el artículo 392.
No serán objeto de publicación los datos relativos al documento nacional de identidad o número de identificación fiscal, número de identidad de extranjero o, en su defecto, el de su pasaporte o documento de viaje a los que se refieren los artículos 386.5.º, 387.1.8.º, 388.3 y 389, último párrafo. Tampoco serán objeto ***de publicación la dirección que pudiese constar sobre los empresarios individuales, cuando coincida con su dirección personal no profesional siempre y cuando sus ingresos anuales sean inferiores a 3,5 veces el*** IPREM.

Modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Para alcanzar el fin propuesto, debemos solicitar la enmienda de 3 artículos de la Ley:

Con la modificación del apartado 2 del Artículo 19. Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales, que quedaría redactado como sigue:

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:
a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.
b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.
3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio

de sus competencias.

Con la introducción de un nuevo apartado en el Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos cuyo título incluiría “e interés legítimo” y quedaría redactado como sigue:

- Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos e interés legítimo.
  3. El tratamiento ***de la dirección personal*** solo podrá considerarse fundado en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero en los términos previstos en el artículo 6.1.f) del Reglamento (UE) 2016/679, siempre que no prevalezcan, tras la realización de una evaluación minuciosa y documentada, los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, teniendo en cuenta las expectativas razonables de los interesados, sobre todo en caso de tratamiento ulterior de los datos, basadas en su relación con el responsable, la información proporcionada sobre el tratamiento, las circunstancias del tratamiento y las posibles consecuencias que pueden derivar del mismo.

Con la modificación de los apartados 2 y 3 y la introducción de un nuevo apartado 4 del Artículo 11. Transparencia e información al afectado., que quedaría redactado como sigue:

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:
a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
d) Los destinatarios de los datos, en su caso.
Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.
3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE)
2016/679 facilitando a aquél la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
En estos supuestos, la información básica incluirá también:
a) Las categorías de datos objeto de tratamiento.
b) Las fuentes concretas de las que procedieran los datos
4. Las disposiciones del apartado 5 del artículo 14 del Reglamento (UE) 2016/679 se aplicarán restrictivamente. Se considerará que la comunicación de la información supone un esfuerzo desproporcionado cuando no pueda disponerse de un medio de contacto escrito (físico o electrónico) con los interesados.

Con la introducción de un nuevo apartado en el Artículo 12. Disposiciones generales sobre ejercicio de los derechos que quedaría redactado como sigue:

8. El responsable del tratamiento comunicará a los destinatarios y encargados del tratamiento cualquier rectificación, supresión, limitación del tratamiento u oposición al tratamiento efectuada con arreglo a la presente Ley para que realicen la misma actuación que él. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Proyecto de Xnet coordinado por Simona Levi conjuntamente con Míriam Carles y a partir del trabajo de investigadoras del posgrado Tecnopolítica y Derechos en la Era Digital dirigido por Simona Levi, Cristina Ribas y David Bondia. La investigadora iniciadora del trabajo ha pedido no hacer público su nombre.

Con contribuciones de los investigadores Alba Soler, Carmelo Ordóñez, Jose Luis Ribés Carlos García, Carlos Amat, G.A.LL. del posgrado sobre Tecnopolítica y Derechos en la Era Digital.

Última actualización: noviembre 2022.

Investigación realizada en parte con el apoyo de la Agència de Transparència del Àrea Metropolitana de Barcelona (AMB) y del Ajuntament de Barcelona (En ambos casos, subvenciones)

ANEXOS

- XNET

ANEXO de

1 – ABUSO DE IDENTIFICACIÓN POR PARTE DE LAS INSTITUCIONES vs MINIMIZACIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

ANÁLISIS DE LA JURISPRUDENCIA Y RESOLUCIONES RELEVANTES

Jurisprudencia y resoluciones internacionales

El Tribunal Europeo de Derechos Humanos, el 14 de abril de 2009, en el caso *Tásaság a Szabadsñagjogokért c. Hungría*[67] admitió que constituye una vulneración del artículo 10 del Convenio Europeo de Derechos Humanos, referido a la libertad de expresión e información, el hecho de negar a una ONG dedicada a la promoción de los derechos fundamentales el acceso al recurso presentado ante el Tribunal Constitucional por un parlamentario, entre otros, para que el tribunal revisase las enmiendas realizadas al Código Penal, considerando que dicho recurso, y en particular cuando es presentada por un miembro del Parlamento, constituye indudablemente una cuestión de interés público.

El Tribunal Europeo aprovechó para recordar la jurisprudencia sistemática del mismo relacionada con la libertad de prensa según la cual el público tiene derecho a recibir información de interés general.

Jurisprudencia y resoluciones nacionales

Tras la entrada en vigor el 10 de diciembre de 2014 de la Ley 19/2019 de Transparencia, acceso a la información pública y buen gobierno, el 17 de diciembre de 2014, Access Info Europe presentó una queja ante el Defensor del Pueblo[68] en la que, entre otros, manifestaba que era contraria a la aplicación del requisito de hacer constar la identidad del solicitante del artículo 17.2.ª) de la Ley 19/2013 en las solicitudes de acceso a la información pública. Lo hacía alegando que la identidad del solicitante era irrelevante cuando se solicitaba dicho acceso y por lo tanto constituía una formalidad innecesaria que requería más esfuerzos y recursos de los que serían necesarios para cumplir con la finalidad de la Ley de transparencia, suponiendo al mismo tiempo una traba para el acceso a la información pública, siendo la no-identificación un factor clave para que la sociedad civil pueda ejercer sus derechos.

A esta queja, el Defensor del Pueblo respondió el 15 de marzo de 2015[69], y sobre la cuestión relativa al requisito de identificación expuso lo siguiente:

> *"Por último, hay que señalar que en nuestro Derecho las solicitudes anónimas no tienen validez ni producen efectos jurídicos. Tanto del artículo 70 de la Ley 30/1992, como del 17.2 de la Ley 19/2013 se desprende con claridad que es necesario acreditar el nombre y apellidos de la persona física o el nombre de la persona jurídica que ejerza el derecho de acceso. No cabe, como defiende ACCESS INFO EUROPE una solicitud anónima, porque así se desprende sin género de dudas del tenor literal del artículo 17.2.ª) y 70.1.a) y d) de la Ley, pero también porque existen una serie de límites al derecho de acceso que habrán de ser ponderados atendiendo a los intereses en juego (artículo 14 de la Ley 19/2013), obligaciones referidas a la protección de datos (artículo 15 de la Ley 19/2013) y causas de no admisión de las solicitudes de acceso, como la de que sea manifiestamente repetitiva o tengan un carácter abusivo o injustificado con la finalidad de transparencia (artículo 18 de la Ley 19/2013), en cuya valoración y estudio puede ser relevante e incluso determinante la identidad del solicitante."*

Así, el Defensor del Pueblo se limitó a confirmar el contenido de la Ley, sin hacer referencia a los tratados internacionales que regulan el supuesto que le fue presentado, entre los cuales, la mayoría reconocen el derecho de obtener información y el Convenio núm. 205 del Consejo de Europa admite que los solicitantes puedan mantener su anonimato.

Además, como es corriente en el Estado español, el Defensor del Pueblo alegó, para defender su posición, que conocer la identidad del solicitante es necesaria para valorar la aplicabilidad de los límites establecidos por la misma Ley de Transparencia. Límites que

[67] *Resumen de la sentencia:* https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-1581%22]}

[68] Access Info Europe presenta una queja ante el Defensor del Pueblo español por la deficiente implementación del derecho de acceso a la información: https://www.access-info.org/es/esp-es/13631

[69] Respuesta del Defensor del Pueblo a la queja de Access Info Europe, 15 de marzo de 2015: https://www.access-info.org/wp-content/uploads/Respuesta_DefensorPueblo_LeyTransp.pdf

pueden evaluarse sin embargo sin necesidad de conocer la identidad del mismo:

- En lo que se refiere a los límites establecidos por el artículo 14 de la Ley 19/2013, son límites objetivos, que hacen referencia a la información solicitada, y en los que la identidad del solicitante no tiene ni debería considerarse.

- En lo que se refiere a los límites previstos por el artículo 15 de la Ley 19/2013, estos hacen referencia a la protección de los datos personales que estén presentes, también, en la información solicitada. El artículo menciona que cuando la información contenga datos personales, deberá hacerse una ponderación razonada "entre el interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada". Vemos que en ningún momento el artículo 15 tiene en consideración la identidad del solicitante sino al interés público de la divulgación de la información.

- Sobre los límites del artículo 18 de la Ley 19/2013, el Defensor del Pueblo no tiene en cuenta todas las causas de inadmisión previstas por el mismo, la mayoría de las cuales hacen referencia a la información solicitada y no a la persona del solicitante. La única causa de inadmisión en este artículo que puede tener en consideración persona del solicitante es la repetitividad de las solicitudes de acceso, para cuya evaluación podrían tenerse en consideración otros parámetros distintos de la identidad del solicitante, como por ejemplo el envío de múltiples solicitudes desde la misma dirección de correo electrónico.

De la formulación de esta queja por parte de Access Info Europe derivó otra resolución del Defensor del Pueblo, de 22 de septiembre de 2015[70], en la que éste respondía al Ministerio de Presidencia, recomendando estudiar la posibilidad de contemplar como vía de presentación de solicitudes de acceso a información pública el correo electrónico en que debiesen reflejarse el nombre, apellidos y el número del DNI. Así, el Defensor, confirmando que la identificación electrónica mediante el sistema Cl@ve resulta excesivamente compleja y larga, disuadiendo el ejercicio del derecho de acceso a la información pública, prevé la posibilidad de que no sea utilizado pero no prevé la posibilidad de no requerir la identificación de los solicitantes cuando piden acceso a información pública, sin cambiar su posición respecto a la resolución anterior.

[70] https://www.defensordelpueblo.es/resoluciones/recomendacion-a-la-oficina-para-la-reforma-de-la-administracion-opera-para-que-estudie-la-posibilidad-de-contemplar-como-via-de-presentacion-por-los-ciudadanos-para-el-ejercicio-del-derecho-de-acces/

LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

Declaración Universal de los Derechos Humanos, adoptada y proclamada por la Asamblea General de las Naciones Unidas en su resolución 217 A (III), de 10 de diciembre de 1948

Artículo 19.

Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

· **Pacto Internacional de Derechos Civiles y Políticos, Resolución 2200 A (XXI) de la Asamblea General de las Naciones Unidas, aprobada el 16 de diciembre de 1966.**

Artículo 19.

1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Convenio de Roma del 4 de noviembre de 1950, del Consejo de Europa.

Artículo 10. *Libertad de expresión.*

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa

Convenio núm. 205 del Consejo de Europa sobre acceso a los documentos públicos de 2009 / Council of Europe Convention No. 205 on Access to Official Documents

Article 4. *Requests for access to official documents*

1 An applicant for an official document shall not be obliged to give reasons for having access to

the official document.

2 Parties may give applicants the right to remain anonymous except when disclosure of identity is essential in order to process the request.

3 Formalities for requests shall not exceed what is essential in order to process the request.

Constitución Española de 1978.

Artículo 105.

La ley regulará:

(…) b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 9. *Sistemas de identificación de los interesados en el procedimiento.*

1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.

2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad. En particular, serán admitidos, los sistemas siguientes:

a) Sistemas basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.

b) Sistemas basados en certificados electrónicos reconocidos o cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

Cada Administración Pública podrá determinar si sólo admite alguno de estos sistemas para realizar determinados trámites o procedimientos, si bien la admisión de alguno de los sistemas de identificación previstos en la letra c) conllevará la admisión de todos los previstos en las letras a) y b) anteriores para ese trámite o procedimiento.

3. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.

Artículo 11. *Uso de medios de identificación y firma en el procedimiento administrativo.*

1. Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.

2. Las Administraciones Públicas sólo requerirán a los interesados el uso obligatorio de firma para:

a) Formular solicitudes.

b) Presentar declaraciones responsables o comunicaciones.

c) Interponer recursos.

d) Desistir de acciones.

e) Renunciar a derechos.

Artículo 13. *Derechos de las personas en sus relaciones con las Administraciones Públicas.*

Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos:

a) A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración.

b) A ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.

c) A utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del ordenamiento jurídico.

d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.

e) A ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones.

f) A exigir las responsabilidades de las Administraciones Públicas y autoridades, cuando así corresponda legalmente.

g) A la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley.

h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

i) Cualesquiera otros que les reconozcan la Constitución y las leyes.

Estos derechos se entienden sin perjuicio de los reconocidos en el artículo 53 referidos a los interesados en el procedimiento administrativo.

Artículo 129. *Principios de buena regulación.*

(…) 5. En aplicación del principio de transparencia, las Administraciones Públicas posibilitarán el acceso sencillo, universal y

actualizado a la normativa en vigor y los documentos propios de su proceso de elaboración, en los términos establecidos en el artículo 7 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno; definirán claramente los objetivos de las iniciativas normativas y su justificación en el preámbulo o exposición de motivos; y posibilitarán que los potenciales destinatarios tengan una participación activa en la elaboración de las normas.

Disposición adicional primera. *Especialidades por razón de materia.*

1. Los procedimientos administrativos regulados en leyes especiales por razón de la materia que no exijan alguno de los trámites previstos en esta Ley o regulen trámites adicionales o distintos se regirán, respecto a éstos, por lo dispuesto en dichas leyes especiales.

2. Las siguientes actuaciones y procedimientos se regirán por su normativa específica y supletoriamente por lo dispuesto en esta Ley:

a) Las actuaciones y procedimientos de aplicación de los tributos en materia tributaria y aduanera, así como su revisión en vía administrativa.

b) Las actuaciones y procedimientos de gestión, inspección, liquidación, recaudación, impugnación y revisión en materia de Seguridad Social y Desempleo.

c) Las actuaciones y procedimientos sancionadores en materia tributaria y aduanera, en el orden social, en materia de tráfico y seguridad vial y en materia de extranjería.

d) Las actuaciones y procedimientos en materia de extranjería y asilo.

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Artículo 2. *Ámbito subjetivo de aplicación.*

1. Las disposiciones de este título se aplicarán a:

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla y las entidades que integran la Administración Local.

b) Las entidades gestoras y los servicios comunes de la Seguridad Social así como las mutuas de accidentes de trabajo y enfermedades profesionales colaboradoras de la Seguridad Social.

c) Los organismos autónomos, las Agencias Estatales, las entidades públicas empresariales y las entidades de Derecho Público que, con independencia funcional o con una especial autonomía reconocida por la Ley, tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad.

d) Las entidades de Derecho Público con personalidad jurídica propia, vinculadas a cualquiera de las Administraciones Públicas o dependientes de ellas, incluidas las Universidades públicas.

e) Las corporaciones de Derecho Público, en lo relativo a sus actividades sujetas a Derecho Administrativo.

f) La Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de

Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con sus actividades sujetas a Derecho Administrativo.

g) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100.

h) Las fundaciones del sector público previstas en la legislación en materia de fundaciones.

i) Las asociaciones constituidas por las Administraciones, organismos y entidades previstos en este artículo. Se incluyen los órganos de cooperación previstos en el artículo 5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en la medida en que, por su peculiar naturaleza y por carecer de una estructura administrativa propia, le resulten aplicables las disposiciones de este título. En estos casos, el cumplimiento de las obligaciones derivadas de la presente Ley serán llevadas a cabo por la Administración que ostente la Secretaría del órgano de cooperación.

2. A los efectos de lo previsto en este título, se entiende por Administraciones Públicas los organismos y entidades incluidos en las letras a) a d) del apartado anterior.

Artículo 3. *Otros sujetos obligados.*

Las disposiciones del capítulo II de este título serán también aplicables a:

a) Los partidos políticos, organizaciones sindicales y organizaciones empresariales

b) Las entidades privadas que perciban durante el período de un año ayudas o subvenciones públicas en una cuantía superior a 100.000 euros o cuando al menos el 40 % del total de sus ingresos anuales tengan carácter de ayuda o subvención pública, siempre que alcancen como mínimo la cantidad de 5.000 euros.

Artículo 4. *Obligación de suministrar información.*

Las personas físicas y jurídicas distintas de las referidas en los artículos anteriores que presten servicios públicos o ejerzan potestades administrativas estarán obligadas a suministrar a la Administración, organismo o entidad de las previstas en el artículo 2.1 a la que se encuentren vinculadas, previo requerimiento, toda la información necesaria para el cumplimiento por aquéllos de las obligaciones previstas en este título. Esta obligación se extenderá a los adjudicatarios de contratos del sector público en los términos previstos en el respectivo contrato.

Artículo 5. *Principios generales.*

1. Los sujetos enumerados en el artículo 2.1 publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública.

2. Las obligaciones de transparencia contenidas en este capítulo se entienden sin perjuicio de la aplicación de la normativa autonómica correspondiente o de otras disposiciones específicas que prevean un régimen más amplio en materia de publicidad.

3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos.

4. La información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización.

Cuando se trate de entidades sin ánimo de lucro que persigan exclusivamente fines de interés social o cultural y cuyo presupuesto sea inferior a 50.000 euros, el cumplimiento de las obligaciones derivadas de esta Ley podrá realizarse utilizando los medios mayor parte de las ayudas o subvenciones públicas percibidas.

5. Toda la información será comprensible, de acceso fácil y gratuito y estará a disposición de las personas con discapacidad en una modalidad suministrada por medios o en formatos adecuados de manera que resulten accesibles y comprensibles, conforme al principio de accesibilidad universal y diseño para todos.

Artículo 6. *Información institucional, organizativa y de planificación.*

1. Los sujetos comprendidos en el ámbito de aplicación de este título publicarán información relativa a las funciones que desarrollan, la normativa que les sea de aplicación así como a su estructura organizativa. A estos efectos, incluirán un organigrama actualizado que identifique a los responsables de los diferentes órganos y su perfil y trayectoria profesional.

2. Las Administraciones Públicas publicarán los planes y programas anuales y plurianuales en los que se fijen objetivos concretos, así como las actividades, medios y tiempo previsto para su consecución. Su grado de cumplimiento y resultados deberán ser objeto de evaluación y publicación periódica junto con los indicadores de medida y valoración, en la forma en que se determine por cada Administración competente.

En el ámbito de la Administración General del Estado corresponde a las inspecciones generales de servicios la evaluación del cumplimiento de estos planes y programas.

Artículo 6 bis. *Registro de actividades de tratamiento.*

Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.

Artículo 7. *Información de relevancia jurídica.*

Las Administraciones Públicas, en el ámbito de sus competencias, publicarán:

a) Las directrices, instrucciones, acuerdos, circulares o respuestas a consultas planteadas por los particulares u otros órganos en la medida en que supongan una interpretación del Derecho o tengan efectos jurídicos.

b) Los Anteproyectos de Ley y los proyectos de Decretos Legislativos cuya iniciativa les corresponda, cuando se soliciten los dictámenes a los órganos consultivos correspondientes. En el caso en que no sea preceptivo ningún dictamen la publicación se realizará en el momento de su aprobación.

c) Los proyectos de Reglamentos cuya iniciativa les corresponda. Cuando sea preceptiva la solicitud de dictámenes, la publicación se producirá una vez que estos hayan sido solicitados a los órganos consultivos correspondientes sin que ello suponga, necesariamente, la apertura de un trámite de audiencia pública.

d) Las memorias e informes que conformen los expedientes de elaboración de los textos normativos, en particular, la memoria del análisis de impacto normativo regulada por el Real Decreto 1083/2009, de 3 de julio.

e) Los documentos que, conforme a la legislación sectorial vigente, deban ser sometidos a un período de información pública durante su tramitación.

Artículo 8. *Información económica, presupuestaria y estadística.*

1. Los sujetos incluidos en el ámbito de aplicación de este título deberán hacer pública, como mínimo, la información relativa a los actos de gestión administrativa con repercusión económica o presupuestaria que se indican a continuación:

a) Todos los contratos, con indicación del objeto, duración, el importe de licitación y de adjudicación, el procedimiento utilizado para su celebración, los instrumentos a través de los que, en su caso, se ha publicitado, el número de licitadores participantes en el procedimiento y la identidad del adjudicatario, así como las modificaciones del contrato. Igualmente serán objeto de publicación las decisiones de desistimiento y renuncia de los contratos. La publicación de la información relativa a los contratos menores podrá realizarse trimestralmente.

Asimismo, se publicarán datos estadísticos sobre el porcentaje en volumen presupuestario de contratos adjudicados a través de cada uno de los procedimientos previstos en la legislación de contratos del sector público.

b) La relación de los convenios suscritos, con mención de las partes firmantes, su objeto, plazo de duración, modificaciones realizadas, obligados a la realización de las prestaciones y, en su caso, las obligaciones económicas convenidas. Igualmente, se publicarán las encomiendas de gestión que se firmen, con indicación de su objeto, presupuesto, duración, obligaciones económicas y las subcontrataciones que se realicen con mención de los adjudicatarios, procedimiento seguido para la adjudicación e importe de la misma.

c) Las subvenciones y ayudas públicas concedidas con indicación de su importe, objetivo o finalidad y beneficiarios.

d) Los presupuestos, con descripción de las principales partidas presupuestarias e información actualizada y comprensible sobre su estado de ejecución y sobre el cumplimiento de los objetivos de estabilidad presupuestaria y sostenibilidad financiera de las Administraciones Públicas.

e) Las cuentas anuales que deban rendirse y los informes de auditoría de cuentas y de fiscalización por parte de los órganos de control externo que sobre ellos se emitan.

f) Las retribuciones percibidas anualmente por los altos cargos y máximos responsables de las entidades incluidas en el ámbito de la aplicación de este título. Igualmente, se harán públicas las indemnizaciones percibidas, en su caso, con ocasión del abandono del cargo.

g) Las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos así como las que autoricen el ejercicio de actividad privada al cese de los altos cargos de la Administración General del Estado o asimilados según la normativa autonómica o local.

h) Las declaraciones anuales de bienes y actividades de los representantes locales, en los términos previstos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Cuando el reglamento no fije los términos en que han de hacerse públicas estas declaraciones se aplicará lo dispuesto en la normativa de conflictos de intereses en el ámbito de la Administración General del Estado. En todo caso, se omitirán los datos relativos a la localización concreta de los bienes inmuebles y se garantizará la privacidad y seguridad de sus titulares.

i) La información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos que sean de su competencia, en los términos que defina cada administración competente.

2. Los sujetos mencionados en el artículo 3 deberán publicar la información a la que se refieren las letras a) y b) del apartado primero de este artículo cuando se trate de contratos o convenios celebrados con una Administración Pública. Asimismo, habrán de publicar la información prevista en la letra c) en relación a las subvenciones que reciban cuando el órgano concedente sea una Administración Pública.

3. Las Administraciones Públicas publicarán la relación de los bienes inmuebles que sean de su propiedad o sobre los que ostenten algún derecho real.

Artículo 12. *Derecho de acceso a la información pública.*

Todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley.

Asimismo, y en el ámbito de sus respectivas competencias, será de aplicación la correspondiente normativa autonómica.

Artículo 13. *Información pública.*

Se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

Artículo 14. *Límites al derecho de acceso.*

1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para:

a) La seguridad nacional.

b) La defensa.

c) Las relaciones exteriores.

d) La seguridad pública.

e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios.

f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva.

g) Las funciones administrativas de vigilancia, inspección y control.

h) Los intereses económicos y comerciales.

i) La política económica y monetaria.

j) El secreto profesional y la propiedad intelectual e industrial.

k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión.

l) La protección del medio ambiente.

2. La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso.

3. Las resoluciones que de conformidad con lo previsto en la sección 2.ª se dicten en aplicación de este artículo serán objeto de publicidad previa disociación de los datos de carácter personal que contuvieran y sin perjuicio de lo dispuesto en el apartado 3 del artículo 20, una vez hayan sido notificadas a los interesados.

Artículo 15. *Protección de datos personales.*

1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.

2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.

3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.

Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios:

a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.

5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso.

Artículo 16. *Acceso parcial.*

En los casos en que la aplicación de alguno de los límites previstos en el artículo 14 no afecte a la totalidad de la información, se concederá el acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida.

Artículo 17. *Solicitud de acceso a la información.*

1. El procedimiento para el ejercicio del derecho de acceso se iniciará con la presentación de la correspondiente solicitud, que deberá dirigirse al titular del órgano administrativo o entidad que posea la información. Cuando se trate de información en posesión de personas físicas o jurídicas que presten servicios públicos o ejerzan potestades administrativas, la solicitud se dirigirá a la Administración, organismo o entidad de las previstas en el artículo 2.1 a las que se encuentren vinculadas.

2. La solicitud podrá presentarse por cualquier medio que permita tener constancia de:

a) La identidad del solicitante.

b) La información que se solicita.

c) Una dirección de contacto, preferentemente electrónica, a efectos de comunicaciones.

d) En su caso, la modalidad que se prefiera para acceder a la información solicitada.

3. El solicitante no está obligado a motivar su solicitud de acceso a la información. Sin embargo, podrá exponer los motivos por los que solicita la información y que podrán ser tenidos en cuenta cuando se dicte la resolución. No obstante, la ausencia de motivación no será por si sola causa de rechazo de la solicitud.

4. Los solicitantes de información podrán dirigirse a las Administraciones Públicas en cualquiera de las lenguas cooficiales del Estado en el territorio en el que radique la Administración en cuestión.

Acuerdo de 18 de noviembre de 2014, de la Comisión Permanente del Consejo General del Poder Judicial, por el que se aprueba el protocolo de integración en la organización interna del Consejo General del Poder Judicial de la gestión de solicitudes de información de los ciudadanos a que se refiere el artículo 21.1 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y se delegan competencias.

1.1.1. *Legitimación activa para el ejercicio del derecho de acceso.*

De conformidad con lo dispuesto en el artículo 12 de la Ley 19/2013, cualquier ciudadano, español o extranjero, persona jurídica privada o pública, es titular del derecho de acceso.

El CGPJ tramitará todas las solicitudes de información con independencia de los datos de identificación proporcionados[71].

Sólo cuando se requiera un acceso cualificado (por ejemplo, si se solicita el acceso presencial a una gran cantidad de documentación) se exigirá una identificación.

Cuando se proceda a tramitar un recurso por inadmisión *ad limine* de la solicitud de acceso o denegación del mismo, se exigirá su presentación por los cauces ordinarios.

Acuerdo de 27 de julio de 2016 del Pleno del Ayuntamiento de Madrid por el que se aprueba la Ordenanza de Transparencia de la Ciudad de Madrid

[71] El Consejo General del Poder Judicial, indica sobre este punto: "Aunque la Ley 19/2013 exige la identificación del solicitante, la falta de necesidad de identificación del solicitante es un estándar internacionalmente fijado, al entenderse que el acceso a la información pública es un derecho fundamental de carácter universal, en cuya garantía priman las obligaciones de transparencia de los poderes públicos frente a cualquier requisito impuesto al ciudadano que solicita el acceso."

Artículo 23. Acceso sin previa identificación del solicitante.

1. En aquellos supuestos en los que el solicitante de información pública no haga constar sus datos de identidad, solo podrá facilitársele aquella información que ya se halle publicada o aquella otra en la que concurran las siguientes circunstancias:

a) No resulte aplicable algún límite de los enumerados en el artículo 14 de la Ley 19/2013, de 9 de diciembre.

b) El acceso no afecte a la protección de datos personales en los términos de lo dispuesto en el artículo 15 de la Ley 19/2013, de 9 de diciembre.

c) No sea aplicable ninguna causa de inadmisión.

En el supuesto de que fuera aplicable alguno de los limites de los párrafos a) y b), alguna causa de inadmisión o algún régimen jurídico específico de acceso, el órgano competente para dar respuesta deberá comunicárselo al solicitante para que, en su caso, decida iniciar el procedimiento regulado en la Ley 19/2013, de 9 de diciembre, de conformidad con lo dispuesto en el articulo 24 de esta ordenanza. Los requisitos para formular esta solicitud serán los que se exigen en dichas normas.

2. Para poder garantizar, en su caso, el suministro de la información o la indicación del lugar en que esta se halla publicada, el solicitante deberá facilitar una dirección de correo electrónico.

3. Cuando la información solicitada esté en posesión de las personas mencionadas en el artículo 3.2, el requerimiento expresará el plazo para la remisión de la información, que no excederá de 15 días hábiles. El incumplimiento de dicho plazo podrá dar lugar a la imposición de las multas coercitivas reguladas en el artículo 48.

4. La respuesta a la solicitud de información por esta vía deberá emitirse en el plazo de un mes desde la fecha en que haya sido asignada su tramitación al órgano competente para resolver.

Si la información suministrada no publicada previamente, fuera relevante y su divulgación resultase de interés general, se publicará en el Portal de Gobierno Abierto, comunicándose al solicitante la localización precisa de la información.

5. El régimen de impugnaciones recogido en la Ley 19/2013, de 9 de diciembre, no será aplicable al acceso que se conceda o deniegue según lo dispuesto en este artículo.

6. La utilización previa de esta vía de acceso, no impedirá la presentación de una solicitud de acceso al amparo de lo dispuesto en la Ley 19/2013, de 9 de diciembre, y el artículo 24 de esta ordenanza, para el supuesto de que el solicitante considere insuficiente o inadecuada la respuesta dada por el órgano competente o quiera obtener una resolución administrativa con el contenido y garantías previstas en el articulo 24.

Ordenanza Tipo de Transparencia, Acceso a la Información y Reutilización, aprobada en Junta de Gobierno de la Federación Española de Municipios y Provincias, de 27-5-2014.

Artículo 26. *Solicitud.*

1. Los órganos competentes para resolver las solicitudes de acceso a la información pública no requerirán a los solicitantes más datos sobre su identidad que los imprescindibles para poder resolver y notificar aquéllas.

Asimismo, prestarán el apoyo y asesoramiento necesario al solicitante para la identificación de la información pública solicitada.

2. No será necesario motivar la solicitud de acceso a la información pública. No obstante, el interés o motivación expresada por el interesado podrá ser tenida en cuenta para ponderar, en su caso, el interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, de acuerdo con los establecido en el artículo 11.

3. La presentación de la solicitud no estará sujeta a plazo.

4. Se comunicará al solicitante el plazo máximo establecido para la resolución y notificación del procedimiento, así como del efecto que pueda producir el silencio administrativo en los términos previstos en la normativa sobre procedimiento administrativo.

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).

Artículo 5. *Principios relativos al tratamiento.*

1. Los datos personales serán

(…) c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); (…)

Considerando (39)

Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

Artículo 25. *Protección de datos desde el diseño y por defecto.*

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento

del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Considerando (78)

La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Disposición adicional octava. *Potestad de verificación de las Administraciones Públicas.*

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

Artículo 24. *Sistemas de información de denuncias internas.*

1. Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.

2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

4. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme al apartado 2 de este artículo, la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas.

5. Los principios de los apartados anteriores serán aplicables a los sistemas de denuncias internas que pudieran crearse en las Administraciones Públicas.

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

Artículo 8. Derechos básicos de los consumidores y usuarios.

Son derechos básicos de los consumidores y usuarios:

a) La protección contra los riesgos que puedan afectar su salud o seguridad.

b) La protección de sus legítimos intereses económicos y sociales; en particular frente a las prácticas comerciales desleales y la inclusión de cláusulas abusivas en los contratos.

c) La indemnización de los daños y la reparación de los perjuicios sufridos.

d) La información correcta sobre los diferentes bienes o servicios y la educación y divulgación para facilitar el conocimiento sobre su adecuado uso, consumo o disfrute.

e) La audiencia en consulta, la participación en el procedimiento de elaboración de las disposiciones generales que les afectan directamente y la representación de sus intereses, a través de las asociaciones, agrupaciones, federaciones o confederaciones de consumidores y usuarios legalmente constituidas.

f) La protección de sus derechos mediante procedimientos eficaces, en especial ante situaciones de inferioridad, subordinación e indefensión.

Proposición de Ley de Protección Integral de los Alertadores de Xnet

Primera transposición europea de la Directiva (UE) 2019/1937, de 23 de octubre de 2019, del Parlamento Europeo y del Consejo sobre la Protección de las Personas que informen sobre infracciones, registrada en el Congreso de los Diputados.

Véase: https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/

- **XNET**

ANEXO de

2 - DERECHO A GRABAR ABUSOS PARA SU DIFUSIÓN PÚBLICA Y POLÍTICAS DE PROTECCIÓN DE DATOS

ANÁLISIS DEL DESARROLLO LEGISLATIVO

Lo primero que hemos de observar respecto a la posibilidad de grabar y difundir conversaciones, imágenes y vídeos es la posible vulneración de derechos fundamentales al hacerlo.

El artículo 18 de la Constitución Española protege:

- *el derecho al honor, a la intimidad personal y familiar y a la propia imagen (Art.18.1 CE).*
- *el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial (Art. 18.3 CE).*
- *la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (Art. 18.4 CE).*

Los puntos 1 y 3 del artículo 18 se encuentran regulados en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, mientras que el 18.4 se regula específicamente en Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y anteriormente por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En la práctica existe jurisprudencia que reconoce que las grabaciones (si cumplen una serie de supuestos) son legales y que no suponen *per se* una vulneración del derecho al honor, a la intimidad personal y familiar y a la propia imagen (18.1) y el secreto de las comunicaciones (18.3). Sin embargo, no está tan claro respecto a la protección de datos de carácter personal (18.4).

La Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen establece en sus artículos 7 y 8 que grabar conversaciones o imágenes de personas en España puede llegar a suponer una intromisión ilegítima en el ámbito de intimidad y de la propia imagen, salvo que 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 o cuando la imagen de una persona determinada aparezca como meramente accesoria en el marco de una información gráfica sobre un suceso o acaecimiento público.

Así mismo, como se ha indicado anteriormente, la jurisprudencia ha ido clarificando que también es legal grabar cuando se cumplan los siguientes requisitos:

- Se trate de un cargo público o de un profesional de notoriedad o con proyección pública y la imagen se capte en un acto público o en lugares abiertos al público.
- La persona captada en la imagen lo sea de forma accesoria en el ámbito de una información gráfica sobre un acto público.
- Se tenga el consentimiento o quien lo grabe sea parte de la conversación, si bien como hemos visto podría cometerse una infracción en materia de protección de datos, por lo que la aplicación de las normativas de protección de datos es un obstáculo en el tema que aquí tratamos, causando inseguridad jurídica.
- Se realice para un fin legítimo que hasta ahora solo se considera para utilizarlo como prueba en un proceso judicial, denunciar un delito o en el ámbito de una relación negocial, no se contempla explícitamente denunciar un abuso, aunque quizás se debería justamente reinterpretar ese punto.

Apuntes sobre la necesidad de consentimiento

No siempre es necesario el consentimiento dentro del marco de la protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen. **La jurisprudencia dictamina que si la grabación la realiza una persona partícipe en la conversación** -aún sin consentimiento de la otra parte-, la grabación (tanto de las conversaciones como vídeo) **no vulnera el derecho a la intimidad y el secreto de las comunicaciones** (*Sentencia 114/1984 del Tribunal Constitucional; Sentencia del Tribunal Supremo de 20/11/2014; Sentencia del Tribunal Supremo de 7/02/2014; Auto de la Audiencia Provincial de Madrid de 28/04/2014).*

Sin embargo, y si bien mediante dicho tipo de grabación no se vulneraría el derecho a la intimidad, sigue existiendo inseguridad jurídica ya que sí podría vulnerarse la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, sobre todo en caso de difusión de las grabaciones. Esto es así porque la Agencia Española de Protección de Datos, AEPD,- en virtud de su competencia- ha venido desarrollando criterios (concretamente *el informe 0077/2013 sobre la antigua Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*) por los que dictamina que grabar imágenes o conversaciones de empleados públicos sin informar al interesado sobre la captación, en los términos del art. 4 de la Ley, y sin estar el tratamiento legitimado, bien por el consentimiento del interesado, bien por alguna de las causas previstas en el art. 6 de la Ley, supone una infracción de la misma, puesto que se considera tratamiento de datos personales. De hecho, en abril de 2018 impuso la primera sanción de 2000 euros a un particular que grabó imágenes de la actuación en la calle de un policía local y la difundió por WhatsApp (*RESOLUCIÓN R/00778/2018 de la AEPD*).

Apuntes sobre la difusión de grabaciones

En la mayoría de los casos no es legal la difusión de las grabaciones. La jurisprudencia se refiere claramente a que está permitido el hecho de grabar para dejar constancia de unos hechos cuando se pretenda la satisfacción de un interés legítimo, como el derecho a tutela judicial efectiva (derecho a la prueba, Art. 24, 2 CE), es decir, su uso como prueba en el ámbito judicial. La difusión está excluida de este supuesto para particulares.

En el caso de medios de comunicación, la jurisprudencia se ha mostrado tendencialmente favorable a la difusión de grabaciones. Sin embargo, por otra parte, independientemente de que la grabación sea lícita, la difusión (identificando a la persona), sí puede vulnerar los derechos del artículo 18 de la Constitución Española en determinados casos. En este sentido, hay jurisprudencia, citando por ejemplo la S*TS 225/2014, de 29 abril, y la STS 574/2017*, en un caso de la publicación de la grabación de una conversación en un medio de comunicación digital (relacionado con un caso de corrupción y blanqueo de capitales en Cataluña de la familia Pujol que está en los tribunales en este momento) dictaminando que se ha vulnerado el derecho a la intimidad y al honor (Art. 18 CE) considerando, en su fundamento de derecho segundo, apartados 6 y 7, que no era necesario publicar el "audio íntegro de la conversación, en la que afloran cuestiones ceñidas al ámbito propio y personal", cuestiones que carecían de interés general que sólo pudieron ser conocidas por el público a través de dicha difusión, que tenía el objetivo de satisfacer el "interés morboso del público por conocer el diálogo entre la actora (presidenta del Partido Popular de Catalunya) y la señora Irene". La sentencia concluye en este sentido que es por este "plus" de información que no era de interés general que declara que prevalece el derecho a la intimidad (Art. 18.1 CE) sobre el derecho de información (Art. 20 .1CE) ya que de haber sido publicados solamente las partes que contenían información relevante para el interés general seguramente hubiese dictaminado en sentido contrario.

Se trata de realizar, en estos casos, una ponderación sobre los derechos a la intimidad personal (art. 18.1 CE) y la libertad de información (art. 20.1 CE), ambos derechos fundamentales reconocidos en la Constitución e interpretados por el Tribunal Constitucional.

En este sentido, la Jurisprudencia de los Tribunales ha establecido que el derecho de información, siempre y cuando la información sea de interés general y realizando un ejercicio de ponderación de los derechos implicados, debe primar sobre el derecho a la

intimidad y a la protección de datos de las personas. Respecto a este principio general siempre se han de tener en cuenta las circunstancias concretas “ad hoc” que puedan establecerse para controlar excesos que puedan lesionar el derecho a la intimidad y a la imagen de las personas.

El Tribunal Constitucional, en relación concretamente con el derecho a la información, ha dicho que prevalece sobre los derechos del art. 18.1 de la CE, siempre y cuando se cumplan dos requisitos esenciales:

- Que la información sea veraz;
- Que tenga relevancia pública, es decir, que aporte información trascendente a la discusión democrática y social.

El requisito de la veracidad de la información exige que esta haya sido obtenida con el deber de diligencia exigible (esto es, contrastando la información con datos objetivos) y no fomentando rumores o insinuaciones injuriosas. En este sentido, resulta interesante destacar que el propio Tribunal Constitucional, en su Sentencia 15/1993, ha tenido oportunidad de aclarar que el requisito de la veracidad no requiere que las informaciones no puedan resultar finalmente erróneas o no probadas en juicio.

Por otra parte, el Tribunal Constitucional aclara que la información debe estar amparada "*en un interés público constitucionalmente relevante*", remitiéndose a su propia doctrina consolidada, en la que establece que un interés público constitucionalmente relevante concurre "*cuando la información que se comunica es relevante para la comunidad*". Estableciendo textualmente que: "*No cabe identificar indiscriminadamente interés público con interés del público, o de sectores del mismo ávidos de curiosidad”.*

El requisito de relevancia pública puede estar relacionada tanto con los hechos publicados como con la persona implicada en los mismos. Así, la ponderación de derechos debe considerar si la información tiene relevancia pública o interés general en cuanto puede contribuir al debate en una sociedad democrática pero también deberá considerar si se proyecta sobre personas que desempeñan un cargo público o tienen una personalidad política y ejercen funciones oficiales, lo cual es sustancialmente distinto de la simple satisfacción de la curiosidad humana por conocer la vida de otros, aunque se trate de personas con notoriedad pública que no ejerzan tales funciones.

La proyección pública de la persona a la que se refieran los actos o hechos comunicados depende, en parte, de las funciones que esta ejerza en la sociedad y del interés público que éstas tengan. Es el caso de quienes ejercen cargos políticos, pero también de quienes desempeñan funciones públicas (por ejemplo, agentes de la Guardia Civil, Comisarios de Policía, funcionarios de los cuerpos de seguridad, etc.). Aun así, debe tenerse en cuenta la jurisprudencia del Tribunal Constitucional (por ejemplo, las Sentencias 7/2014 y 172/1990) en las que decide que revelar datos no relacionados con los hechos o la profesión ejercida, relativos a la vida íntima de los implicados, no estaría cubierto por el derecho a la información.

Dicho esto, casi siempre el amparo se refiere al ámbito del periodismo, y la ciudadanía no se considera como un actor relevante en la tutela del interés general, cosa que criticamos.

A parte del mencionado artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, las únicas referencias a la libertad de información se encuentran en el artículo 20 de la CE, sobre los derechos de libertad de expresión y de información, y el RGPD (art. 85), si bien en este último caso son muy frágiles y no se han desarrollado en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de España.

Como comentado, afirmamos que actualmente la LOPDGDD es un grave obstáculo para sacar a la luz abusos.

Además, la difusión de las grabaciones en ciertos supuestos está sujeta a sanciones tanto por Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales como por el artículo 197 del Código Penal

relativo a la revelación de secretos. Así mismo, en el momento de la publicación inicial del presente informe, el artículo 36 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana consideraba como infracción grave y sancionable (…) "23. El uso no autorizado de imágenes o datos personales o profesionales de autoridades o miembros de las Fuerzas y Cuerpos de Seguridad que pueda poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, con respeto al derecho fundamental a la información". Esta infracción se ha visto afectada por la sentencia del Tribunal Constitucional que a día 19/11/2020, dando la razón al contenido de este informe, declara inconstitucional el inciso "no autorizado" del artículo 36.23 de la Ley de Seguridad Ciudadana que permitía sancionar el uso no autorizado de las imágenes de servidores públicos – policía en este caso -. (https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2020_108/NOTA%20INFORMATIVA%20N%C2%BA%20108-2020.pdf).

ANÁLISIS DE LA JURISPRUDENCIA Y RESOLUCIONES RELEVANTES.

DERECHO A LA INTIMIDAD (Art. 18.1 Constitución Española (CE))

Grabar conversaciones en la que uno es partícipe sin consentimiento es legal. No vulnera *per sé* el derecho a la intimidad. Dependerá del contexto y contenido de la grabación en cada caso, es decir, sí podría vulnerar el derecho a la intimidad si las conversaciones tratan sobre la vida personal o familiar.

Jurisprudencia:

STC 114/1984 del Tribunal Constitucional:

"Quien graba una conversación de otros atenta, independientemente de toda otra consideración, al derecho reconocido en el art. 18.3 CE. Por el contrario, quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado (18.1 CE)."

Tribunal Supremo, en Sentencias 883/1994, 178/1996, 914/1996, 702/1997 y 286/1998, así como Audiencia Provincial de Madrid, Auto de fecha 28 de abril del 2004:

"la grabación de una conversación que tiene lugar entre dos personas y que uno de los intervinientes desea conservar *para tener constancia fidedigna de lo tratado entre ambos,* ***no supone una invasión de la intimidad*** *o espacio reservado de la persona ya que el que resulta grabado ha accedido voluntariamente a tener ese contacto y es tributario y responsable de las expresiones utilizadas y del contenido de la conservación .....****Cuando una persona emite voluntariamente sus opiniones o secretos a un contertulio sabe de antemano que se despoja de sus intimidades y se las trasmite****, más o menos confiadamente, a los que les escuchan, los cuales podrán usar su contenido sin incurrir en ningún reproche jurídico."*

Sentencia del Tribunal Supremo STS 222/2015, 16 de abril de 2015:

En este caso fueron grabados y sorprendidos unos guardias civiles que, en su defensa, alegaron la vulneración de sus derechos a la intimidad, el honor y la propia imagen (art. 18.1 CE) a causa de que "*fueran grabados en el lugar de los hechos, que era un cuarto reservado para el cacheo de los equipajes de los viajeros, los actos cometidos por los recurrentes mediante cámaras ocultas y con deficiencias en su autorización judicial y posterior tratamiento*".

El Tribunal Supremo resuelve que "*el hecho de grabar las imágenes relativas a la actuación profesional de los Guardias en el lugar en la que la misma se llevaba a cabo, cuando había fundadas sospechas de su irregular proceder, en modo alguno puede suponer ilícita intromisión en su intimidad y, menos aún, al honor o la propia imagen*".

Sentencia del Tribunal Supremo de 20/11/2014: grabar una conversación un empleado y su jefe, hablando exclusivamente de temas laborales, no constituye ninguna intromisión ilegítima en el Derecho a la Intimidad personal (ni tampoco vulneración alguna del derecho al secreto de las comunicaciones).

Respecto al derecho a la propia imagen (fotografías de una policía en acto de servicio y su publicación por un periódico). *La Sentencia del Tribunal Constitucional 72/2007* dictamina que tampoco hay vulneración:

"No se discute (...) que la publicación de la imagen se produjo sin el consentimiento de la demandante. Estamos ante un documento que reproduce la imagen de una ***persona en el ejercicio de un cargo público*** *-la propia demandante de amparo admite expresamente que por su condición de Sargento de la policía municipal de Madrid desempeña un cargo público- y que la fotografía en cuestión fue captada con motivo de un* ***acto público*** *(un desalojo por orden judicial, que para ser llevado a cabo precisó del auxilio de los agentes de la policía municipal, ante la resistencia violenta de los afectados),* ***en un lugar público*** *(una calle de un*

barrio madrileño), por lo que en modo alguno resulta irrazonable concluir, como se razona en la Sentencia impugnada, que concurre el supuesto previsto en el art. 8.2 a) de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen".

Sentencia del Tribunal Supremo 621/2004, de 1 de julio (anterior a la aprobación de la Ley de Protección de la Seguridad Ciudadana):

Publicación en un diario de una fotografía de un Guardia Civil para ilustrar una noticia sobre la aprehensión de un alijo de hachís, apareciendo el Guardia Civil uniformado y acompañado del perro adiestrado que descubrió la droga. El agente demandó al periódico, argumentando que la publicación de la fotografía, en la que se veía su rostro era una intromisión ilegítima en su derecho a la protección de la propia imagen y que, además, en su caso las funciones profesionales que desempeñaba exigían su anonimato (es decir, la excepción del último párrafo del artículo 8.2 de la Ley 1/1982). El Tribunal Supremo desestimó su pretensión y concluyó que debía prevalecer el derecho a la libertad de información. En primer lugar, el Tribunal Supremo consideró que la noticia era de interés general, las informaciones eran veraces, los agentes tienen consideración de "cargo público" en el sentido del artículo 8.2 de la Ley 1/1982, por las funciones que desempeñan, y, finalmente, que la imagen había sido tomada mientras aquél ejercía sus funciones profesionales. En segundo lugar, concluyó el Tribunal Supremo que las funciones que desempeñaba el agente cuando fue tomada la foto no requerían anonimato y, en cualquier caso, éste no había puesto ningún medio para evitar ser reconocido.

STC 101/2003, de 2 de junio, del del Tribunal Constitucional: El cargo u ocupación de la persona afectada será un factor que analizar, teniendo en cuenta que los cargos públicos o las personas que por su profesión se ven expuestas al público tendrán que soportar un grado mayor de crítica o de afectación a su intimidad que las personas que no cuenten con esa exposición al público.

SECRETO DE LAS COMUNICACIONES (Art. 18.3 Constitución Española (CE))

Grabar conversaciones de terceros en la que no se participa sin consentimiento es ilegal y vulnera el secreto de las comunicaciones. Sólo puede realizarse por orden judicial o si se es un detective privado en el ejercicio de sus funciones.

Jurisprudencia:

STC 11/1984 del Tribunal Constitucional:

"Quien graba una conversación de otros atenta, independientemente de toda otra consideración, al derecho reconocido en el art. 18.3 CE. "

Tribunal Supremo en STC de 7 de febrero de 2014.

"Sea cual sea el ámbito objetivo del concepto de «comunicación», la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia erga omnes) ajenos a la comunicación misma. ***La presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación es indispensable para configurar el ilícito constitucional aquí perfilado****."*

PROTECCIÓN DE DATOS PERSONALES (Art. 18.4 Constitución Española (CE))

Aplicando de forma estricta la antigua Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) captar imágenes o conversaciones (así como su tratamiento y difusión) supone una infracción en materia de protección de datos. Aunque el Reglamento General de protección de Datos (UE) 2016/679 puede ofrecer alguna ventana de oportunidad, la nueva Ley Orgánica

3/2018 de 5 de Diciembre de Protección de Datos Personales y Garantía de los Derechos Digital no ha variado significativamente esta situación, así como las interpretaciones de la Agencia Española de Protección de Datos.

El Tribunal Constitucional ha interpretado que la protección de datos se trata de un derecho independiente, aunque obviamente estrechamente relacionado con la intimidad (*SSTC 254/1993, de 20 de julio y 290/2000, de 30 de noviembre*).

La STC 292/2000, establece que "***el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto***",

> "*la función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado … Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin*" (Fundamento jurídico 6).
>
> También el fundamento jurídico 7 declara que es complemento indispensable del derecho fundamental del art. 18.4 CE *"la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo".* Por consiguiente, el Pleno del Tribunal ha señalado como elemento caracterizador de la definición constitucional del art. 18.4 CE, de su núcleo esencial, el derecho del afectado a ser informado de quién posee los datos personales y con qué fin.

Respecto al desarrollo de jurisprudencia e interpretación legislativa por parte de la Agencia Española de Protección de Datos, hay dos aspectos principales a valorar: a) Interpretación de Ias obligaciones de información y consentimiento y b) Interpretación de la *Excepción doméstica.*

a) Interpretación de las obligaciones de información y consentimiento.

Sentencia del TC 29/2013 de 11 de febrero de 2013 de la Sala Primera dictamina que **la grabación de imágenes del trabajador sin su consentimiento y sin informarle de la finalidad y uso concreto** de las imágenes (control laboral y no exclusivamente seguridad y protección de las instalaciones) **vulnera el art. 18.4.**

Esta es la sentencia es precisamente la que sustenta el informe *0077/2013* de la AEPD sobre la **prohibición de grabar (y difundir) imágenes de empleados públicos** que establece que:

- todo tratamiento ha de cumplir los principios del art. 4 LOPD, y entre ellos que los datos sean "*adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido*". Por tanto, la finalidad de la captación ha de existir y ser legítima; si no existe tal finalidad, el tratamiento no puede llevarse a cabo;

- que en todo caso ha de informarse al interesado sobre la captación, en los términos del art. 5 LOPD, constituyendo tal deber de información contenido esencial del derecho fundamental;

- que el tratamiento ha de estar legitimado, bien por el consentimiento del interesado, bien por alguna de las causas previstas en el art. 6 LOPD.

No obstante, con posterioridad la *Sentencia del TC 39/2016,* de 3 de marzo de 2016, clarifica y establece que la instalación por una empresa en la entrada de uno de sus establecimientos del distintivo informativo de "Zona videovigilada" regulado por la antigua *Instrucción 1/2006 de la AEPD*, cumple con la obligación de informar al trabajador de la instalación de dichos sistemas y que **en *el ámbito laboral el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial*** *y , siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes.* (art. 6.2 LOPD y las facultades de control empresarial que reconoce el art. 20.3 del texto refundido de la Ley del Estatuto de los Trabajadores).

Si bien ambos casos son ligeramente diferentes en cuanto a la finalidad y uso de los datos (control de horarios en el primero y el control del patrimonio e instalaciones de la empresa en el segundo), en ambos casos la relación negocial (cumplimiento de contrato) se utiliza como alternativa al consentimiento del artículo 6 LOPD. **Lo relevante es que el consentimiento (que no la información sobre la recogida de datos) no es siempre absoluto.**

Por su parte, la Ley Orgánica 3/2018 de 5 de Diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales -aprobada recientemente para adaptar la normativa del Estado español al Reglamento General de Protección de Datos (UE) 2016/679-, en el Artículo 89, sobre Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, regula las condiciones bajo las que pueden realizarse estas grabaciones y concilia ambos casos:

> *1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.*
>
> *En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.*
>
> *2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.*
>
> *3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.*

Respecto a la grabación de funcionarios públicos por parte de particulares, como comentado, recientemente (abril 2018), la RESOLUCIÓN R/00778/2018 de la AEPD impone una sanción de 2.000 euros a un particular por grabar las actuaciones de la policía local en la vía pública, argumentando que la captación de imágenes de personas identificables sin esfuerzos desproporcionados y su posterior difusión a través de Whatsapp constituyen, de acuerdo con las definiciones contenidas en la antigua LOPD y su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada. Este hecho implica cumplir con los criterios arriba mencionados establecidos por el informe de 2013 de la AEPD, entre los cuales se encuentran el deber de informar de la captación de imágenes a los implicados en las mismas y la obtención del consentimiento si no puede legitimarse mediante otra base jurídica que lo permita.

Todo esto imposibilita *de facto* la revelación de abusos, siendo estas dos condiciones simplemente imposibles de obtener

justamente en estos casos.

La entrada en vigor del nuevo Reglamento General de Protección de Datos (UE) 2016/679 parece abrir una ventana de oportunidad al hacer constar las bases jurídicas concretas que pueden legitimar la captación y difusión de imágenes por parte de la ciudadanía cuando se cometan abusos, tales como la obligación legal, el interés público o el interés legítimo[72].

Asimismo, el artículo 85 del RGPD establece que cada Estado Miembro conciliará ***por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información***, ***incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria***, estableciendo *para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, (…) exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.*

Sin embargo, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en el Artículo 8 sobre "tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos" matiza algunas de las bases jurídicas que hubiesen podido ser utilizadas para legitimar dicho tratamiento, sin desarrollar su aplicación concreta, dejando dicho desarrollo para una ley posterior que deberá prever los casos en que puedan utilizarse y las condiciones de su utilización, provocando que dichas bases jurídicas sean inaplicables en la práctica.

La obligación de conciliar estos derechos fundamentales ya se estableció en la citada Sentencia Lindqvist en 2003 en la que el Tribunal de Justicia de La Unión Europea dispuso, concretamente en relación con las libertades de expresión e información, que:

> *"Por otro lado, resultan de la adopción, por parte de los Estados miembros, de disposiciones nacionales que garantizan la adaptación del Derecho interno a dicha Directiva y de la eventual aplicación de las citadas disposiciones por las autoridades nacionales.*
>
> *En consecuencia, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con la Directiva 95/46, sino también procurar que la interpretación de ésta que tomen como base no entre en conflicto con los derechos fundamentales tutelados por el ordenamiento jurídico comunitario o con los otros principios generales del Derecho comunitario como el principio de proporcionalidad.*
>
> *(…) Incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los derechos e intereses en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario."*

También una reciente **Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de febrero de 2019, Sergejs Buivids c. Datu valsts inspekcija**, **consideró que aún ser de aplicación la normativa de protección de datos a un particular** que publicó en Youtube un vídeo de la actuación policial, siguiendo la interpretación de la excepción doméstica que se detallará en el próximo subapartado, **debía tenerse en consideración la finalidad de dicha difusión que podía interpretarse como un tratamiento con fines exclusivamente periodísticos, estableciendo criterios y elementos para la armonización de la ponderación entre el derecho a la libertad de información y expresión con el derecho a la protección de datos personales,** bajo el paraguas del artículo 9 de la Directiva 95/46, sustituido actualmente por el artículo 85 del RGPD, y la interpretación de las actividades

[72] Por ejemplo, en la Resolución del expediente nº E/01849/2018 (https://www.aepd.es/es/documento/e-01849-2018.pdf), en un caso completamente distinto del mencionado, la AEPD admitió que aun ser de aplicación la normativa de protección de datos a una víctima de violencia de género que publicó información sobre su agresor en un grupo de Facebook, al considerar que dicha publicación se amparaba en su interés legítimo, motivo por el que se archivó la causa y no se la sancionó. A raíz de este hecho, pueden considerarse aplicables otras bases jurídicas distintas del consentimiento para legitimar el tratamiento de datos personales que se propone en el presente informe.

periodísticas establecidas en la Sentencia de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07:

> *"Se desprende de la jurisprudencia del Tribunal de Justicia que* ***las «actividades periodísticas» son las que tienen por finalidad divulgar al público información, opiniones o ideas, por cualquier medio de transmisión*** *(véase, en este sentido, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinaporssi y Satamedia, C-73/07, EU:C:2008:727, apartado 61).*
>
> *Aunque incumbe al tribunal remitente comprobar si, en el caso de autos, el tratamiento de datos personales que realizo el Sr. Buivids responde a esta finalidad, no es menos cierto que* ***el Tribunal de Justicia puede proporcionar a ese tribunal los elementos interpretativos necesarios para que lleve a cabo el examen que le corresponde****.*
>
> *De este modo, a la vista de la jurisprudencia del Tribunal de Justicia citada en los apartados 52 y 53 de la presente sentencia,* ***que el Sr. Buivids no sea periodista profesional no permite excluir que la grabación del video controvertido, así como su publicación en un sitio de Internet de videos en el que los usuarios pueden enviarlos, verlos y compartirlos, pueda acogerse a lo establecido en esa disposición.***
>
> *En particular, el hecho de que el Sr. Buivids haya publicado esa grabación en un sitio Internet de este tipo, en el caso de autos el sitio www.youtube.com,* ***no puede, en sí mismo, privar a dicho tratamiento de datos personales de la condición de haberse efectuado «exclusivamente con fines periodísticos»****, en el sentido del artículo 9 de la Directiva 95/46.*
>
> *En efecto, ha de tenerse en cuenta la evolución y la multiplicación de los medios de comunicación y de difusión de información. Así, el Tribunal de Justicia ya ha declarado que* ***el soporte en el que se transmiten los datos****, clásico como el papel o las ondas de radio, o electrónico como Internet,* ***no es determinante para apreciar si se trata de una actividad «con fines exclusivamente periodísticos»*** *(véase, en este sentido, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinaporssi y Satamedia, C-73/07, EU:C:2008:727, apartado 60).*
>
> *Dicho esto, como señaló en esencia la Abogado General en el punto 55 de sus conclusiones,* ***no puede considerarse que cualquier información publicada en Internet, relativa a datos personales, este comprendida en el concepto de «actividades periodísticas» y disfrute por ello de las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46.***
>
> *En el caso de autos,* ***el tribunal remitente debe comprobar si se desprende del video controvertido que su grabación y su publicación tenían como única finalidad la divulgación al público de información, opiniones o ideas*** *(véase, en este sentido, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinaporssi y Satamedia, C-73/07, EU:C:2008:727, apartado 62).*
>
> *Para ello, el tribunal remitente podrá tomar en consideración,* ***en particular, el hecho de que, según el Sr. Buivids, el video se publicara en un sitio de Internet para llamar la atención de la sociedad sobre las practicas supuestamente irregulares de la Policía que se desarrollaron en su toma de declaración****.*
>
> *Sin embargo, debe precisarse que la comprobación de tales prácticas irregulares no es un requisito para la aplicabilidad del artículo 9 de la Directiva 95/46.*
>
> *En cambio,* ***si resulta que la grabación y la publicación de este video no tenían como única finalidad la divulgación al público de información, opiniones o ideas, no podrá considerarse que el tratamiento de datos personales controvertido en el litigio principal se haya realizado «con fines exclusivamente periodísticos».***
>
> *Además, procede recordar que las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46 solo deben*

aplicarse en la medida en que resulten necesarias para conciliar dos derechos fundamentales, a saber, el derecho a intimidad y el derecho a la libertad de expresión (véase, en este sentido, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinaporssi y Satamedia, C-73/07, EU:C:2008:727, apartado 55).

(…) A este respecto, se desprende de dicha jurisprudencia que, ***para efectuar la ponderación entre el derecho al respeto de la intimidad y el derecho a la libertad de expresión, el Tribunal Europeo de Derechos Humanos ha desarrollado una serie de criterios pertinentes que deben tenerse en cuenta, concretamente la contribución a un debate de interés general, la notoriedad de la persona afectada, el objeto del reportaje, el comportamiento anterior del interesado, el contenido, la forma y las repercusiones de la publicación, la forma y las circunstancias en las que se obtuvo información y su veracidad*** *(véase, en este sentido, la sentencia del TEDH de 27 de junio de 2017, Satakunnan Markkinaporssi Oy y Satamedia Oy c. Finlandia, CE:ECHR:2017:0627JUD000093113, apartado 165).* ***Asimismo, deberá tomarse en consideración la posibilidad de que el responsable del tratamiento adopte medidas que permitan mitigar el alcance de la injerencia en el derecho a la intimidad.***

En el presente asunto, se desprende de los autos en poder del Tribunal de Justicia que no se puede excluir que la grabación y la publicación del video controvertido, que se efectuaron sin informar a los interesados de la realización de esa grabación y de su finalidad, constituya una injerencia en el derecho fundamental al respeto de la intimidad de estas personas, es decir, los policías que figuran en dicho video.

Si resulta que la grabación y la publicación del video controvertido tenían por única finalidad la divulgación al público de información, opiniones o ideas, corresponde al tribunal remitente apreciar si las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46 resultan necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión, y si tales exenciones y excepciones no exceden de lo estrictamente necesario.

Habida cuenta de las consideraciones anteriores, procede responder a la segunda cuestión prejudicial que el artículo 9 de la Directiva 95/46 debe interpretarse en el sentido de que ***hechos como los del litigio principal, a saber, la grabación en video de policías en una comisaría durante una toma de declaración y la publicación del video grabado en un sitio de Internet de videos en el que los usuarios pueden enviarlos, verlos y compartirlos, pueden constituir un tratamiento de datos personales con fines exclusivamente periodísticos, en el sentido de dicha disposición, siempre que se deduzca de dicho video que las citadas grabación y publicación tienen como única finalidad la divulgación al público de información, opiniones o ideas, lo que debe comprobar el tribunal remitente.****"*[73]

No obstante, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, no ha incluido ninguna disposición relativa a la conciliación del derecho a la libertad de expresión e información con el derecho a la protección de datos personales como **veremos** en el siguiente capítulo, no habiendo establecido ninguna exención o excepción respecto a las obligaciones en materia de protección de datos para proteger las libertades de expresión e información y dejando en manos de las Agencias y Autoridades de Protección de Datos y a los Tribunales la labor de interpretar los límites que deben constar en actos legislativos.

b) Interpretación de la excepción doméstica.

La "excepción doméstica" consiste en la excepción de aplicación de la normativa de protección de datos a los particulares que actúan fuera de su ámbito profesional y sin interés económico alguno. Se encontraba prevista en el artículo 2 de la de la antigua LOPD y actualmente la encontramos en el artículo 2.2.c) del RGPD y 2.2a) de la Ley Orgánica 3/2018 de Protección de Datos y

[73] *Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de febrero de 2019, Sergejs Buivids c. Datu valsts inspekcija, apartados 53 a 62 y 66 a 69. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0345*

garantía de los derechos digitales (LOPDGDD).

Aún existir esta excepción, debemos hacer constar que, siguiendo las interpretaciones hechas tanto por las autoridades de protección de datos europeas como por los tribunales, la casi totalidad de las actividades que supongan un "tratamiento de datos", incluso cuando son llevadas a cabo por particulares, están sujetas a la legislación de protección de datos si su publicación se realiza de forma que pueda alcanzar un número de personas que vaya más allá del ámbito doméstico. En este sentido encontramos la jurisprudencia que sigue:

> Sentencia Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, asunto C-101/01 Lindqvist, párrafos 46 y 47 (a los que se remite la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de diciembre de 2008, asunto C-73/07, Satamedia, párrafos 43 y 44):
>
> *"En cuanto a la excepción prevista en el segundo guion del artículo 3, apartado 2, de la Directiva 95/46, en el duodécimo considerando de esta última, relativo a dicha excepción,* ***se citan como ejemplos de tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas la correspondencia y la llevanza de un repertorio de direcciones.***
>
> ***En consecuencia, esta excepción debe interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es éste el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas.***
>
> Sentencia Audiencia Nacional, de 15 de junio de 2006:
>
> *"Lo relevante para la sujeción al régimen de protección de datos no será por tanto que haya existido tratamiento, sino si dicho tratamiento se ha desarrollado en un ámbito o finalidad que no sea exclusivamente personal o doméstico. Qué ha de entenderse por "personal" o "doméstico" no resulta tarea fácil.* (...) ***Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos****".*
>
> Dictamen 5/2009 relativo a las redes sociales en línea, del Grupo de Trabajo del Artículo 29, adoptado el 12 de junio de 2009.
>
> *" (...)The Directive does not impose the duties of a data controller on an individual who processes personal data "in the course of a purely personal or household activity" - the so-called "household exemption". In some instances, the activities of a user of an SNS may not be covered by the household exemption and the user might be considered to have taken on some of the responsibilities of a data controller. Some of these instances are developed below:*
>
> *(…)* ***If an SNS user acts on behalf of a company or association or uses the SNS mainly as a platform to advance commercial, political or charitable goals, the exception does not apply****. Here, the user assumes the full responsibilities of a data controller who is disclosing personal data to another data controller (SNS) and to third parties (other SNS users or potentially even other data controllers with access to the data). In these circumstances,* ***the user needs the consent of the persons concerned or some other legitimate basis provided in the Data Protection Directive.***
>
> *(…)* ***A high number of contacts could be an indication that the household exception does not apply and therefore that the user would be considered a data controller.***
>
> *(…)* ***even if the household exemption does not apply, the SNS user may benefit from other exemptions such as***

the exemption for journalistic purposes, artistic or literary expression. In those cases, a balance needs to be struck between freedom of expression and the right to privacy.*"*

Informe Jurídico 0077/2013 de la AEPD:

"(…) ***parece difícil entender que la captación de imágenes o videos por particulares de los empleados públicos sea realizada en el ámbito de la esfera íntima de aquellos particulares****, en las relaciones familiares o de amistad. Sólo el hecho de que las grabaciones sean realizadas en el ámbito laboral, en el lugar donde los empleados públicos prestan sus servicios, y sin relación alguna con ellos que exceda de la puramente profesional, parece llevarnos a la conclusión que en el supuesto planteado no es de aplicación la excepción doméstica. En definitiva, si las imágenes captadas o grabadas por particulares no se refieren a su esfera más íntima,* ***serán de aplicación las normas sobre protección de datos personales, tanto para la obtención de la imagen como para su difusión o publicación posterior, en tanto que ésta última constituye una cesión o comunicación de datos de carácter personal*** *tal y como viene definida por el artículo 3 j) de la LOPD, esto es, como "Toda revelación de datos realizada a una persona distinta del interesado"."*

"(…) para que nos hallemos ante la exclusión prevista en el artículo 2 LOPD, lo relevante es que se trate de una actividad propia de una relación personal o familiar, ***equiparable a la que podría realizarse sin la utilización de Internet****, por lo que no lo serán aquellos supuestos en que la publicación se efectúe en una página de libre acceso para cualquier persona o cuando el alto número de personas invitadas a contactar con dicha página resulte indicativo de que dicha actividad se extiende más allá de lo que es propio de dicho ámbito".*

Además, la citada RESOLUCIÓN R/00778/2018 de la AEPD, que impone sanción de 2.000 euros a un particular por grabar y difundir las actuaciones de la policía local, **considera que el mero hecho de compartir las imágenes por WhatsApp es sancionable** al haberse hecho accesibles a un número indeterminado de personas, sin entrar a analizar con quien se comparte ni con cuántos contactos.

En otras resoluciones referidas posteriores a la actividad en Internet de particulares encontramos criterios similares:

- La AEPD considera que "resulta plenamente aplicable la normativa de protección de datos" en el supuesto de la resolución por archivo de actuaciones del expediente nº: E/01849/2018[74] en que una víctima de violencia de género **publicó en un grupo privado de Facebook con más de 700 miembros** la sentencia que condenaba a su agresor, archivándose la causa por considerar la AEPD que concurría el interés legítimo de la víctima.

- La Audiencia Nacional, por su parte, **consideró adecuado el razonamiento de la AEPD que sancionó a un particular que publicó en su perfil de Facebook un video** de una vista de un juicio oral, considerándolo una falta continuada por no fue eliminado de dicho perfil[75].

- La AEPD, en la resolución del procedimiento sancionador PS/00292/2019[76] sancionó también a un particular que **incluyó el nombre, número y fotografía de otra persona en una web de contactos** cuyas condiciones de servicio establecían claramente que "EL ANUNCIANTE es responsable de todo lo que publica, de sus actos y de todo daño que pudiera ocasionar".

- Recientemente la AEPD consideró que la normativa resultaba de aplicación a un particular que **publicó en su estado de WhatsApp** fotografías íntimas y pantallazos de conversaciones privadas, aunque rebajó la sanción porque el contenido

[74] https://www.aepd.es/es/documento/e-01849-2018.pdf
[75] SAN, Sala de lo Contencioso, 2264/2018, de 11 de mayo de 2018.
[76] https://www.aepd.es/es/documento/ps-00292-2019.pdf

tubo un “alcance “meramente local”, sólo se afectó una persona y el infractor es una persona física.”[77]

El Dictamen del Grupo de Trabajo del Artículo 29 (GT29) no ha sido ratificado por el Comité Europeo de Protección de Datos (CEPD, *European Data Protection Board*) que lo sustituye, y, por lo tanto, dejó de tener aplicación en el momento en que quedó derogada la Directiva 95/46/EC. Este hecho, juntamente con **el Considerando 18 del Reglamento General de Protección de Datos que incluye entre las actividades personales y domésticas “la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades”,** podría contribuir al avance en este sentido y que las grabaciones a que se refiere este informe puedan ser publicadas por los usuarios, **debiendo distinguirse de las conductas que obran en interés público de aquellas que buscan socavar la reputación de terceras personas (lo cual, debemos recordar, se encuentra también protegido en el ámbito civil y penal, según los casos).**

[77] https://elpais.com/economia/2020/02/06/mis_derechos/1580977149_547064.html

LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

Constitución Española

Artículo 18 (1,3 y 4)

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Jurisprudencia orientativa sobre este artículo aquí

Artículo 20 (1.a y d)

1. Se reconocen y protegen los derechos:

a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.

d) A comunicar o recibir libremente información veraz por cualquier medio de difusión.

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen

Artículo 7.

Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:

1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.

3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.

4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.

5. 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, salvo los casos previstos en el artículo octavo, dos.

6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.

7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas.

Artículo 8.

Uno. No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley, ni cuando predomine un interés histórico, científico o cultural relevante.

Dos. En particular, el derecho a la propia imagen no impedirá:

a) 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**.

b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social.

c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.

Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza.

Código Penal. TÍTULO X Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

CAPÍTULO PRIMERO. ***Del descubrimiento y revelación de secretos***

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años

cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana

Artículo 36. *Se considera infracción grave:*

(..) 23. El uso no autorizado de imágenes o datos personales o profesionales de autoridades o miembros de las Fuerzas y Cuerpos de Seguridad que pueda poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, con respeto al derecho fundamental a la información.

Actualización a 20/11/2020: el 19/11/2020 el Tribunal Constitucional declara inconstitucional el inciso “no autorizado” del artículo 36.23 de la Ley de Seguridad Ciudadana (Ley Mordaza). Nota de prensa: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2020_108/NOTA%20INFORMATIVA%20N%C2%BA%20108-2020.pdf

Artículo 39. *Sanciones.*

1. Las infracciones muy graves se sancionarán con multa de 30.001 a 600.000 euros; las graves, con multa de 601 a 30.000 euros, y las leves, con multa de 100 a 600 euros.

Artículo 52. *Valor probatorio de las declaraciones de los agentes de la autoridad.*

En los procedimientos sancionadores que se instruyan en las materias objeto de esta Ley, las denuncias, atestados o actas formulados por los agentes de la autoridad en ejercicio de sus funciones que hubiesen presenciado los hechos, previa ratificación

en el caso de haber sido negados por los denunciados, constituirán base suficiente para adoptar la resolución que proceda, salvo prueba en contrario y sin perjuicio de que aquéllos deban aportar al expediente todos los elementos probatorios disponibles.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 77.5 "Los documentos formalizados por los funcionarios a los que se reconoce la condición de autoridad y en los que, observándose los requisitos legales correspondientes se recojan los hechos constatados por aquéllos harán prueba de éstos salvo que se acredite lo contrario.".

Reglamento Europeo de Protección de datos (UE) 2016/679

Artículo 2. ***Ámbito de aplicación material***

(…) 2. El presente Reglamento no se aplica al tratamiento de datos personales:

(…) c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

Considerando 18

El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

Artículo 6. ***Licitud del tratamiento***

1. El tratamiento solo será **lícito si se cumple al menos una** de las siguientes condiciones:

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.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades en el ejercicio de sus funciones.

Considerando 32

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Considerando 40

Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

Considerando 41

Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia») y del Tribunal Europeo de Derechos Humanos.

Considerando 42

Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo, debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

Considerando 43

Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el

consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento.

Considerando 45

Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

Considerando 47

El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

Artículo 23 *Limitaciones*

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

Artículo 85. ***Tratamiento y libertad de expresión y de información***

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

Ley Orgánica 3/2018 de Protección de Datos y garantía de los derechos digitales

Artículo 2. ***Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94***

(…) 2. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento General de Protección de Datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo. (...)

Artículo 6. ***Tratamiento basado en el consentimiento del afectado***

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

Artículo 8. ***Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos***

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

Artículo 8. ***Derechos básicos de los consumidores y usuarios.***

Son derechos básicos de los consumidores y usuarios:

a) La protección contra los riesgos que puedan afectar su salud o seguridad.

b) La protección de sus legítimos intereses económicos y sociales; en particular frente a las prácticas comerciales desleales y la inclusión de cláusulas abusivas en los contratos.

c) La indemnización de los daños y la reparación de los perjuicios sufridos.

d) La información correcta sobre los diferentes bienes o servicios y la educación y divulgación para facilitar el conocimiento sobre su adecuado uso, consumo o disfrute.

e) La audiencia en consulta, la participación en el procedimiento de elaboración de las disposiciones generales que les afectan directamente y la representación de sus intereses, a través de las asociaciones, agrupaciones, federaciones o confederaciones de consumidores y usuarios legalmente constituidas.

f) La protección de sus derechos mediante procedimientos eficaces, en especial ante situaciones de inferioridad, subordinación e indefensión.

Proposición de Ley de Protección Integral de los Alertadores de Xnet

Primera transposición europea de la Directiva (UE) 2019/1937, de 23 de octubre de 2019, del Parlamento Europeo y del Consejo sobre la Protección de las Personas que informen sobre infracciones, registrada en el Congreso de los Diputados.

Véase: https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/

ANEXO de

3 - LA MANCADA TRANSPOSICIÓN DEL ARTÍCULO 85 EN ESPAÑA – LA DESPROTECCIÓN DE LA LIBERTAD DE INFORMACIÓN EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

ANÁLISIS DEL DESARROLLO LEGISLATIVO

Tanto el derecho a la protección de datos personales como las libertades de expresión e información son derechos fundamentales autónomos reconocidos tanto a nivel internacional como nacional. Aun así, estas regulaciones permiten limitaciones a estos derechos. En concreto, se limitan entre sí ya que el ejercicio del derecho a la libertad de expresión puede verse limitado por afectar la vida privada de las personas y la vida privada de ciertas personas puede verse limitada y expuesta cuando se dan ciertas circunstancias.

Las organizaciones de la sociedad civil de toda la Unión Europea llevan mucho tiempo advirtiendo que las "flexibilidades" del Reglamento europeo 2016/679 General de Protección de Datos (en adelante, RGPD) que permiten distintas medidas de implementación en los Estados Miembros conducirán a diferencias en los niveles de protección aplicables en cada Estado. Por ejemplo, en Rumanía, la Association for Technology and Internet (ApTI) advierte que la nueva Ley de protección de datos proporciona menos protección que la ley anterior que implementó la Directiva 95/46/EC[78].

El RGPD incluye ciertas provisiones que permiten a los Estados Miembros un cierto margen de adaptación. Por ejemplo, la edad para prestar consentimiento (artículo 8)[79].

Del mismo modo, y siguiendo la tradición establecida por el TEDH[80], el RGPD dejó en manos de los Estados Miembros la tarea de establecer los límites entre el derecho a la protección de datos personales y las libertades de expresión e información, en concreto, en su artículo 85 y considerando 153, utilizando un lenguaje poco claro que no da indicaciones sobre cómo los estados deberían regular los límites entre las libertades de expresión e información y el derecho a la protección de datos personales.

> **Artículo 85. Tratamiento y libertad de expresión y de información.**
>
> "1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.
>
> 2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.
>
> 3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas."
>
> **Considerando (153)**
>
> "El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida

[78] Valentina Pavel, "European Commission urged to investigate Romanian GDPR implementation", GDPR Today, Edición n°3, Marzo 2019. https://www.gdprtoday.org/european-commission-urged-to-investigate-romanian-gdpr-implementation/

[79] Ingrida Milkaite y la Dra. Eva Lievens han realizado un mapeo para la Universidad de Ghent sobre las distintas edades para prestar consentimiento que se han previsto en los distintos Estados Miembros: https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751

[80] Sentencias Lindqvist y Satukunnan Markkinapörssi OY and Satamedia OY c. Finland. Establecen que la ponderación y limitación entre la libertad de expresión y el derecho a la vida privada debe realizarse por parte de las autoridades de los estados miembros, remitiéndose por ende a los jueces y tribunales.

> la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio. "

Los derechos fundamentales no son absolutos y para ejercerlos debe tenerse en cuenta el contexto en que se ejercen y la posible afectación de otros derechos, también fundamentales. En este sentido, Margaitis Schinas tras el escándalo protagonizado por la Autoridad de Protección de Datos de Rumanía, hizo las siguientes declaraciones como portavoz de la Comisión Europea[81]:

> "El derecho a la protección de datos personales no es un derecho absoluto. El artículo 85 del Reglamento General de Protección de Datos indica claramente que el derecho a la protección de datos debe equilibrarse con las libertades de expresión e información. Utilizar el Reglamento General de Protección de Datos contra estos dos otros derechos fundamentales sería un abuso claro de la regulación. Por lo tanto, es sumamente importante que las autoridades de Rumanía implementen esta obligación en el derecho nacional para proveer excepciones y derogaciones para proteger las fuentes periodísticas en particular de los poderes de la Autoridad de protección de datos cuando sea necesario para respetar la libertad de información y expresión de los medios."
>
> "La protección de datos no puede utilizarse como una puerta trasera para forzar a los periodistas a decir o hacer cosas que tienen derecho a no decir o no hacer bajo la libertad de expresión e información y protección de las fuentes".

La Ley Orgánica 3/2018 de Protección de Datos y garantía de los derechos digitales publicada en el BOE en diciembre de 2018, sólo menciona la libertad de expresión en el artículo 85 estableciendo que "Todos tienen derecho a la libertad de expresión en Internet", pero aún afirmar este derecho no incluye medidas para conciliarlo con el derecho a la protección de datos personales.

Con este gesto, el poder legislativo deja a merced de las Autoridades de Protección de Datos y de los jueces y tribunales este deber de conciliación, que deberá realizarse en cada caso concreto, como se ha hecho hasta ahora, impidiendo que los ciudadanos y profesionales conozcan de antemano si pueden o no difundir informaciones, es decir, impidiendo que puedan ejercer sus derechos con seguridad, sometiendo sus libertades a las voluntades del poder administrativo o judicial que determinaran *a posteriori* si se han vulnerado o no los derechos de terceros, arriesgándose por lo tanto a ser sancionados.

Las únicas previsiones de la Ley que comprenden alguna previsión que involucra ambos estos derechos son insuficientes e ineficaces en la práctica. Nos referimos en concreto a los artículos 85, 86, 93, 94 y 95 de la LOPDGDD, relativos al derecho de rectificación, al derecho de supresión u olvido y al derecho de portabilidad de datos.

[81] https://audiovisual.ec.europa.eu/en/video/I-163519

Especialmente, el artículo 85 de la LOPDGDD remite a la Ley Orgánica 2/1984, la cual establece un período de 7 días para ejercer el derecho de rectificación, lo que hace que el mismo sea ineficaz en la mayoría de los casos en que el usuario detecta información sobre si mismo en medios de comunicación digitales una vez ha expirado dicho plazo. No solo resulta ineficaz sino también innecesario, puesto que el ejercicio del derecho de rectificación previsto en el artículo 16 del RGPD y en el artículo 14 de la LOPDGDD procedería en todos los casos en los que la rectificación de la Ley Orgánica 2/1984 fuese posible, sin la limitación temporal que la misma establece.

Como dice Joaquín Urías, "por definición, todos los derechos subjetivos garantizados en la Constitución encajan como un puzle perfecto en el que ninguno anula otro y entre todos construyen la imagen perfecta de lo que es la libertad individual en nuestro Estado de derecho. La tarea del intérprete y el aplicador de la Constitución es definir con carácter general y el máximo detalle posible cada una de las piezas de ese puzle, permitiendo que quien ejerce la libertad de expresión sepa siempre cuándo estará protegido por la Constitución y cuando no."[82] Pero en el contexto jurídico actual es difícil saber cuándo una información puede ser publicada e incluso cuando pueden ser requeridas informaciones sobre las fuentes periodísticas".[83]

En otros países de la Unión Europea se han regulado mínimamente las condiciones en que la normativa de protección de datos deja de aplicarse o se aplica de forma limitada.

Aun así, la regulación por parte de los Estados Miembros, igual como en lo referido a las edades para prestar el consentimiento al tratamiento de datos personales, es dispar y no hay criterios fijos aplicables en todo el sí de la Unión Europea, los cuales debieron ser establecidos por el Reglamento Europeo, para asegurar un régimen uniforme aplicable a toda la Unión.

[82] Joaquín Urías, "Libertad de Expresión. Una Inmersión Rápida". Tibidabo Ediciones (2019). Pg. 54.

[83] Privacy International. "#TeleormanLeaks explained: privacy, freedom of expression, and public interest", 21 de noviembre de 2018. https://privacyinternational.org/blog/2456/teleormanleaks-explained-privacy-freedom-expression-and-public-interest

ANÁLISIS DE LA JURISPRUDENCIA RELEVANTE

Los conflictos entre la libertad de información y el derecho a la privacidad ya existían antes de Internet. La Jurisprudencia de los Tribunales estableció que el derecho de información, siempre y cuando tenga el carácter de interés general y realizando un ejercicio de ponderación de los derechos implicados, debe primar sobre el derecho a la intimidad de las personas, aunque deberán tenerse en cuenta las circunstancias concretas "ad hoc" que puedan establecerse para controlar excesos que puedan lesionar el derecho a la intimidad y a la imagen de las personas.

Concretamente, el Tribunal Europeo de Derechos Humanos ya estableció los criterios a tener en cuenta para equilibrarlos la libertad de información y el derecho a la privacidad cuando entran en conflicto:

- La persona o personas involucradas en la información: si se trata de personas actuando en un contexto público como políticos o figuras públicas o si bien se trata de individuales[84]
- El interés público de la información: debe valorarse en cada caso concreto por parte de las autoridades nacionales si los hechos objeto de la información pueden contribuir al debate en una sociedad democrática y son de interés público o si bien aún ser relativos a una figura pública son parte de su vida privada. Aun así, ha sido admitido que en algunas circunstancias el derecho a ser informado podrá extenderse a aspectos de la vida privada de las figuras públicas[85].
- La veracidad de la información: No se requiere que la información sea absolutamente veraz, sino que pueda verificarse su contenido y que el autor haya sido lo suficientemente diligente para comprobar la realidad del contenido.
- El contenido, la manera en que se obtiene la información y la forma y consecuencias de la difusión.
- La conducta del afectado antes de la publicación[86]: si el afectado hizo públicos los hechos no podrá quejarse

Estos criterios fueron señalados por la **Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de febrero de 2019,**

[84] STEDH Von Hannover v. Germany (no.2) [Grand Chamber], 2012. http://hudoc.echr.coe.int/eng?i=001-139414 : "§110. The role or function of the person concerned and the nature of the activities that are the subject of the report and/or photo constitute another important criterion, related to the preceding one. In that connection a distinction has to be made between private individuals and persons acting in a public context, as political figures or public figures. Accordingly, whilst a private individual unknown to the public may claim particular protection of his or her right to private life, the same is not true of public figures (see Minelli v. Switzerland (dec.), no. 14991/02, 14 June 2005, and Petrenco, cited above, § 55). A fundamental distinction needs to be made between reporting facts capable of contributing to a debate in a democratic society, relating to politicians in the exercise of their official functions for example, and reporting details of the private life of an individual who does not exercise such functions (see Von Hannover, cited above, § 63, and Standard Verlags GmbH, cited above, § 47).

While in the former case the press exercises its role of "public watchdog" in a democracy by imparting information and ideas on matters of public interest, that role appears less important in the latter case. Similarly, although in certain special circumstances the public's right to be informed can even extend to aspects of the private life of public figures, particularly where politicians are concerned, this will not be the case – despite the person concerned being well known to the public – where the published photos and accompanying commentaries relate exclusively to details of the person's private life and have the sole aim of satisfying public curiosity in that respect (see Von Hannover, cited above, § 65 with the references cited therein, and Standard Verlags GmbH, cited above, § 53; see also point 8 of the Resolution of the Parliamentary Assembly – paragraph 71 above). In the latter case, freedom of expression calls for a narrower interpretation (see Von Hannover, cited above, § 66; Hachette Filipacchi Associés (ICI PARIS), cited above, § 40; and MGN Limited, cited above, § 143)."

[85] STEDH Von Hannover v. Germany (no.2) [Grand Chamber], 2012. §110.

[86] STEDH Von Hannover v. Germany (no.2) [Grand Chamber], 2012: "§111. The conduct of the person concerned prior to publication of the report or the fact that the photo and the related information have already appeared in an earlier publication are also factors to be taken into consideration (see Hachette Filipacchi Associés (ICI PARIS), cited above, §§ 52-53, and Sapan, cited above, § 34). However, the mere fact of having cooperated with the press on previous occasions cannot serve as an argument for depriving the party concerned of all protection against publication of the photo at issue (see Egeland and Hanseid, cited above, § 62)."

Sergejs Buivids c. Datu valsts inspekcija, que **consideró que aún ser de aplicación la normativa de protección de datos a un particular** que publicó en Youtube un vídeo de la actuación policial, siguiendo la interpretación de la excepción doméstica establecida desde 2003 por el mismo tribunal[87], **debía tenerse en consideración la finalidad de dicha difusión que podía interpretarse como un tratamiento con fines exclusivamente periodísticos, estableciendo criterios y elementos para la armonización de la ponderación entre el derecho a la libertad de información y expresión con el derecho a la protección de datos personales,** bajo el paraguas del artículo 9 de la Directiva 95/46, sustituido actualmente por el artículo 85 del RGPD, y la interpretación de las actividades periodísticas establecidas en la Sentencia de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07. Aun así, recordó que corresponde a los tribunales nacionales comprobar en cada caso concreto si los criterios mencionados y la excepción periodística son de aplicación.

> *"Se desprende de la jurisprudencia del Tribunal de Justicia que **las «actividades periodísticas» son las que tienen por finalidad divulgar al público información, opiniones o ideas, por cualquier medio de transmisión** (véase, en este sentido, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinaporssi y Satamedia, C-73/07, EU:C:2008:727, apartado 61).*
>
> *Aunque incumbe al tribunal remitente comprobar si, en el caso de autos, el tratamiento de datos personales que realizo el Sr. Buivids responde a esta finalidad, no es menos cierto que **el Tribunal de Justicia puede proporcionar a ese tribunal los elementos interpretativos necesarios para que lleve a cabo el examen que le corresponde**.*
>
> *De este modo, a la vista de la jurisprudencia del Tribunal de Justicia citada en los apartados 52 y 53 de la presente sentencia, **que el Sr. Buivids no sea periodista profesional no permite excluir que la grabación del video controvertido, así como su publicación en un sitio de Internet de videos en el que los usuarios pueden enviarlos, verlos y compartirlos, pueda acogerse a lo establecido en esa disposición.***
>
> *En particular, el hecho de que el Sr. Buivids haya publicado esa grabación en un sitio Internet de este tipo, en el caso de autos el sitio www.youtube.com, **no puede, en sí mismo, privar a dicho tratamiento de datos personales de la condición de haberse efectuado «exclusivamente con fines periodísticos»**, en el sentido del artículo 9 de la Directiva 95/46.*
>
> *En efecto, ha de tenerse en cuenta la evolución y la multiplicación de los medios de comunicación y de difusión de información. Así, el Tribunal de Justicia ya ha declarado que **el soporte en el que se transmiten los datos**, clásico como el papel o las ondas de radio, o electrónico como Internet, **no es determinante para apreciar si se trata de una actividad «con fines exclusivamente periodísticos»** (véase, en este sentido, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinaporssi y Satamedia, C-73/07, EU:C:2008:727, apartado 60).*
>
> *Dicho esto, como señaló en esencia la Abogado General en el punto 55 de sus conclusiones, **no puede considerarse que cualquier información publicada en Internet, relativa a datos personales, este comprendida en el concepto de «actividades periodísticas» y disfrute por ello de las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46.***
>
> *En el caso de autos, **el tribunal remitente debe comprobar si se desprende del video controvertido que su grabación y su publicación tenían como única finalidad la divulgación al público de información, opiniones o ideas** (véase, en este sentido, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinaporssi y Satamedia, C-73/07, EU:C:2008:727, apartado 62).*
>
> *Para ello, el tribunal remitente podrá tomar en consideración, **en particular, el hecho de que, según el Sr. Buivids, el video se publicara en un sitio de Internet para llamar la atención de la sociedad sobre las practicas***

[87] Sentencia Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, asunto C-101/01 Lindqvist.

***supuestamente irregulares de la Policía que se desarrollaron en su toma de declaración**.*

Sin embargo, debe precisarse que la comprobación de tales prácticas irregulares no es un requisito para la aplicabilidad del artículo 9 de la Directiva 95/46.

*En cambio, **si resulta que la grabación y la publicación de este video no tenían como única finalidad la divulgación al público de información, opiniones o ideas, no podrá considerarse que el tratamiento de datos personales controvertido en el litigio principal se haya realizado ≪con fines exclusivamente periodísticos≫.***

Además, procede recordar que las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46 solo deben aplicarse en la medida en que resulten necesarias para conciliar dos derechos fundamentales, a saber, el derecho a intimidad y el derecho a la libertad de expresión (véase, en este sentido, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinaporssi y Satamedia, C-73/07, EU:C:2008:727, apartado 55).

*(…) A este respecto, se desprende de dicha jurisprudencia que, **para efectuar la ponderación entre el derecho al respeto de la intimidad y el derecho a la libertad de expresión, el Tribunal Europeo de Derechos Humanos ha desarrollado una serie de criterios pertinentes que deben tenerse en cuenta, concretamente la contribución a un debate de interés general, la notoriedad de la persona afectada, el objeto del reportaje, el comportamiento anterior del interesado, el contenido, la forma y las repercusiones de la publicación, la forma y las circunstancias en las que se obtuvo información y su veracidad** (véase, en este sentido, la sentencia del TEDH de 27 de junio de 2017, Satakunnan Markkinaporssi Oy y Satamedia Oy c. Finlandia, CE:ECHR:2017:0627JUD000093113, apartado 165). **Asimismo, deberá tomarse en consideración la posibilidad de que el responsable del tratamiento adopte medidas que permitan mitigar el alcance de la injerencia en el derecho a la intimidad.***

En el presente asunto, se desprende de los autos en poder del Tribunal de Justicia que no se puede excluir que la grabación y la publicación del video controvertido, que se efectuaron sin informar a los interesados de la realización de esa grabación y de su finalidad, constituya una injerencia en el derecho fundamental al respeto de la intimidad de estas personas, es decir, los policías que figuran en dicho video.

*Si resulta que la grabación y la publicación del video controvertido tenían por única finalidad la divulgación al público de información, opiniones o ideas, corresponde al tribunal remitente apreciar si las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46 resultan necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión, y si tales exenciones y excepciones no exceden de lo estrictamente necesario. Habida cuenta de las consideraciones anteriores, procede responder a la segunda cuestión prejudicial que el artículo 9 de la Directiva 95/46 debe interpretarse en el sentido de que **hechos como los del litigio principal, a saber, la grabación en video de policías en una comisaría durante una toma de declaración y la publicación del video grabado en un sitio de Internet de videos en el que los usuarios pueden enviarlos, verlos y compartirlos, pueden constituir un tratamiento de datos personales con fines exclusivamente periodísticos, en el sentido de dicha disposición, siempre que se deduzca de dicho video que las citadas grabación y publicación tienen como única finalidad la divulgación al público de información, opiniones o ideas, lo que debe comprobar el tribunal remitente.**"*[88]

En el ámbito nacional, el Tribunal Constitucional, en relación concretamente con el derecho a la información, ha dicho que prevalece sobre los derechos del art. 18.1 de la CE, siempre y cuando se cumplan dos requisitos esenciales:

- Que la información sea veraz;

[88] *Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de febrero de 2019, Sergejs Buivids c. Datu valsts inspekcija, apartados 53 a 62 y 66 a 69. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0345*

- Que tenga relevancia pública, es decir, que aporte información trascendente a la discusión democrática y social.

El requisito de la veracidad de la información exige que esta haya sido obtenida con el deber de diligencia exigible (esto es, contrastando la información con datos objetivos) y no fomentando rumores o insinuaciones injuriosas. En este sentido, resulta interesante destacar que el propio Tribunal Constitucional, en su Sentencia 15/1993, ha tenido oportunidad de aclarar que el requisito de la veracidad no requiere que las informaciones no puedan resultar finalmente erróneas o no probadas en juicio.

Por otra parte, el Tribunal Constitucional aclara que la información debe estar amparada "*en un interés público constitucionalmente relevante*", remitiéndose a su propia doctrina consolidada, en la que establece que un interés público constitucionalmente relevante concurre "*cuando la información que se comunica es relevante para la comunidad*". Estableciendo textualmente que: "*No cabe identificar indiscriminadamente interés público con interés del público, o de sectores del mismo ávidos de curiosidad".*

El requisito de relevancia pública puede estar relacionada tanto con los hechos publicados como con la persona implicada en los mismos. Así, la ponderación de derechos debe considerar si la información tiene relevancia pública o interés general en cuanto puede contribuir al debate en una sociedad democrática pero también deberá considerar si se proyecta sobre personas que desempeñan un cargo público o tienen una personalidad política y ejercen funciones oficiales, lo cual es sustancialmente distinto de la simple satisfacción de la curiosidad humana por conocer la vida de otros, aunque se trate de personas con notoriedad pública que no ejerzan tales funciones.

A parte del artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que limita la libertad de información atendiendo al derecho a la intimidad, las únicas referencias a la libertad de información se encuentran en el artículo 20 de la CE, sobre los derechos de libertad de expresión y de información, y el RGPD (artículo 85), si bien en este último caso son muy frágiles y **no se han desarrollado en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).**

Como comentado, la LOPDGDD no ha incluido ninguna disposición relativa a la conciliación (derogación o excepción a las disposiciones del RGPD) del derecho a la libertad de expresión e información con el derecho a la protección de datos personales, para proteger las libertades de expresión e información y ha dejado en manos de las Agencias y Autoridades de Protección de Datos y a los Tribunales la labor de interpretar los límites que deben constar en actos legislativos, como se había hecho hasta ahora desde la **Sentencia del Tribunal de Justicia de la Unión Europea Lindqvist**[89] en la que el Tribunal de Justicia de La Unión Europea dispuso, concretamente en relación con las libertades de expresión e información, que:

> *"Por otro lado, resultan de la adopción, por parte de los Estados miembros, de disposiciones nacionales que garantizan la adaptación del Derecho interno a dicha Directiva y de la eventual aplicación de las citadas disposiciones por las autoridades nacionales.*
>
> *En consecuencia, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con la Directiva 95/46, sino también procurar que la interpretación de ésta que tomen como base no entre en conflicto con los derechos fundamentales tutelados por el ordenamiento jurídico comunitario o con los otros principios generales del Derecho comunitario como el principio de proporcionalidad.*
>
> *(…) Incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los derechos e intereses en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario."*

Por lo tanto, consideramos que la LOPDGDD incumple las indicaciones del mismo artículo 85 del RGPD que establece que los Estados Miembros deben conciliar *por ley* el derecho a la protección de los datos personales en virtud del presente

[89] **Sentencia Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, asunto C-101/01 Lindqvist, párrafos 46 y 47.**

Reglamento con el derecho a la libertad de expresión y de información**, **incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria, estableciendo *para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, (…) exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.*

LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

Declaración Universal de Derechos Humanos, proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948

Artículo 12.

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Artículo 19.

Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

% **Pacto Internacional de Derechos Civiles y Políticos Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas en su resolución 2200 A (XXI), de 16 de diciembre de 1966.**

% **Artículo 17.**

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

% **Artículo 19.**

1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Roma, 4.XI.1950. Modificado

por los Protocolos nos. 11 y 14completado por el Protocolo adicional y los Protocolos nos. 4, 6, 7, 12, 13 y 16.

Artículo 8. *Derecho al respeto a la vida privada y familiar.*

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Artículo 10. *Libertad de expresión.*

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial.

Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01)

Artículo 7. *Respeto de la vida privada y familiar*

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8. *Protección de datos de carácter personal.*

1.Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2.Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legitimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3.El respeto de estas normas quedar sujeto al control de una autoridad independiente.

Artículo 11. *Libertad de expresión y de información.*

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

2. Se respetan la libertad de los medios de comunicación y su pluralismo.

Artículo 52. *Alcance de los derechos garantizados.*

1. Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta debe ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o la necesidad de protección de los derechos y libertades de los demás.

Constitución Española de 1978

Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Artículo 20.

1. Se reconocen y protegen los derechos:

a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.

b) A la producción y creación literaria, artística, científica y técnica.

c) A la libertad de cátedra.

d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.

3. La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España.

4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.

5. Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.

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)

Artículo 8. *Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.*

1.Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2.El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3.El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 58. *Poderes.*

1.Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

2.Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3.Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;

e) acreditar los organismos de certificación con arreglo al artículo 43;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

4.El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

5.Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

6.Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Considerando (129)

Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Dichos poderes deben incluir también el poder de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición. Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva. Esto no debe obstar a que se impongan requisitos adicionales con arreglo al Derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión.

Artículo 85. *Tratamiento y libertad de expresión y de información.*

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

Considerando (153)

El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al

presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio.

Considerando (4)

El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Sección 2.ª Potestades de investigación y planes de auditoría preventiva

Artículo 51. *Ámbito y personal competente.*

1. La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas.

2. La actividad de investigación se llevará a cabo por los funcionarios de la Agencia Española de Protección de Datos o por funcionarios ajenos a ella habilitados expresamente por su Presidencia.

3. En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia Española de Protección de Datos ejercerá sus facultades con arreglo a lo previsto en la presente ley orgánica y bajo la orientación y en presencia del personal de esta.

4. Los funcionarios que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio,

incluso después de haber cesado en él.

Artículo 52. *Deber de colaboración.*

1. Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.

Cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

2. En el marco de las actuaciones previas de investigación, cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, las informaciones y datos que resulten imprescindibles con la exclusiva finalidad de lograr la identificación de los responsables de las conductas que pudieran ser constitutivas de infracción del Reglamento (UE) 2016/679 y de la presente ley orgánica.

En el supuesto de las Administraciones tributarias y de la Seguridad Social, la información se limitará a la que resulte necesaria para poder identificar inequívocamente contra quién debe dirigirse la actuación de la Agencia Española de Protección de Datos en los supuestos de creación de entramados societarios que dificultasen el conocimiento directo del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica.

3. Cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información los datos que obren en su poder y que resulten imprescindibles para la identificación del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica cuando se hubiere llevado a cabo mediante la utilización de un servicio de la sociedad de la información o la realización de una comunicación electrónica. A tales efectos, los datos que la Agencia Española de Protección de Datos podrá recabar al amparo de este apartado son los siguientes:

a) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de telefonía fija o móvil:

1.º El número de teléfono de origen de la llamada en caso de que el mismo se hubiese ocultado.

2.º El nombre, número de documento identificativo y dirección del abonado o usuario registrado al que corresponda ese número de teléfono.

3.º La mera confirmación de que se ha realizado una llamada específica entre dos números en una determinada fecha y hora.

b) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de la sociedad de la información:

1.º La identificación de la dirección de protocolo de Internet desde la que se hubiera llevado a cabo la conducta y la fecha y hora de su realización.

2.º Si la conducta se hubiese llevado a cabo mediante correo electrónico, la identificación de la dirección de protocolo de Internet desde la que se creó la cuenta de correo y la fecha y hora en que la misma fue creada.

3.º El nombre, número de documento identificativo y dirección del abonado o del usuario registrado al que se le hubiera asignado la dirección de Protocolo de Internet a la que se refieren los dos párrafos anteriores.

Estos datos deberán ser cedidos, previo requerimiento motivado de la Agencia Española de Protección de Datos, exclusivamente

en el marco de actuaciones de investigación iniciadas como consecuencia de una denuncia presentada por un afectado respecto de una conducta de una persona jurídica o respecto a la utilización de sistemas que permitan la divulgación sin restricciones de datos personales. En el resto de los supuestos la cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales cuando resultara exigible.

Quedan excluidos de lo previsto en este apartado los datos de tráfico que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya cesión solamente podrá tener lugar de acuerdo con lo dispuesto en ella, previa autorización judicial solicitada por alguno de los agentes facultados a los que se refiere el artículo 6 de dicha ley.

Artículo 53. *Alcance de la actividad de investigación.*

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

2. Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio constitucionalmente protegido del inspeccionado, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial.

3. Cuando se trate de órganos judiciales u oficinas judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial.

Artículo 85. *Derecho de rectificación en Internet.*

1. Todos tienen derecho a la libertad de expresión en Internet.

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales.*

Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

Artículo 93. *Derecho al olvido en búsquedas de Internet.*

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.*

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.*

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Artículo séptimo.

Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:

1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.

3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.

4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.

5. 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, salvo los casos previstos en el artículo octavo, dos.

6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.

7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas.

Ley de Protección Integral de Alertadores de Xnet[90]

Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

[90] **h**ttps://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/

- **XNET**

ANEXO de

4 – ABUSOS EN EL ÁMBITO ELECTORAL: CÓMO HEMOS LLEGADO A QUE NOS PAREZCA NORMAL QUE LOS DATOS DEL PADRÓN MUNICIPAL ACABEN EN MANOS DE LOS PARTIDOS POLÍTICOS

ANÁLISIS DEL DESARROLLO LEGISLATIVO

Apuntes sobre los tratamientos llevados a cabo por parte de los Ayuntamientos

Multitud de tratamientos son realizados por los Ayuntamientos tras la inscripción al Padrón municipal. En este informe nos concentraremos en los tratamientos relacionados con las distintas transmisiones de datos del flujo de datos mencionado, analizando los datos que son recogidos y comunicados, la base jurídica que los legitima, su finalidad y la información que se proporciona, o no, a los interesados.

a. Recogida de los datos: Inscripción al Padrón Municipal de habitantes

La inscripción al padrón municipal de habitantes es una obligación que debe cumplir "toda persona que viva en España" y que se encuentra establecida en el **artículo 15 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local** (en adelante, LRBRL):

> *"Toda persona que viva en España está obligada a inscribirse en el Padrón del municipio en el que resida habitualmente.*
> *Quien viva en varios municipios deberá inscribirse únicamente en el que habite durante más tiempo al año.*
> *El conjunto de personas inscritas en el Padrón municipal constituye la población del municipio.*
> *Los inscritos en el Padrón municipal son los vecinos del municipio.*
> *La condición de vecino se adquiere en el mismo momento de su inscripción en el Padrón."*

Vemos, por lo tanto, que **la Ley impone la obligación a la población de inscribirse al padrón**, el cumplimiento de obligaciones legales constituyendo una base jurídica legitimadora del tratamiento de acuerdo con el Reglamento (UE) 2016/679 General de Protección de Datos (en adelante, RGPD) y la Ley Orgánica 3/2018 de Protección de Datos y garantía de los derechos digitales (en adelante, LOPDGDD).
Aun así, la LRBRL obliga a las personas y no a las instituciones, por lo tanto, **la recogida de los datos para la inscripción del padrón se fundamentaría en el ejercicio de poderes públicos del Ayuntamiento**, previsto también tanto en el RGPD como en la LOPDGDD:

Artículo 6.1.c) RGPD: *"el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento."*

Artículo 8.1 LOPDGDD: *"El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679."*

Artículo 6.1.e) RGPD: *"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."*

Artículo 8.2 LOPDGDD: *"El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley."*

Los datos recogidos para realizar la inscripción en el Padrón se encuentran enumerados en el artículo 16.2 de la LRBRL según el cual es obligatorio solicitar ciertos datos, además de lo que *"puedan ser necesarios para la elaboración del Censo Electoral*", **dejando que sea otra norma la que establezca cuales son necesarios para la elaboración del censo**.

"La inscripción en el Padrón municipal contendrá como obligatorios sólo los siguientes datos:
a) Nombre y apellidos.
b) Sexo.
c) Domicilio habitual.
d) Nacionalidad.
e) Lugar y fecha de nacimiento.
f) Número de documento nacional de identidad o, tratándose de extranjeros:

• Número de la tarjeta de residencia en vigor, expedida por las autoridades españolas, o en su defecto, número del documento acreditativo de la identidad o del pasaporte en vigor expedido por las autoridades del país de procedencia, tratándose de ciudadanos nacionales de Estados Miembros de la Unión Europea, de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo o de Estados a los que, en virtud de un convenio internacional se extienda el régimen jurídico previsto para los ciudadanos de los Estados mencionados.

• Número de identificación de extranjero que conste en documento, en vigor, expedido por las autoridades españolas o, en su defecto, por no ser titulares de éstos, el número del pasaporte en vigor expedido por las autoridades del país de procedencia, tratándose de ciudadanos nacionales de Estados no comprendidos en el inciso anterior de este párrafo,

salvo que, por virtud de Tratado o Acuerdo Internacional, disfruten de un régimen específico de exención de visado en materia de pequeño tráfico fronterizo con el municipio en el que se pretenda el empadronamiento, en cuyo caso, se exigirá el correspondiente visado.
g) Certificado o título escolar o académico que se posea.
h) Cuantos otros datos puedan ser necesarios para la elaboración del Censo Electoral, siempre que se garantice el respeto a los derechos fundamentales reconocidos en la Constitución."

La finalidad del tratamiento también se encuentra establecida en el artículo 16.1 de la LRBRL, sirviendo como prueba de la residencia en el municipio.

"El Padrón municipal es el registro administrativo donde constan los vecinos de un municipio. Sus datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo. Las certificaciones que de dichos datos se expidan tendrán carácter de documento público y fehaciente para todos los efectos administrativos.
La inscripción en el Padrón Municipal sólo surtirá efecto de conformidad con lo dispuesto en el artículo 15 de esta ley por el tiempo que subsista el hecho que la motivó y, en todo caso, deberá ser objeto de renovación periódica cada dos años cuando se trate de la inscripción de extranjeros no comunitarios sin autorización de residencia permanente. […]"

Sobre la información que debe proporcionarse a los interesados, es importante tener en cuenta el **principio de transparencia establecido en el artículo 5 del RGPD**, referido, en gran parte, a la información de qué deben disponer los interesados cuando sus datos personales van a ser objeto de tratamiento, para que puedan controlar los usos que se hacen de estos datos y quién tiene acceso a los mismos, o en otras palabras, a quién pueden ser comunicados. Este principio se ha visto reforzado con la entrada en vigor del RGPD, que ha incrementado las obligaciones informativas de los responsables y en consecuencia el derecho de información de los interesados. El **artículo 12 y los considerandos 39 y 58 del RGPD** concretan este principio y establecen que esta información debe permitir que el interesado sepa y comprenda cual es la finalidad del tratamiento y los datos que se recogen, detalles que en este caso se encuentran establecidos en la Ley, además de informar sobre la identidad del responsable. La información debe ser gratuita, clara, transparente, accesible y fácil de entender, utilizando un lenguaje sencillo, pudiendo utilizar incluso iconos.

Artículo 12. *Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.*
"1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.
(…) 5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito.
(…) 7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. (…)"

Considerando (39) *"Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar*

totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.
Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento."

Considerando (58) *"El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender."*

Los artículos 13 y 14 del RGPD y el artículo 11 de la LOPDGDD establecen la información concreta que debe proporcionarse a los interesados según si el responsable del tratamiento, en este caso el Ayuntamiento, recoge los datos directamente de los interesados o por el contrario son recogidos de otras fuentes. En este caso, **el Ayuntamiento recoge directamente de los interesados los datos, por lo tanto, son aplicables los artículos 13 del RGPD y 11.1 y 2 de la LOPDGDD**.

Artículo 13. *Información que deberá facilitarse cuando los datos personales se obtengan del interesado.*
1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la

existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:
a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

La única excepción existente para no tener que proporcionar dicha información es que el interesado ya disponga de ella. **Como podrá observarse, el resto de entidades entre las que se comparte la información del Padrón, el Ayuntamiento y el Registro Civil son los únicos que deben informar a los interesados ya que otras excepciones son aplicables en su caso. Así es necesario incidir en la obligación de los Ayuntamientos de informar de los destinatarios de los datos o categorías de destinatarios de los datos.**

Por su parte, **el artículo 11 de la LOPDGDD reduce considerablemente la información que debe proporcionarse en un primer momento al interesado**, en la cual no incluye los posibles destinatarios de los datos:

Artículo 11. *Transparencia e información al afectado.*
1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al

deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:
a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

Así, los interesados sólo podrán saber quienes son los posibles destinatarios de los datos cuando soliciten mayor información sobre el tratamiento de sus datos o cuando consulten el Registro de Actividades del Tratamiento dónde también deben preverse *"las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales"* **(artículo 30.1.d) del RGPD)**, que de acuerdo con el artículo **31.2 de la LOPDGDD** debe hacerse público por parte de las entidades previstas en el artículo **77.1** de la misma, entre las cuales se encuentran las *"entidades que integran la Administración Local"*. Concretamente, el Registro de Actividades del Tratamiento debe publicarse en la sede de transparencia de la entidad, de acuerdo con la **Disposición Final 11ª de la LOPDGDD**.

El artículo 16.3 de la LRBRL menciona que los datos del Padrón se comunicarán a otras Administraciones públicas que lo soliciten sin consentimiento del afectado cuando sean necesarios para el ejercicio de sus respectivas competencias.

"3. Los datos del Padrón Municipal se cederán a otras Administraciones públicas que lo soliciten sin consentimiento previo al afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y en las leyes de estadística de las comunidades autónomas con competencia en la materia."

Vemos que la práctica más común cuando se informa a los interesados para indicar cuáles son los destinatarios de los datos es hacer mención a categorías genéricas como "otras Administraciones Públicas" o mencionar solamente los destinatarios, sin mencionar la base jurídica concreta que legitima la comunicación de datos, es decir, la ley que la establece, ni la finalidad concreta del tratamiento. Creemos que debería rectificarse urgentemente esta práctica para que los interesados puedan saber en todo momento cual es el destino de sus datos personales, por quién serán utilizados y puedan oponerse a ello.

b. Comunicación de los datos: al Instituto Nacional de Estadística. Actualización de los datos del Padrón Municipal de Habitantes.

La comunicación de los datos recogidos por los Ayuntamientos para la inscripción al Padrón municipal de habitantes al Instituto Nacional de Estadística se encuentra prevista en el artículo 17.3 de la LRBRL:

> *"Los Ayuntamientos remitirán al Instituto Nacional de Estadística los datos de sus respectivos Padrones, en la forma que reglamentariamente se determine por la Administración General del Estado, a fin de que pueda llevarse a cabo la coordinación entre los Padrones de todos los municipios.*
> *El Instituto Nacional de Estadística, en aras a subsanar posibles errores y evitar duplicidades, realizará las comprobaciones oportunas, y comunicará a los Ayuntamientos las actuaciones y operaciones necesarias para que los datos padronales puedan servir de base para la elaboración de estadísticas de población a nivel nacional, para que las cifras resultantes de las revisiones anuales puedan ser declaradas oficiales, y para que los Ayuntamientos puedan remitir, debidamente actualizados, los datos del Censo Electoral.*
> *Corresponderá al Presidente del Instituto Nacional de Estadística la resolución de las discrepancias que, en materia de empadronamiento, surjan entre los Ayuntamientos, Diputaciones Provinciales, Cabildos y Consejos insulares o entre estos entes y el Instituto Nacional de Estadística, así como elevar al Gobierno de la Nación la propuesta de cifras oficiales de población de los municipios españoles, comunicándolo en los términos que reglamentariamente se determinan al Ayuntamiento interesado.*
> *El Instituto Nacional de Estadística remitirá trimestralmente a los Institutos estadísticos de las comunidades autónomas u órganos competentes en la materia, y en su caso, a otras Administraciones públicas los datos relativos a los padrones en los municipios de su ámbito territorial en los que se produzcan altas o bajas de extranjeros en las mismas condiciones señaladas en el artículo 16.3 de esta ley."*

El artículo entonces supone la base jurídica para la comunicación de los datos de los Ayuntamientos al Instituto Nacional de Estadística (en adelante, INE), ya que es obligación de los Ayuntamientos remitir esta información de acuerdo con el mismo. Así el tratamiento se encuentra legitimado por el cumplimiento de una obligación legal aplicable al responsable del tratamiento **(artículo 6.1.c) del RGPD y 8.1 de la LOPDGDD)**.

Como menciona el artículo, la finalidad es la de elaborar estadísticas de población a nivel nacional y actualizar los datos que serán finalmente enviados por los Ayuntamientos a la Oficina del Censo Electoral. El INE por lo tanto recoge los datos de todos los Ayuntamientos para cruzarlos y ver si hay diferencias entre ellos. Por ejemplo, si alguien empadronado en el municipio X se encuentra empadronado más tarde en el municipio Y, cuando el INE remita de nuevo los datos a los Ayuntamientos, el municipio X deberá modificar los datos que tiene sobre la persona que está empadronada en otro municipio. **La obligación de actualizar los datos del Padrón Municipal de Habitantes por parte de los Ayuntamientos se encuentra prevista en el artículo 17.1 y 2 de la LRBRL:**

> *"1. La formación, mantenimiento, revisión y custodia del Padrón municipal corresponde al Ayuntamiento, de acuerdo con lo que establezca la legislación del Estado.*
> *Con este fin, los distintos organismos de la Administración General del Estado, competentes por razón de la materia, remitirán periódicamente a cada Ayuntamiento información sobre las variaciones de los datos de sus vecinos que con carácter obligatorio deben figurar en el Padrón municipal, en la forma que se establezca reglamentariamente.*
> *La gestión del Padrón municipal se llevará por los Ayuntamientos con medios informáticos. Las Diputaciones Provinciales, Cabildos y Consejos insulares asumirán la gestión informatizada de los Padrones de los municipios que, por su insuficiente capacidad económica y de gestión, no puedan mantener los datos de forma automatizada.*

2. Los Ayuntamientos realizarán las actuaciones y operaciones necesarias para mantener actualizados sus Padrones de modo que los datos contenidos en éstos concuerden con la realidad.
Si un ayuntamiento no llevara a cabo dichas actuaciones, el Instituto Nacional de Estadística, previo informe del Consejo de Empadronamiento, podrá requerirle previamente concretando la inactividad, y si fuere rechazado, sin perjuicio de los recursos jurisdiccionales que procedan, podrá acudir a la ejecución sustitutoria prevista en el artículo 60 de la presente ley."

La cuestión que debe tratase aquí es si el INE debe informar a los interesados sobre la comunicación de los datos por parte de los Ayuntamientos y el tratamiento que lleva a cabo. **El artículo 14 del RGPD y el artículo 11.3 de la LOPDGDD recogen la obligación de informar en caso de no recoger los datos directamente del interesado**, añadiendo que debe informarse de la fuente de los datos y las categorías de datos que se tratan.

Pero el artículo 14.5 del RGPD establece excepciones a la aplicación de este deber, entre las cuales se encuentra la prevista en la **letra c)**:

"5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que: (…)
c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, (…)"

Por lo tanto, el INE no debe informar individualmente a los interesados porque la comunicación de los datos se encuentra establecida por el Derecho del Estado Español y si no lo ha advertido el Ayuntamiento al momento de recoger la información, este es un tratamiento que la ciudadanía no conoce al momento de proporcionar sus datos personales y sobre el que no goza de control alguno.

Podría discutirse que el INE debe informar a los interesados del tratamiento de sus datos por tratarlos para finalidades distintas de las indicadas o previstas en el momento de la recogida por el Ayuntamiento de acuerdo con **el artículo 13.3 del RGPD que establece que el responsable del tratamiento deberá facilitar al interesado, antes de realizar el tratamiento con finalidades distintas de las de la recogida, la información sobre estas finalidades**:

"3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2."

En efecto, **el artículo 6.4 y el considerando 50 del RGPD establecen que sólo podrán tratarse los datos para fines distintos de los de la recogida cuando el tratamiento posterior de los mismos sea compatible con los fines de su recogida inicial**, teniendo en cuenta el contexto de recogida de los datos y la naturaleza de los mismos, la relación del interesado con el responsable del tratamiento y las expectativas razonables del interesado respecto al tratamiento de sus datos.

Artículo 6. *Licitud del tratamiento.*
"4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en

el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización."

Considerando (50) *"El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si 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, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. (…)"*

Apuntes sobre los tratamientos llevados a cabo por parte de la Oficina del Censo Electoral

Para los tratamientos de datos personales que hacen referencia a la Ley Orgánica del Régimen Electoral General (en adelante, LOREG) deberá tenerse en cuenta todo lo previsto en la misma porque el artículo 2.3 de la LOPDGDD establece que su aplicación en este caso sólo será supletoria:

Artículo 2. *Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.*
"(…) 3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles."

Esta regulación no solo se refiere a la contenida en la LOREG sino también a la multitud de disposiciones reglamentarias sobre el censo electoral a las que esta se remite.

a. Comunicación de los datos: Inscripción al Censo Electoral y comunicación recibida de Ayuntamientos y Registros Civiles

El **artículo 32 de la LOREG establece que la inscripción en el censo electoral es obligatoria y que son los Ayuntamientos quienes tramitan de oficio la inscripción en el mismo** de quienes residen en su término municipal.

> *"1. La inscripción en el censo electoral es obligatoria. Además del nombre y los apellidos, único dato necesario para la identificación del elector en el acto de la votación, sin perjuicio de lo dispuesto en el artículo 85, se incluirá entre los restantes datos censales el número del Documento Nacional de Identidad.*
> *2. Los Ayuntamientos tramitan de oficio la inscripción de los residentes en su término municipal."*

Según este mismo artículo **los únicos datos que son necesarios para la elaboración del censo son el nombre, apellidos y DNI**, y para acreditar la identidad el día de la votación deberá hacerse mediante el DNI o en su defecto el pasaporte o permiso de conducir o tarjeta de residencia en el caso de extranjeros (**artículo 85 de la LOREG**). Estos datos se encuentran detallados en el **artículo 2.1 del Real Decreto 157/1996, de 2 de febrero, por el que se dispone la actualización mensual del censo electoral y se regulan los datos necesarios para la inscripción en el mismo**.

> **Artículo 2**. *Datos necesarios para la inscripción en el censo electoral.*
> *"1. La inscripción en el censo electoral contendrá los siguientes datos:*
> *Nombre y apellidos.*
> *Residencia: provincia y municipio.*
> *Domicilio.*
> *Sexo.*
> *Lugar de nacimiento: provincia y municipio.*
> *Fecha de nacimiento: día, mes y año.*
> *Grado de escolaridad: certificado de escolaridad o titulación académica.*
> *Número del documento nacional de identidad. […]"*

> **Artículo 3**: *Información del Registro Civil.*
> *"Los encargados del Registro Civil comunicarán mensualmente a las delegaciones provinciales de la Oficina del Censo Electoral cualquier circunstancia que pueda afectar a las inscripciones en el censo electoral, en particular por:*
> *a) Defunción o declaración de fallecimiento.*
> *b) Adquisición, recuperación o pérdida de la nacionalidad española.*
> *c) Cambio de nombre o de apellidos.*
> *d) Cambio de sexo.*
> *e) Declaración de modificación judicial de la capacidad en la que se prive expresamente a la persona con capacidad modificada judicialmente del derecho de sufragio activo."*

Por lo tanto, puede observarse que los datos que contiene el censo son similares a los previstos por el artículo 16.2 de la LRBRL y

el legislador no ha hecho uso de la habilitación prevista por el mismo.

La finalidad del tratamiento por parte de la Oficina del Censo Electoral es la de gestionar las personas físicas que tienen reconocido su derecho al sufragio activo y se encuentra determinada por el **artículo 31.1. de la LOREG**:

> *"1. El censo electoral contiene la inscripción de quienes reúnen los requisitos para ser elector y no se hallen privados, definitiva o temporalmente, del derecho de sufragio."*

Para la cuestión relativa a la información de los interesados, la LOREG no establece nada al efecto y por lo tanto, la Oficina del Censo Electoral debería seguir las normas previstas tanto por el RGPD como por la LOPDGDD. En este punto vemos que los datos no son obtenidos por la Oficina del Censo directamente del interesado y por lo tanto es de aplicación el artículo 14 del RGPD y la misma excepción aplicable en el caso del INE. En consecuencia, la Oficina del Censo Electoral no debe informar a los electores sobre el tratamiento de sus datos aunque esta afirmación podría discutirse al ser tratados los datos con finalidades distintas de las de su recogida.

b. Actualización de los datos del Censo Electoral

En lo que respecta a la actualización de los datos, que también debería llevarse a cabo de acuerdo con los principios previstos en el artículo 5 del RGPD, la LOREG establece una regulación específica en sus artículos 34 y siguientes:

> **Artículo treinta y cuatro**. *Carácter y vigencia del censo electoral.*
> El censo electoral es permanente y su actualización es mensual, con referencia al día primero de cada mes.
>
> **Artículo treinta y cinco**. *Actualización del Censo Electoral*.
> 1. Para la actualización mensual del censo los Ayuntamientos enviarán a las Delegaciones Provinciales de la Oficina del Censo Electoral, hasta el penúltimo día hábil de cada mes, y en la forma prevista por las instrucciones de dicho organismo, todas las modificaciones del Padrón producidas en dicho mes.
> 2. Si algún Ayuntamiento no cumpliera con la obligación establecida en el párrafo anterior, el Director de la Oficina del Censo dará cuenta de ello a la Junta Electoral Central para que por la misma se adopten las medidas procedentes.
> 3. En la actualización correspondiente al primer mes del año se acompañarán, además, las altas, con la calificación de menor, de los residentes que cumplirán dieciocho años entre el 1 de enero y el 31 de diciembre del año siguiente.

Además, existe una regulación específica de la actualización de los datos del censo por medio del Real Decreto 157/1996, de 2 de febrero, antes mencionado, la Orden EHA/642/2011, de 25 de marzo, del Ministerio de Economía y Hacienda, por la que se dictan normas técnicas para la actualización mensual del Censo Electoral[91] y la Resolución de 19 de julio de 1996, de la Dirección de la Oficina del Censo Electoral, por la que se aprueban los modelos referidos en la Orden de 24 de abril de 1996 por la que se dictan normas técnicas para la actualización del censo electoral[92].

[91] https://www.boe.es/boe/dias/2011/03/26/pdfs/BOE-A-2011-5462.pdf

[92] http://www.juntaelectoralcentral.es/cs/jec/documentos/RES_1996_0_1.pdf

Artículo 1: *Procedimiento para la actualización mensual del censo electoral.*
"1. La Oficina del Censo Electoral procederá a realizar la actualización del censo electoral con referencia al día primero de cada mes, conforme establece el artículo 34 de la Ley Orgánica del Régimen Electoral General.
2. A tal fin, los ayuntamientos remitirán mensualmente a las delegaciones provinciales de la Oficina del Censo Electoral la información de las altas, bajas y modificaciones de los datos de los residentes en sus respectivos términos municipales, conforme establece el artículo 35 de la Ley Orgánica del Régimen Electoral General. […]"

Artículo 3: *Información del Registro Civil.*
"Los encargados del Registro Civil comunicarán mensualmente a las delegaciones provinciales de la Oficina del Censo Electoral cualquier circunstancia que pueda afectar a las inscripciones en el censo electoral, en particular por:
a) Defunción o declaración de fallecimiento.
b) Adquisición, recuperación o pérdida de la nacionalidad española.
c) Cambio de nombre o de apellidos.
d) Cambio de sexo.
e) Declaración de modificación judicial de la capacidad en la que se prive expresamente a la persona con capacidad modificada judicialmente del derecho de sufragio activo."

b. Comunicación de los datos: Distribución de Copias del Censo a los partidos políticos y tratamiento por parte de los partidos.

Cuando el Tribunal Constitucional declaró inconstitucional[93] el apartado 1 del artículo 58bis de la LOREG, incorporado por la Disposición final tercera, apartado dos de la LOPDGDD, y durante los meses precedentes a la sentencia, se discutió ampliamente sobre la facultad de los partidos políticos de recoger datos de los electores de sus perfiles de redes sociales u otras fuentes, pero no se discutió tanto sobre la comunicación de datos a los partidos políticos de los datos incluidos en el censo y de las consecuencias que esta comunicación puede tener sobre los electores.

Esta comunicación de datos se encuentra prevista en el artículo 41.5 de la LOREG que establece que los representantes de cada candidatura podrán obtener una copia del censo en formato informático.

"5. Los representantes de cada candidatura podrán obtener dentro de los dos días siguientes a la proclamación de su candidatura una copia del censo del distrito correspondiente, ordenado por mesas, en soporte apto para su tratamiento informático, que podrá ser utilizado exclusivamente para los fines previstos en la presente Ley. Alternativamente los representantes generales podrán obtener en las mismas condiciones una copia del censo vigente de los distritos donde su partido, federación o coalición presente candidaturas. Asimismo, las Juntas Electorales de Zona dispondrán de una copia del censo electoral utilizable, correspondiente a su ámbito.
Las Juntas Electorales, mediante resolución motivada, podrán suspender cautelarmente la entrega de las copias del censo a los representantes antes citados cuando la proclamación de sus candidaturas haya sido objeto de recurso o cuando se considere que podrían estar incursas en alguna de las circunstancias previstas en el artículo 44.4 de esta Ley."

El primer apartado del artículo 41 de la LOREG habilita a que se regule mediante Real Decreto el contenido de las listas electorales

[93] STC 76/2019, de 22 de mayo de 2019.
https://www.boe.es/boe/dias/2019/06/25/pdfs/BOE-A-2019-9548.pdf

y de las copias del censo, lo cual se hizo mediante el Real Decreto 1799/2003, de 26 de diciembre, por el que se regula el contenido de las listas electorales y de las copias del censo electoral, cuyo artículo 5 contiene los plazos en que se entregarán a las candidaturas las copias y los datos que las mismas contendrán:

> **Artículo 5**. *Copias del censo electoral.*
> *"1. Las copias del censo electoral que se faciliten en virtud de lo dispuesto en el artículo 41, apartados 4 y 5, de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, contendrán a los electores ordenados de igual forma que en las listas de votación, con las exclusiones que correspondan por la aplicación del artículo 6 de este real decreto.*
>
> *2. Las entregas a los representantes de las candidaturas de las copias del censo de residentes en España se realizarán entre los días vigésimo octavo y vigésimo noveno posteriores a la convocatoria y las del censo de electores residentes-ausentes que viven en el extranjero, entre los días trigésimo quinto y trigésimo sexto después de la convocatoria, con la información de las solicitudes de voto disponible hasta el trigésimo cuarto día posterior a la convocatoria.*
>
> *3. Los datos de cada elector serán los siguientes:*
> *3.1 Electores residentes en España (españoles y nacionales de otros Estados con derecho de voto en España).*
> *a) Número de orden.*
> *b) Apellidos y nombre.*
> *c) Provincia y municipio de residencia.*
> *d) Distrito, sección y mesa electoral.*
> *e) Domicilio.*
> *f) Fecha de nacimiento: día, mes y año.*
> *g) País de nacionalidad, para los electores nacionales de otros Estados.*
> *3.2 Electores residentes-ausentes que viven en el extranjero:*
> *a) Número de orden.*
> *b) Indicador de haber solicitado el voto.*
> *c) Apellidos y nombre.*
> *d) Provincia y municipio de inscripción a efectos electorales.*
> *e) Domicilio.*
> *f) País de residencia.*
> *g) Fecha de nacimiento: día, mes y año. (…)"*

Además, encontramos la Orden de 3 de febrero de 1987 por la que se regula la distribución de copias del Censo Electoral en soporte magnético y la expedición de certificados de inscripción en el Censo Electoral, y la Instrucción 4/2009, de 17 de diciembre, de la Junta Electoral Central, sobre actuaciones de la Oficina del Censo Electoral en relación a la entrega de copias del censo electoral a las candidaturas y al envío de la documentación para ejercer el voto por correo donde se establece el plazo para solicitar las copias del censo en su primer punto:

> *"**1. Plazo para que los representantes de las candidaturas puedan solicitar las copias del censo electoral**.*
> *El plazo normal para que los representantes de las candidaturas puedan solicitar las copias del censo electoral a que tienen derecho en aplicación de lo dispuesto en el artículo 41.5 de la LOREG es el que establece el artículo 4.º de la Orden de 3 de febrero de 1987, del Ministerio de Economía y Hacienda, por la que se regula la distribución de copias del censo electoral en soporte magnético y la expedición de certificados de inscripción en el censo electoral; es decir, el plazo*

> *que media entre el día de la designación de representante y el de la proclamación de candidatos, quedando condicionada la solicitud de copias a la confirmación de la referida proclamación.*
> *En tanto permanezca vigente la referida Orden Ministerial de 3 de febrero de 1987 es preciso hacer una interpretación de dicha previsión reglamentaria a la luz del derecho fundamental a la participación política reconocido en el artículo 23 de la Constitución, lo que lleva a entender que las solicitudes presentadas tras la finalización de ese plazo puedan, excepcionalmente, ser atendidas por la Oficina del Censo Electoral, previa autorización expresa de la Junta Electoral Provincial competente, siempre que, en el momento de la solicitud, la entrega de la copia del censo pudiera todavía servir para el cumplimiento de los fines previstos legalmente."*

Sin embargo, ni la base jurídica que legitima el tratamiento, ni la finalidad de esta comunicación de datos no se establece en ninguno de los tres textos mencionados, ni tampoco se establece obligación, por parte de los partidos políticos de informar a los electores sobre el tratamiento de sus datos. Entendemos, por lo tanto, que es de aplicación la LOPDGDD en lo no previsto por la LOREG, al ser aplicable supletoriamente.

Sobre la base jurídica del tratamiento, el artículo 41 de la LOREG establece que los partidos políticos podrán obtener una copia del censo, lo que constituye una posibilidad y no una obligación legal (artículo 6.1.c del RGPD y 8.1 de la LOPDGDD). Tampoco es aplicable la base jurídica del consentimiento (artículo 6.1.a del RGPD) porque, como se verá más adelante, la ciudadanía tiene el derecho de oponerse a que su nombre se incluya en la lista pero no deben consentir a ello. La comunicación de datos por parte de la Oficina del Censo goza de base jurídica del tratamiento al tratarse de una competencia atribuida por una norma con rango de ley, pero **no goza de base jurídica el tratamiento por parte de los partidos políticos, salvo considerar que se encuentra legitimado por el interés legítimo de los mismos** (artículo 6.1.f) del RGPD).

El artículo 5 del RGPD establece el principio de *"limitación de la finalidad"* según el cual los datos personales serán *"recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines"*.

Para modificar la LOREG para que no establezca dicha comunicación de datos podemos además apoyarnos en el principio de minimización de datos establecido por el artículo 5.1.c) del RGPD y el principio de privacidad desde el diseño y por defecto del artículo 25 del RGPD.

Para más complejidad – e incumplimientos – debe incidirse en el hecho de que **los partidos, una vez disponen de los datos del censo deben cumplir con ciertas medidas previstas por la normativa que desarrolla la LOREG**. Una de estas medidas, de acuerdo con la Orden de 3 de febrero de 1987 por la que se regula la distribución de copias del Censo Electoral en soporte magnético y la expedición de certificados de inscripción en el Censo Electoral, es la prohibición de facilitar cualquier tipo de información particularizada sobre datos personales incluidos en el censo, conforme el artículo 41.2 de la LOREG.

También se prevé, en la Instrucción 4/2009 antes mencionado un compromiso de utilización de las copias del censo y la **obligación de inmediata eliminación de las mismas tras la conclusión del proceso electoral**:

> *"3. Compromiso de utilización de las copias del censo electoral y exención de la obligación de devolución de éstas.*
> *El artículo 41.5 de la LOREG señala que las copias del censo electoral que pueden obtener los representantes de las*

> *candidaturas deben facilitarse en soporte apto para su tratamiento informático, añadiendo que dichas copias sólo podrán ser utilizadas exclusivamente para los fines previstos en la citada ley. […]*
>
> *A la vista de las consideraciones anteriores, esta Junta Electoral Central ha decidido modificar su anterior doctrina, eliminando el deber de devolución de los soportes entregados a las candidaturas. A cambio, se estima necesario reforzar el compromiso de los representantes de las candidaturas de no conservación de la información total o parcial relativa a las copias del censo electoral.*
> *En conclusión, debe entenderse suprimida la obligación de los representantes de las candidaturas de devolver las copias del censo electoral entregadas, si bien, en el momento de su recepción los responsables de la candidatura habrán de firmar una declaración en la que asumirán el compromiso de no utilizar las copias del censo electoral para fines no previstos en la LOREG, y la obligación de inmediata eliminación de dicha información tras la conclusión del proceso electoral."*

Esta eliminación sin embargo, choca con lo previsto en la Orden de 3 de febrero de 1987, también mencionada anteriormente, la cual en su punto segundo, en el apartado segundo dispone lo siguiente:

> *"2. En el caso de que, dentro del período anual de revisión del Censo Electoral, se convoquen varios procesos electorales aquellos partidos, federaciones o coaliciones que hayan obtenido ya copia del Censo Electoral en soporte magnético, no podrán volver a solicitar nueva copia, salvo que se justifique el deterioro de la copia anterior."*

Consideramos que estas medidas no son suficientes teniendo en cuenta la voluntad tanto del RGPD como de la LOPDGDD de mejorar la protección de los datos personales de la ciudadanía y abogamos por lo tanto por la modificación de la LOREG en los términos mencionados.

Apuntes sobre el ejercicio de derechos por parte de la ciudadanía

Deben diferenciarse dos momentos de ejercicio de los derechos en el régimen establecido por la LOREG y su normativa de desarrollo:

> **a. Derechos que pueden ejercerse en cualquier momento**

El **derecho de acceso** es el derecho que tiene cada elector de solicitar un certificado personal de inscripción en el Censo Electoral, ya sea para conocer los datos personales que figuren en el mismo o por otros motivos particulares. Este derecho se encuentra previsto en distintos artículos de la LOREG:

> • El **artículo 38.1 de la LOREG** prevé que *"Con los datos consignados en los artículos anteriores, las Delegaciones Provinciales de la Oficina del Censo Electoral mantendrán a disposición de los interesados el censo actualizado para su consulta permanente, que podrá realizarse a través de los Ayuntamientos, Consulados o en la propia Delegación Provincial."*

• El **artículo 41 de la LOREG** regula, como se ha observado, el acceso al censo por parte de los partidos políticos, entre otros.

• Los **artículos 72 y 73 de la LOREG** regulan la emisión de certificados de inscripción en el censo para el voto por correo, su contenido desarrollándose por los Reales Decretos 1732/1985 y 1733/1985, ambos del 24 de septiembre.

La Orden de 3 de febrero de 1987 por la que se regula la distribución de copias del Censo Electoral en soporte magnético y la expedición de certificados de inscripción en el Censo Electoral, prevé específicamente el modo de solicitud del acceso por parte de los electores a los datos que constan en el Censo electoral, concretamente para solicitar la certificación de inscripción en el Censo Electoral:

> Octavo.
> "1. El elector que solicite certificación de inscripción en el Censo Electoral, deberá hacer constar en la solicitud los datos indicados en el punto 7.o 1 de esta Orden (además del nombre y apellidos de ésta, la fecha y el lugar de nacimiento (municipio y provincia) y la residencia de dicha persona en la fecha de referencia del Censo Electoral vigente, con expresión de la vía urbana y número, así como el municipio y la provincia en que estaba inscrito en el Padrón Municipal de Habitantes como residente).
>
> 2. La solicitud deberá hacerse personalmente en la Delegación de la Oficina del Censo Electoral correspondiente a la provincia a la que pertenece el municipio en el que se encuentra inscrito en el Censo Electoral.
> Se exigirá, junto con la solicitud, la presentación del documento nacional de identidad, pasaporte o permiso de conducir, para comprobación de los datos del elector.
>
> 3. En caso de enfermedad o incapacidad que impida la formulación personal de la solicitud, ésta podrá ser efectuada en nombre del elector, por persona debidamente autorizada, acreditando ésta su identidad y representación con documento autenticado por Notario o para los españoles residentes en el extranjero autenticado por el Cónsul."
>
> Noveno.
> "En el caso de que la certificación se solicite para acreditar la cualidad de elector de un candidato o interventor, la solicitud podrá ser formulada por el representante del partido, federación, coalición o agrupación, designado de acuerdo con el artículo 43 de la Ley 5/1985, debiendo aportar documento sobre conformidad del elector para su presentación como candidato o interventor y haciendo constar en la misma los datos indicados en el punto 7.o, 1 de esta Orden."

La Instrucción de 20 de enero de 2004, de la Junta Electoral Central, sobre consulta vía Internet de los datos del censo electoral, en este sentido prevé que *"Los Ayuntamientos que faciliten a los electores a través de Internet el acceso a sus datos censales deberán incluir a tal fin los mismos datos de cada elector que figuren en las listas en soporte papel."*

También encontramos la Instrucción 7/2007, de 12 de abril, de la Junta Electoral Central, sobre la certificación censal específica prevista en el artículo 85.1 de la LOREG.

Otro **derecho** que puede ejercerse en cualquier momento es el **de rectificación**, previsto por el **artículo 38.2 y 3 de la LOREG**, como el derecho a reclamar sobre los datos censales, y:

> *"2. Las reclamaciones sobre los datos censales se dirigirán a las Delegaciones Provinciales de la Oficina del Censo Electoral, que resolverán en el plazo de cinco días a contar desde la recepción de aquéllas.*
> *Los Ayuntamientos y Consulados remitirán inmediatamente las reclamaciones que reciban a las respectivas Delegaciones Provinciales de la Oficina del Censo Electoral.*
> *Los representantes de las candidaturas o representantes de los partidos, federaciones y coaliciones podrán impugnar el censo de las circunscripciones que hubieren registrado un incremento de residentes significativo y no justificado que haya dado lugar a la comunicación a que se refiere el artículo 30.c), dentro del plazo de cinco días siguientes al momento en que tuvieren conocimiento de la referida comunicación.*
>
> *3. La Oficina del Censo Electoral adoptará las medidas oportunas para facilitar la tramitación por los Ayuntamientos y Consulados de las consultas y reclamaciones. […]"*

b. Derechos cuyo ejercicio se limita al período electoral

Hay especificaciones para el ejercicio del **derecho de acceso** en período electoral previstas en el **artículo 39 de la LOREG**:

> *"2. Los ayuntamientos y consulados estarán obligados a mantener un servicio de consulta de las listas electorales vigentes de sus respectivos municipios y demarcaciones durante el plazo de ocho días, a partir del sexto día posterior a la convocatoria de elecciones.*
> *La consulta podrá realizarse por medios informáticos, previa identificación del interesado, o mediante la exposición al público de las listas electorales, si no se cuenta con medios informáticos suficientes para ello.*
>
> *(…) 7. La Oficina del Censo Electoral remitirá a todos los electores una tarjeta censal con los datos actualizados de su inscripción en el censo electoral y de la Sección y Mesa en la que le corresponde votar, y comunicará igualmente a los electores afectados las modificaciones de Secciones, locales o Mesas, a que se refiere el artículo 24 de la presente Ley Orgánica."*

El **derecho de reclamación en período electoral incluye no sólo el derecho de rectificación y el derecho de oposición a ser incluido en las copias del censo remitidas a los partidos** y también está previsto en el artículo 39 de la LOREG:

> *"3.Dentro del plazo anterior[94], cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección*

[94] *Artículo 39.2 de la LOREG: "ocho días, a partir del sexto día posterior a la convocatoria de elecciones".*

correspondiente a su domicilio anterior.[…]
5. Las reclamaciones podrán presentarse directamente en las delegaciones provinciales de la Oficina del Censo Electoral correspondiente o a través de los ayuntamientos o consulados, quienes las remitirán inmediatamente a las respectivas Delegaciones.
6. La Delegación Provincial de la Oficina del Censo Electoral, en un plazo de tres días, resolverá las reclamaciones presentadas y ordenará las rectificaciones pertinentes, que habrán de ser expuestas al público el décimo séptimo día posterior a la convocatoria. Asimismo se notificará la resolución adoptada a cada uno de los reclamantes y a los Ayuntamientos y Consulados correspondientes."

El procedimiento a seguir para la reclamación en período electoral se encuentra regulado, según el tipo de elecciones, en dos Ordenes del Ministerio de Economía y Hacienda distintas: La Orden de 21 de marzo de 1991 por la que se regula el proceso de reclamación administrativa en período electoral y la Orden de 15 de abril de 1994 por la que se regula el proceso de reclamación administrativa en período electoral para las elecciones al Parlamento Europeo.

ANÁLISIS DE LA JURISPRUDENCIA RELEVANTE

El derecho fundamental a la protección de datos está presente en la jurisprudencia española desde 1993, pero su definición más clara tuvo lugar con la **Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre**, la cual contenía las definiciones del derecho a la protección de datos contenidas en la jurisprudencia anterior en sus **fundamentos jurídicos 6 y 7**:

"el derecho fundamental a la protección de datos persigue garantizar a esa persona sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado."

"El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce quiénes los poseen, y con qué fin."

"el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, a la intimidad, y que sirven a la capital función que desempeña un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, F.J. 7)."

> *"De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos 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, sea el Estado o un particular, 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. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.*
> *En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos."*

Así, el Tribunal Constitucional incluye en el contenido esencial del derecho fundamental a la protección de datos lo siguiente:

• La posibilidad de conocer quién trata los datos y para qué, que actualmente se traduciría por el **principio de transparencia y derecho de información** previstos en la normativa.

• La **facultad de decidir qué datos se proporcionan a terceros y de consentir su tratamiento** (recogida, obtención, acceso, almacenamiento, uso, ya sea por quién los recoge o por parte de terceos) de los datos personales. Aunque ahora la normativa prevé que no sólo el consentimiento puede autorizar el tratamiento de datos personales, hay quién aún defiende que sólo podrán tratarse los datos con el consentimiento del interesado y que las otras bases jurídicas del tratamiento previstas en el ordenamiento jurídico constituyen restricciones al derecho a la protección de datos personales que deben estar debidamente justificadas, cumplir con lo previsto en el artículo 23 del RGPD y establecidas por Ley de acuerdo con la doctrina constitucional.

• La **facultad de oponerse al tratamiento** por parte de terceros y por determinados fines, que actualmente se traduciría por el derecho de oposición previsto en la normativa.

Cualquier restricción de cualquiera de estos componentes del derecho a la protección de datos deberá estar establecido por Ley porque los límites a los derechos fundamentales deben cumplir con la **reserva de Ley** prevista en el **artículo 53.1 de la Constitución**, la cual implica que toda limitación de un derecho fundamental, en este caso el de protección de datos personales, debe establecerse por Ley, y según la STC 292/2000, FJ 11, debe ser "*necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero, FJ 6; 18/1999, de 22 de febrero FJ 2)*." Cuanto al fin legítimo, la STC 292/2000, en su FJ 15, se refiere al mismo como "*la protección de otros derechos o bienes constitucionales (STC 104/2000, de 13 de abril, FJ 8 y las allí citadas)*".

Estos límites, de acuerdo con el mismo fundamento jurídico 11, "*o bien pueden ser restricciones directas del derecho fundamental mismo, (…), o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 C.E.*"

La STC 292/2000, FJ 14, declaró inconstitucional el artículo 21.1 de la antigua LOPD 15/1999 porque no fijó "*por sí misma, como le impone la Constitución, (art. 53.1 C.E.), los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado (art. 11 L.O.P.D., en relación con lo dispuesto en los arts. 4, 6 y 34.e L.O.P.D.), sino que se ha limitado a identificar la norma que puede hacerlo en su lugar*."

Así, consideró que no solicitar el consentimiento del interesado para que las administraciones públicas se comunicasen los datos de la ciudadanía para usos distintos de los de la recogida, suponía un límite a la protección de los datos personales que debía estar regulado por Ley y no reglamentariamente, como establecía el artículo 21.1 de la antigua LOPD. Lo explicaba en la **Sentencia del Tribunal Constitucional 17/2013, de 31 de enero**, en su **fundamento jurídico 4**, del siguiente modo:

> *"Con arreglo a tales criterios en la STC 292/2000 declaramos inconstitucional un determinado inciso del apartado 1 del art. 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, por cuanto regulaba la posibilidad de que una norma reglamentaria permitiera la cesión de datos entre Administraciones públicas para ser empleados en el ejercicio de competencias o para materias distintas a las que motivaron su originaria recogida sin necesidad de recabar previamente el consentimiento del interesado (art. 11.1 LOPD, en relación con lo dispuesto en los arts. 4.1 y 2 y 5.4 y 5), soslayando de esta forma la obligada reserva de ley derivada del art. 53.1 para el establecimiento de la regulación y los límites de un derecho fundamental.*
>
> *En conclusión, tal como establece nuestra doctrina, es claro que la Ley Orgánica de protección de datos no permite la comunicación indiscriminada de datos personales entre Administraciones públicas dado que, además, estos datos están, en principio, afectos a finalidades concretas y predeterminadas que son las que motivaron su recogida y tratamiento. Por tanto, la cesión de datos entre Administraciones públicas sin consentimiento del afectado, cuando se cedan para el ejercicio de competencias distintas o que versen sobre materias distintas de aquellas que motivaron su recogida, únicamente será posible, fuera de los supuestos expresamente previstos por la propia Ley Orgánica de protección de datos, si existe previsión legal expresa para ello [art. 11.2 a) en relación con el 6.1 LOPD] ya que, a tenor de lo dispuesto en el art. 53.1 CE, los límites al derecho a consentir la cesión de los datos a fines distintos para los que fueron recabados están sometidos a reserva de ley. Reserva legal que, como es obvio, habrá de cumplir con los restantes requisitos derivados de nuestra doctrina –esencialmente, basarse en bienes de dimensión constitucional y respetar las exigencias del principio de proporcionalidad– para poder considerar conforme con la Constitución la circunstancia de que la norma legal en cuestión no contemple, por tanto, la necesidad de contar con el consentimiento del afectado para autorizar la cesión de datos."*

Sin embargo, en la Sentencia del Tribunal Constitucional 17/2013 no se declara inconstitucional el acceso a los datos necesarios que consten en la Agencia Tributaria, la Seguridad Social o el Padrón Municipal, para la actuación de la Administración estatal en el ámbito de la Ley Orgánica de derechos y libertades de los extranjeros, ni el acceso a los datos del Padrón Municipal por parte de la

Dirección General de la Policía, sino que se **establece su constitucionalidad siempre que se interpreten en los términos de los fundamentos jurídicos 7 y 9 respectivamente**.

En lo que respecta al fundamento jurídico 7, el mismo autoriza el acceso a los mencionados datos condicionándolo a que el acceso esté relacionado con un determinado expediente, tratándose entonces de un acceso específico en cada caso, para los datos que sean exclusivamente necesarios o pertinentes para la resolución del mismo. Por lo tanto, **no puede procederse a un acceso masivo** a todos los datos personales que custodian estas administraciones.

Sobre el fundamento jurídico 9, el Tribunal Constitucional admite su constitucionalidad porque se establece por Ley, cumpliendo con la reserva de Ley, y la misma prevé la finalidad perseguida y que el acceso se realizará "*con las máximas medidas de seguridad*" y quedará constancia en al Dirección General de Policía de cada acceso, la identificación de usuario, fecha y hora en que se realizó, así como de los datos consultados" y que dichas medidas "s*on susceptibles de control*", añadiendo que "*el acceso solamente será posible, en las condiciones antes dichas, cuando el concreto dato en cuestión resulte pertinente y necesario en relación con la finalidad que ha justificado el acceso, quedando garantizada la posibilidad de analizar si, en cada caso concreto, el acceso tenía amparo en lo establecido en la ley pues, en caso contrario, no resultará posible su uso*." Por lo tanto, el acceso a los datos tampoco puede ser masivo y debe cumplir con ciertas exigencias tales como la **justificación del acceso respecto a la finalidad perseguida**.

Aún así, existe un **voto particular de la Sentencia del Tribunal Constitucional 17/2013 del Magistrado Pablo Pérez Tremps**, contrario a lo dispuesto en el fundamento jurídico 9 por considerar la interpretación de la mayoría como indeterminada y poco ajustada al juicio de proporcionalidad:

> *" En primer término, debe decirse que la interpretación conforme que realiza la sentencia no consigue colmar la indeterminación de la norma impugnada, lo que impide garantizar la proporcionalidad e idoneidad de la medida en cuestión. Así, sin ánimo de ser exhaustivo, puede decirse que existen profundas indeterminaciones en relación con el sujeto habilitado para el acceso, así como con la forma, objeto y garantías del acceso. Por ejemplo, se habilita de forma general a la Dirección General de la Policía para acceder a los datos, sin que la norma, ni la interpretación conforme, aclaren si el acceso se permite al titular de ese órgano (el Director General de la Policía) o a cualquier órgano o unidad integrados en dicha dirección, aunque la lectura completa de la norma permite deducir que podrá acceder cualquier miembro de la Dirección General de la Policía, en la medida en que se establece en la propia disposición impugnada que «quedará constancia en la Dirección General de la Policía de cada acceso, la identificación de usuario, fecha y hora en que se realizó, así como de los datos consultados». Esto supone un amplio universo de sujetos habilitados, lo que va en detrimento de la proporcionalidad de la medida y del mandato de predeterminación de las medidas limitativas de derechos fundamentales.*
>
> *Por lo que hace a la forma de acceso, se deduce que la misma será telemática y directa, sin necesidad de autorización del municipio, y además, según la posición de interpretación conforme de la mayoría, motivada. Sin embargo, no se establecen límites o condiciones al objeto de acceso que puede abarcar la totalidad de los «datos de inscripción padronal de los extranjeros existentes en los padrones municipales», lo que no sólo incluye su domicilio, objeto fundamental del padrón, sino también su número de pasaporte [art. 16.2 f) LOEx], en defecto de número de identidad de extranjero, con las implicaciones que, como veremos, eso tiene respecto de la identificación de extranjeros en situación de irregularidad administrativa.*

> *Por último, aunque la norma prevé que el acceso se realizará con las «máximas medidas de seguridad», éstas no se concretan, más allá de que quedará constancia de cada acceso, de la identidad del accedente, de la fecha y hora del acceso y de los datos consultados. La posición de la mayoría afirma que el acceso, y la motivación que lo inspira, «estará sujeta a control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional contencioso-administrativo, y entiende que habrá de evitarse que se produzca un uso torticero de la facultad de acceso, así como un acceso indiscriminado o masivo. Todas estas previsiones, no obstante, resultan excesivamente indeterminadas e insuficientes. Por dar sólo un ejemplo, no se contempla que el propio afectado pueda conocer que se ha producido el acceso y, en consecuencia, queda indefenso respecto de una medida limitativa de un derecho fundamental ante la que no puede protegerse plenamente en caso de un eventual acceso indebido en su información padronal."*

Además de cuestionar los términos utilizados por la Ley, que considera indeterminados, del mismo modo que la interpretación del Tribunal, **el Magistrado plantea que el Tribunal no tuvo presente la imposibilidad de los interesados de conocer el acceso por parte de la Policía a sus datos personales inscritos lo que limita su derecho a la protección de datos personales porque al no conocer el tratamiento por parte de la Policía tampoco puede oponerse al mismo**.

Sobre el **derecho de información de los interesados**, el cual ha sido reforzado con el Reglamento (UE) 2016/679 General de Protección de Datos, hay jurisprudencia del Tribunal Constitucional, anterior al RGPD y a las Sentencias mencionadas, que ya definía qué facultades se incluyen en el **principio de transparencia, incluyendo dentro de su ámbito de aplicación las Administraciones Públicas**. Un ejemplo de esta jurisprudencia lo encontramos en la **Sentencia del Tribunal Constitucional 254/1999, de 20 de julio, en su Fundamento Jurídico 7º**[95]:

> *"(…) Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 C.E., y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente (STC 11/1981, fundamento jurídico 8º, y 101/1991, fundamento jurídico 2º)."*

Teniendo en cuenta la jurisprudencia analizada, el hecho que la inscripción al padrón es obligatoria y que por lo tanto, y como ya advertía la sentencia 17/2013, en su fundamento jurídico 8, "*constituye una excepción al principio básico de la necesidad del consentimiento del ciudadano para la legalidad del tratamiento*", que hoy se ampara bajo la base jurídica del interés público o ejercicio de poderes públicos, **y que no se informa correctamente a los interesados de la comunicación de estos datos a los partidos políticos en el momento de su recogida**, siendo privados así del derecho a oponerse a su tratamiento y comunicación, **además de no ser datos necesarios para el cumplimiento de las misiones que los partidos realizan** con los mismos, de acuerdo con los principios de minimización de datos y de privacidad desde el diseño y por defecto, **debería suprimirse la comunicación de datos prevista por la LOREG a los partidos políticos de los datos del censo electoral, que además supone un acceso masivo a los mismos y no limitado a los datos necesarios**.

En lo referido a los datos necesarios en el contexto electoral, debe tenerse en cuenta un **Dictamen CNS 48/2019 de la Autoritat**

[95] http://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1993-21425.pdf

Catalana de Protecció de Dades[96] (en adelante, APDCAT) que haciendo referencia al principio de minimización de datos recuerda que:

> *"deben realizarse únicamente los tratamientos de datos que resulten necesarios o proporcionados en atención a la finalidad que los motiva.*
> *De este modo, si la finalidad perseguida en un determinado contexto (en nuestro caso, el envío de información electoral) puede ser lograda sin necesidad de llevar a cabo un tratamiento de datos personales, sin verse por ello alterada o perjudicada dicha finalidad, debería optarse necesariamente por esta posibilidad, atendiendo a que el tratamiento de datos de carácter personal supone, como consagra el Tribunal Constitucional en su sentencia 292/2000, una limitación al derecho del afectado a disponer de la información referida a su persona."*

Así la APDCAT concluye que sólo son necesarios para el envío de propaganda electoral por correo electrónico el nombre, apellidos y dirección de correo electrónico, y el resto de datos que constan en el censo no deben ser comunicados a las candidaturas. Además, el dictamen recuerda que el colegio deberá tomar medidas para permitir que los colegiados puedan oponerse a dicho tratamiento. Finalmente, en base al mismo razonamiento, la APDCAT dispone que no es necesario comunicar a las candidaturas el censo electoral de colegiados porque el envío de comunicaciones electorales puede realizarse sin que se produzca dicho tratamiento de datos. Debe recordarse que en el contexto del dictamen la APDCAT tubo en cuenta la normativa específica que regula los tratamientos de datos personales en período electoral, consistente en la Ley 7/2006, de 31 de mayo, del ejercicio de profesiones titulada y colegios profesionales y los Estatutos del colegio profesional que planteó la consulta, que priman por encima de la normativa de protección de datos personales al tratarse de una regulación más específica.

Finalmente, debemos mencionar la **Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo**, dónde también se analizó la aplicación de la normativa de protección de datos consistente en la Ley Orgánica 3/2018 de Protección de Datos y garantía de los derechos digitales y del Reglamento (UE) 2016/679 General de Protección de Datos, en el contexto de la Ley Orgánica del Régimen Electoral General (en adelante, LOREG), sobretodo en el aspecto relativo a las garantías que esta última establece respecto al tratamiento de datos personales. En este sentido la sentencia, en sus fundamentos de derecho 8 y 9, admite **que es la propia LOREG la que debe establecer las garantías mínimas (consistentes en la legitimación, delimitación del tratamiento y garantías y medidas que deben aplicarse) para el tratamiento**:

> *"Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas. (…)*
> *Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. (…)* ***Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares****. (…)*
> *En efecto, como expondremos a continuación, la insuficiencia de la ley no puede ser colmada por vía interpretativa a partir de las pautas e indicaciones que se puedan extraer de los citados textos normativos (i). Tampoco puede ser colmada por el titular de una potestad normativa limitada como es la Agencia Española de Protección de Datos (ii) o mediante una interpretación conforme (iii). Finalmente, una remisión implícita como la pretendida tampoco resultaría*

[96] https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2019/Documents/ca_cns_2019_048.pdf

coherente con el marco regulador europeo (iv), perspectiva que, como se dijo, no puede ser irrelevante para nuestro enjuiciamiento constitucional.

(i) ***Es evidente que si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización*** *que sacrifica la reserva de ley ex art. 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (…)*
Pero ***lo mismo ocurre si****, como sostiene el abogado del Estado,* ***la norma incluye una remisión para la integración de la ley con las garantías adecuadas establecidas en dos textos normativos sin mayores precisiones, esto es, sin reglas claras y precisas que delimiten efectiva y eficazmente las garantías adecuadas que se consideran aplicables; más aún, cuando tales textos normativos, por un lado, se componen de noventa y nueve artículos (el RGPD) y noventa y siete artículos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria única y dieciséis disposiciones finales (la LOPDGDD), y, por otro lado, ninguna de ellas se refiere específicamente a las garantías adecuadas*** *para la protección de la categoría especial de datos que son los relativos a las opiniones políticas de las personas. Eso dejaría la decisión en manos, no del legislador, sino exclusivamente a disposición de la determinación reglamentaria* ***del Gobierno o bien, en ausencia de este último, del aplicador del derecho, el cual tendría que deducir por su cuenta cuáles de las garantías previstas en ambas normas de remisión resultan aplicables al tratamiento en cuestión****. Todo ello supondría una insuficiencia manifiesta en el contenido mínimo exigible, en condiciones de certeza y previsibilidad, a la configuración legal del derecho fundamental a la protección de datos personales.*

(ii) La insuficiencia legal que venimos analizando tampoco puede ser colmada, en ejercicio de sus potestades, por la Agencia Española de Protección de Datos. (…) Por tanto, la circunstancia de que, con posterioridad a la interposición del presente recurso contra la ley, la Presidencia de la Agencia Española de Protección de Datos haya aprobado la Circular 1/2019, de 7 de marzo, para abordar esa laguna, tal como se indicó anteriormente, no puede subsanar la insuficiencia constitucional de la que adolece el art. 58 bis LOREG introducido por la Ley Orgánica 3/2018 por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas en el marco de actividades electorales. (…)

(iii) La falta de previsión legal de un elemento cuya previsión es necesaria para que se pueda considerar que se respeta el contenido esencial, tampoco se puede superar con la técnica de la interpretación conforme, pues esta técnica, que viene impuesta por el principio de conservación de la ley, se aplica cuanto existen "varias interpretaciones posibles igualmente razonables" y permite descartar aquella o aquellas que darían lugar a que el precepto incurriera en inconstitucionalidad [SSTC 168/2016, de 6 de octubre, FJ 4 b); y 97/2018, de 19 de septiembre, FJ 7, por todas]. ***En el presente caso no estamos ante "varias interpretaciones posibles igualmente razonables", sino ante la insuficiencia de regulación detectada en una norma de desarrollo de un derecho fundamental****.*

iv) Por último, ***debemos recordar que el Reglamento General de Protección de Datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales*** *que no son especiales. En cambio, no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende,* ***tampoco fija las garantías que deben observar los diversos tratamientos posibles*** *de datos sensibles,* ***adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso****; (…)* ***Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso****. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas, no*

prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento General de Protección de Datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.

9. ***De lo anterior se concluye que la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales****."*

Puesto que esta misma sentencia dictamina en su fundamento jurídico 6 que "el nivel y la naturaleza de las garantías adecuadas no se pueden determinar de una vez para todas, pues, por un lado, deben revisarse y actualizarse cuando sea necesario y, por otro lado, el principio de proporcionalidad obliga a verificar si, con el desarrollo de la tecnología, aparecen posibilidades de tratamiento que resultan menos intrusivas o potencialmente menos peligrosas para los derechos fundamentales", insistimos en nuestra voluntad de derogar la comunicación de datos a los partidos políticos para así garantizar una mayor protección de la intimidad y los datos personales de toda la ciudadanía.

LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local

Artículo 15.
Toda persona que viva en España está obligada a inscribirse en el Padrón del municipio en el que resida habitualmente. Quien viva en varios municipios deberá inscribirse únicamente en el que habite durante más tiempo al año.
El conjunto de personas inscritas en el Padrón municipal constituye la población del municipio.
Los inscritos en el Padrón municipal son los vecinos del municipio.
La condición de vecino se adquiere en el mismo momento de su inscripción en el Padrón.

Artículo 16.
1. El Padrón municipal es el registro administrativo donde constan los vecinos de un municipio. Sus datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo. Las certificaciones que de dichos datos se expidan tendrán carácter

de documento público y fehaciente para todos los efectos administrativos.
La inscripción en el Padrón Municipal sólo surtirá efecto de conformidad con lo dispuesto en el artículo 15 de esta ley por el tiempo que subsista el hecho que la motivó y, en todo caso, deberá ser objeto de renovación periódica cada dos años cuando se trate de la inscripción de extranjeros no comunitarios sin autorización de residencia permanente.
El transcurso del plazo señalado en el párrafo anterior será causa para acordar la caducidad de las inscripciones que deban ser objeto de renovación periódica, siempre que el interesado no hubiese procedido a tal renovación. En este caso, la caducidad podrá declararse sin necesidad de audiencia previa del interesado.

2. La inscripción en el Padrón municipal contendrá como obligatorios sólo los siguientes datos:
a) Nombre y apellidos.
b) Sexo.
c) Domicilio habitual.
d) Nacionalidad.
e) Lugar y fecha de nacimiento.
f) Número de documento nacional de identidad o, tratándose de extranjeros:
• Número de la tarjeta de residencia en vigor, expedida por las autoridades españolas, o en su defecto, número del documento acreditativo de la identidad o del pasaporte en vigor expedido por las autoridades del país de procedencia, tratándose de ciudadanos nacionales de Estados Miembros de la Unión Europea, de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo o de Estados a los que, en virtud de un convenio internacional se extienda el régimen jurídico previsto para los ciudadanos de los Estados mencionados.

• Número de identificación de extranjero que conste en documento, en vigor, expedido por las autoridades españolas o, en su defecto, por no ser titulares de éstos, el número del pasaporte en vigor expedido por las autoridades del país de procedencia, tratándose de ciudadanos nacionales de Estados no comprendidos en el inciso anterior de este párrafo, salvo que, por virtud de Tratado o Acuerdo Internacional, disfruten de un régimen específico de exención de visado en materia de pequeño tráfico fronterizo con el municipio en el que se pretenda el empadronamiento, en cuyo caso, se exigirá el correspondiente visado.
g) Certificado o título escolar o académico que se posea.
h) Cuantos otros datos puedan ser necesarios para la elaboración del Censo Electoral, siempre que se garantice el respeto a los derechos fundamentales reconocidos en la Constitución.

3. Los datos del Padrón Municipal se cederán a otras Administraciones públicas que lo soliciten sin consentimiento previo al afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y en las leyes de estadística de las comunidades autónomas con competencia en la materia.

Artículo 17.
1. La formación, mantenimiento, revisión y custodia del Padrón municipal corresponde al Ayuntamiento, de acuerdo con lo que establezca la legislación del Estado.
Con este fin, los distintos organismos de la Administración General del Estado, competentes por razón de la materia, remitirán periódicamente a cada Ayuntamiento información sobre las variaciones de los datos de sus vecinos que con carácter obligatorio

deben figurar en el Padrón municipal, en la forma que se establezca reglamentariamente.
La gestión del Padrón municipal se llevará por los Ayuntamientos con medios informáticos. Las Diputaciones Provinciales, Cabildos y Consejos insulares asumirán la gestión informatizada de los Padrones de los municipios que, por su insuficiente capacidad económica y de gestión, no puedan mantener los datos de forma automatizada.

2. Los Ayuntamientos realizarán las actuaciones y operaciones necesarias para mantener actualizados sus Padrones de modo que los datos contenidos en éstos concuerden con la realidad.
Si un ayuntamiento no llevara a cabo dichas actuaciones, el Instituto Nacional de Estadística, previo informe del Consejo de Empadronamiento, podrá requerirle previamente concretando la inactividad, y si fuere rechazado, sin perjuicio de los recursos jurisdiccionales que procedan, podrá acudir a la ejecución sustitutoria prevista en el artículo 60 de la presente ley.

3. Los Ayuntamientos remitirán al Instituto Nacional de Estadística los datos de sus respectivos Padrones, en la forma que reglamentariamente se determine por la Administración General del Estado, a fin de que pueda llevarse a cabo la coordinación entre los Padrones de todos los municipios.
El Instituto Nacional de Estadística, en aras a subsanar posibles errores y evitar duplicidades, realizará las comprobaciones oportunas, y comunicará a los Ayuntamientos las actuaciones y operaciones necesarias para que los datos padronales puedan servir de base para la elaboración de estadísticas de población a nivel nacional, para que las cifras resultantes de las revisiones anuales puedan ser declaradas oficiales, y para que los Ayuntamientos puedan remitir, debidamente actualizados, los datos del Censo Electoral.
Corresponderá al Presidente del Instituto Nacional de Estadística la resolución de las discrepancias que, en materia de empadronamiento, surjan entre los Ayuntamientos, Diputaciones Provinciales, Cabildos y Consejos insulares o entre estos entes y el Instituto Nacional de Estadística, así como elevar al Gobierno de la Nación la propuesta de cifras oficiales de población de los municipios españoles, comunicándolo en los términos que reglamentariamente se determinan al Ayuntamiento interesado.
El Instituto Nacional de Estadística remitirá trimestralmente a los Institutos estadísticos de las comunidades autónomas u órganos competentes en la materia, y en su caso, a otras Administraciones públicas los datos relativos a los padrones en los municipios de su ámbito territorial en los que se produzcan altas o bajas de extranjeros en las mismas condiciones señaladas en el artículo 16.3 de esta ley.

4. Adscrito al Ministerio de Economía y Hacienda se crea el Consejo de Empadronamiento como órgano colegiado de colaboración entre la Administración General del Estado y los Entes Locales en materia padronal, de acuerdo con lo que reglamentariamente se establezca.
El Consejo será presidido por el Presidente del Instituto Nacional de Estadística y estará formado por representantes de la Administración General del Estado y de los Entes Locales.
El Consejo funcionará en Pleno y en Comisión, existiendo en cada provincia una Sección Provincial bajo la presidencia del Delegado del Instituto Nacional de Estadística y con representación de los Entes Locales.
El Consejo de Empadronamiento desempeñará las siguientes funciones:

A) Elevar a la decisión del Presidente del Instituto Nacional de Estadística propuesta vinculante de resolución de las discrepancias que surjan en materia de empadronamiento entre Ayuntamientos, Diputaciones Provinciales, Cabildos, Consejos insulares o entre estos entes y el Instituto Nacional de Estadística.
B) Informar, con carácter vinculante, las propuestas que eleve al Gobierno el Presidente del Instituto Nacional de Estadística sobre cifras oficiales de población de los municipios españoles.

C) Proponer la aprobación de las instrucciones técnicas precisas para la gestión de los padrones municipales.
D) Cualquier otra función que se le atribuya por disposición legal o reglamentaria.

5. La Administración General del Estado, en colaboración con los Ayuntamientos y Administraciones de las Comunidades Autónomas confeccionará un Padrón de españoles residentes en el extranjero, al que será de aplicación las normas de esta Ley que regulan el Padrón municipal.
Las personas inscritas en este Padrón se considerarán vecinos del municipio español que figura en los datos de su inscripción únicamente a efectos del ejercicio del derecho de sufragio, no constituyendo, en ningún caso, población del municipio.

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).

Considerando (26)
Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

Artículo 5. Principios relativos al tratamiento
1. Los datos personales serán:
a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten

exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6. Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
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. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:
a) el Derecho de la Unión, o
b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento. La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Considerando (31)
Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

Considerando (41)
Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia») y del Tribunal Europeo de Derechos Humanos.

Considerando (45)
Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la

determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

Considerando (50)
El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si 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, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.
Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado
1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:
a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o
b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. 8.La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Considerando (39)
Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la

información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

Considerando (58)
El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado
1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:
a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su

rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado
1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
d) las categorías de datos personales de que se trate;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:
a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los

datos;
d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
e) el derecho a presentar una reclamación ante una autoridad de control;
f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:
a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:
a) el interesado ya disponga de la información;
b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Artículo 25. Protección de datos desde el diseño y por defecto
1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento,

a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 30. Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:
a) 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;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d)las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:
a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c)en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales.

Artículo 2. *Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94*
1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Esta ley orgánica no será de aplicación:
a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.
b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.
c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

4. El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

Artículo 8. *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos*

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 11. *Transparencia e información al afectado*
1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:
a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
En estos supuestos, la información básica incluirá también:
a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

Artículo 31. *Registro de las actividades de tratamiento*
1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.
El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las

actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.
Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica 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.

Disposición final undécima. *Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*
Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en los siguientes términos:
Uno. Se añade un nuevo artículo 6 bis, con la siguiente redacción:

«**Artículo 6 bis**. *Registro de actividades de tratamiento*
Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.»
Dos. El apartado 1 del artículo 15 queda redactado como sigue:
«1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.
Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.»

Artículo 77. *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*
1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:
a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.

j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 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 sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.
Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

Disposición final tercera. *Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General*
Se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que queda redactada como sigue:
Uno. El apartado 3 del artículo treinta y nueve queda redactado como sigue:

> *«3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no*

inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.»

Dos. Se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente:

*«**Artículo cincuenta y ocho bis**. Utilización de medios tecnológicos y datos personales en las actividades electorales.*
1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.
2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.
3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.
4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.
5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

Artículo treinta y uno.
1. El censo electoral contiene la inscripción de quienes reúnen los requisitos para ser elector y no se hallen privados, definitiva o temporalmente, del derecho de sufragio.

2. El censo electoral está compuesto por el censo de los electores residentes en España y por el censo de los electores residentes-ausentes que viven en el extranjero. Ningún elector podrá figurar inscrito simultáneamente en ambos censos.

3. El Censo Electoral es único para toda clase de elecciones, sin perjuicio de su posible ampliación para las elecciones Municipales y del Parlamento Europeo a tenor de lo dispuesto en los artículos 176 y 210 de la presente Ley Orgánica.

Artículo treinta y dos.
1. La inscripción en el censo electoral es obligatoria. Además del nombre y los apellidos, único dato necesario para la identificación del elector en el acto de la votación, sin perjuicio de lo dispuesto en el artículo 85, se incluirá entre los restantes datos censales el número del Documento Nacional de Identidad.

2. Los Ayuntamientos tramitan de oficio la inscripción de los residentes en su término municipal.

3. Las Oficinas Consulares de Carrera y Secciones Consulares de las Misiones Diplomáticas tramitarán de oficio la inscripción de los españoles residentes en su demarcación en la forma que se disponga reglamentariamente.

Artículo treinta y cuatro. *Carácter y vigencia del censo electoral*
El censo electoral es permanente y su actualización es mensual, con referencia al día primero de cada mes.

Artículo treinta y cinco. *Actualización del Censo Electoral*
1. Para la actualización mensual del censo los Ayuntamientos enviarán a las Delegaciones Provinciales de la Oficina del Censo Electoral, hasta el penúltimo día hábil de cada mes, y en la forma prevista por las instrucciones de dicho organismo, todas las modificaciones del Padrón producidas en dicho mes.

2. Si algún Ayuntamiento no cumpliera con la obligación establecida en el párrafo anterior, el Director de la Oficina del Censo dará cuenta de ello a la Junta Electoral Central para que por la misma se adopten las medidas procedentes.

3. En la actualización correspondiente al primer mes del año se acompañarán, además, las altas, con la calificación de menor, de los residentes que cumplirán dieciocho años entre el 1 de enero y el 31 de diciembre del año siguiente.

Artículo treinta y siete. *Actualización del Censo a cargo del Registro Civil y del Registro de Penados y Rebeldes*
Los encargados del Registro Civil comunicarán mensualmente a las Delegaciones Provinciales de la Oficina del Censo Electoral cualquier circunstancia que pueda afectar a las inscripciones en el censo electoral.

Artículo treinta y ocho.
1. Con los datos consignados en los artículos anteriores, las Delegaciones Provinciales de la Oficina del Censo Electoral mantendrán a disposición de los interesados el censo actualizado para su consulta permanente, que podrá realizarse a través de los Ayuntamientos, Consulados o en la propia Delegación Provincial.

2. Las reclamaciones sobre los datos censales se dirigirán a las Delegaciones Provinciales de la Oficina del Censo Electoral, que resolverán en el plazo de cinco días a contar desde la recepción de aquéllas.
Los Ayuntamientos y Consulados remitirán inmediatamente las reclamaciones que reciban a las respectivas Delegaciones Provinciales de la Oficina del Censo Electoral.
Los representantes de las candidaturas o representantes de los partidos, federaciones y coaliciones podrán impugnar el censo de

las circunscripciones que hubieren registrado un incremento de residentes significativo y no justificado que haya dado lugar a la comunicación a que se refiere el artículo 30.c), dentro del plazo de cinco días siguientes al momento en que tuvieren conocimiento de la referida comunicación.

3. La Oficina del Censo Electoral adoptará las medidas oportunas para facilitar la tramitación por los Ayuntamientos y Consulados de las consultas y reclamaciones.

4. Los recursos contra las resoluciones en esta materia de las Delegaciones de la Oficina del Censo Electoral se tramitarán por el procedimiento preferente y sumario previsto en el número 2 del artículo 53 de la Constitución.

Artículo treinta y nueve. *Rectificación del Censo en período electoral*
1. Para cada elección el Censo Electoral vigente será el cerrado el día primero del segundo mes anterior a la convocatoria.

2. Los ayuntamientos y consulados estarán obligados a mantener un servicio de consulta de las listas electorales vigentes de sus respectivos municipios y demarcaciones durante el plazo de ocho días, a partir del sexto día posterior a la convocatoria de elecciones.
La consulta podrá realizarse por medios informáticos, previa identificación del interesado, o mediante la exposición al público de las listas electorales, si no se cuenta con medios informáticos suficientes para ello.

3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.

4. También en el mismo plazo los representantes de las candidaturas podrán impugnar el censo de las circunscripciones que en los seis meses anteriores hayan registrado un incremento de residentes significativo y no justificado que haya dado lugar a la comunicación a que se refiere el artículo 30.c).

5. Las reclamaciones podrán presentarse directamente en las delegaciones provinciales de la Oficina del Censo Electoral correspondiente o a través de los ayuntamientos o consulados, quienes las remitirán inmediatamente a las respectivas Delegaciones.

6. La Delegación Provincial de la Oficina del Censo Electoral, en un plazo de tres días, resolverá las reclamaciones presentadas y ordenará las rectificaciones pertinentes, que habrán de ser expuestas al público el décimo séptimo día posterior a la convocatoria. Asimismo se notificará la resolución adoptada a cada uno de los reclamantes y a los Ayuntamientos y Consulados correspondientes.

7. La Oficina del Censo Electoral remitirá a todos los electores una tarjeta censal con los datos actualizados de su inscripción en el censo electoral y de la Sección y Mesa en la que le corresponde votar, y comunicará igualmente a los electores afectados las modificaciones de Secciones, locales o Mesas, a que se refiere el artículo 24 de la presente Ley Orgánica.

Artículo cuarenta y uno.

1. Por real decreto se regularán los datos personales de los electores, necesarios para su inscripción en el censo electoral, así como los de las listas y copias del censo electoral.

2. Queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral, a excepción de los que se soliciten por conducto judicial.

3. No obstante, la Oficina del Censo Electoral puede facilitar datos estadísticos que no revelen circunstancias personales de los electores.

4. Las comunidades autónomas podrán obtener una copia del censo, en soporte apto para su tratamiento informático, después de cada convocatoria electoral, además de la correspondiente rectificación de aquél.

5. Los representantes de cada candidatura podrán obtener dentro de los dos días siguientes a la proclamación de su candidatura una copia del censo del distrito correspondiente, ordenado por mesas, en soporte apto para su tratamiento informático, que podrá ser utilizado exclusivamente para los fines previstos en la presente Ley. Alternativamente los representantes generales podrán obtener en las mismas condiciones una copia del censo vigente de los distritos donde su partido, federación o coalición presente candidaturas. Asimismo, las Juntas Electorales de Zona dispondrán de una copia del censo electoral utilizable, correspondiente a su ámbito.
Las Juntas Electorales, mediante resolución motivada, podrán suspender cautelarmente la entrega de las copias del censo a los representantes antes citados cuando la proclamación de sus candidaturas haya sido objeto de recurso o cuando se considere que podrían estar incursas en alguna de las circunstancias previstas en el artículo 44.4 de esta Ley.

6. Excepcionalmente y por razones debidamente justificadas, podrá excluirse a las personas que pudieran ser objeto de amenazas o coacciones que pongan en peligro su vida, su integridad física o su libertad, de las copias del censo electoral a que se refiere el apartado 5 del presente artículo.

Artículo cuarenta y cuatro.
1. Pueden presentar candidatos o listas de candidatos:
a) Los partidos y federaciones inscritos en el registro correspondiente.
b) Las coaliciones constituidas según lo dispuesto en el apartado siguiente.
c) Las agrupaciones de electores que reúnan los requisitos establecidos por las disposiciones especiales de la presente Ley.

2. Los partidos y federaciones que establezcan un pacto de coalición para concurrir conjuntamente a una elección deben comunicarlo a la Junta competente, en los diez días siguientes a la convocatoria. En la referida comunicación se debe hacer constar la denominación de la coalición, las normas por las que se rige y las personas titulares de sus órganos de dirección o coordinación.

3. Ningún partido, federación, coalición o agrupación de electores puede presentar más de una lista de candidatos en una circunscripción para la misma elección. Los partidos federados o coaligados no pueden presentar candidaturas propias en una circunscripción si en la misma concurre, para idéntica elección, candidatos de las federaciones o coaliciones a que pertenecen.

4. En todo caso, los partidos políticos, las federaciones o coaliciones de partidos, y las agrupaciones de electores no podrán presentar candidaturas que, de hecho, vengan a continuar o suceder la actividad de un partido político declarado judicialmente ilegal y disuelto, o suspendido. A estos efectos, se tendrá en cuenta la similitud sustancial de sus estructuras, organización y funcionamiento, de las personas que los componen, rigen, representan, administran o integran cada una de las candidaturas, de la procedencia de los medios de financiación o materiales, o de cualesquiera otras circunstancias relevantes que, como su disposición a apoyar la violencia o el terrorismo, permitan considerar dicha continuidad o sucesión.

Artículo cincuenta y ocho bis. *Utilización de medios tecnológicos y datos personales en las actividades electorales*
1. (Anulado)

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.

Artículo setenta y dos.
Si el ámbito territorial del medio o el de su programación fueran más limitados que el de la elección convocada, la distribución de espacios se hace atendiendo al número total de votos que obtuvo cada partido, federación o coalición en las circunscripciones comprendidas en el correspondiente ámbito de difusión o, en su caso, de programación.
En el caso de las elecciones al Parlamento Europeo, la distribución de espacios se realiza atendiendo al número total de votos que obtuvo cada partido, federación o coalición en el ámbito territorial del correspondiente medio de difusión o el de su programación.

Artículo setenta y tres.
1. Para la distribución de espacios gratuitos de propaganda en las elecciones a cualquiera de las dos Cámaras de las Cortes Generales solamente se tienen en cuenta los resultados de las precedentes elecciones al Congreso de los Diputados.

2. Si simultáneamente a las elecciones al Congreso de los Diputados se celebran elecciones a una Asamblea Legislativa de Comunidad Autónoma o elecciones municipales, sólo se tiene en cuenta los resultados de las anteriores elecciones al Congreso, para la distribución de espacios en la programación general de los medios nacionales.

3. Si las elecciones a una Asamblea Legislativa de Comunidad Autónoma se celebran simultáneamente a las elecciones municipales, sólo se tiene en cuenta los resultados de las anteriores elecciones a dicha Asamblea para la distribución de espacios en los medios de difusión de esa Comunidad Autónoma o en los correspondientes programas regionales de los medios nacionales.

4. En el supuesto previsto en el párrafo anterior, y siempre que no sea aplicable la regla del párrafo segundo de este artículo, la distribución de espacios en la programación general de los medios nacionales se hace atendiendo a los resultados de las anteriores elecciones municipales.

5. Si simultáneamente a las elecciones al Parlamento Europeo se celebran elecciones a cualquiera de las dos Cámaras de las Cortes Generales o elecciones municipales, sólo se tienen en cuenta los resultados de las anteriores elecciones al Congreso o, en su caso, de las elecciones municipales, para la distribución de espacios en la programación general de los medios nacionales.

6. Si simultáneamente a las elecciones al Parlamento Europeo se celebran elecciones a una Asamblea Legislativa de Comunidad Autónoma, sólo se tienen en cuenta los resultados de las anteriores elecciones a dicha Asamblea para la distribución de espacios en los medios de difusión de esa Comunidad Autónoma o en los correspondientes programas regionales de los medios nacionales.

7. A falta de regulación expresa en este artículo las Juntas Electorales competentes establecen los criterios para la distribución de espacios en los medios de comunicación de titularidad pública en los supuestos de coincidencia de elecciones.

Artículo ochenta y cinco.
1. El derecho a votar se acredita por la inscripción en los ejemplares certificados de las listas del censo o por certificación censal

específica y, en ambos casos, por la identificación del elector, que se realiza mediante documento nacional de identidad, pasaporte o permiso de conducir en que aparezca la fotografía del titular o, además, tratándose de extranjeros, con la tarjeta de residencia.

2. Los ejemplares certificados de las listas del censo a los que se refiere el párrafo anterior contendrán exclusivamente los ciudadanos mayores de edad en la fecha de la votación.

3. Asimismo pueden votar quienes acrediten su derecho a estar inscritos en el censo de la sección mediante la exhibición de la correspondiente sentencia judicial.

4. Cuando la Mesa, a pesar de la exhibición de alguno de los documentos previstos en el apartado 1, tenga duda, por si o a consecuencia de la reclamación que en el acto haga públicamente un interventor, apoderado u otro elector, sobre la identidad del individuo que se presenta a votar, la Mesa a la vista de los documentos acreditativos y del testimonio que puedan presentar los electores presentes, decide por mayoría. En todo caso se mandará pasar tanto de culpa al Tribunal competente para que exija la responsabilidad del que resulte usurpador de nombre ajeno o del que lo haya negado falsamente.

5. La certificación censal específica, a través de la cual el ciudadano acredita con carácter excepcional su inscripción en el censo electoral, se regirá en cuanto a su expedición, órgano competente para la misma, plazo y supuestos en que proceda, por lo que disponga al respecto la Junta Electoral Central mediante la correspondiente Instrucción.

Real Decreto 1732/1985, de 24 de septiembre, por el que se regulan las Condiciones de los Locales y las Características oficiales de los elementos materiales a Utilizar en los Procesos electorales.

Real Decreto 1733/1985, de 24 de septiembre, sobre Solicitud del Voto por correo en caso de Enfermedad o incapacidad que impida formularla personalmente.

Real Decreto 157/1996, de 2 de febrero, por el que se dispone la actualización mensual del censo electoral y se regulan los datos necesarios para la inscripción en el mismo.

Real Decreto 1799/2003, de 26 de diciembre, por el que se regula el contenido de las listas electorales y de las copias del censo electoral.

Orden, del Ministerio de Economía y Hacienda, de 3 de febrero de 1987, por la que se regula la distribución de copias del Censo Electoral en soporte magnético y la expedición de certificados de inscripción en el Censo Electoral.

Orden, del Ministerio de Economía y Hacienda, de 21 de marzo de 1991, por la que se regula el proceso de reclamación administrativa en período electoral.

Orden, del Ministerio de Economía y Hacienda, de 15 de abril de 1994, por la que se regula el proceso de reclamación administrativa en período electoral para las elecciones al Parlamento Europeo.

Orden, del Ministerio de Economía y Hacienda, Instrucción 7/2007, de 12 de abril, de la Junta Electoral Central, sobre la certificación censal específica prevista en el artículo 85.1 de la LOREG.

Resolución, de la Dirección de la Oficina del Censo Electoral, de 19 de julio de 1996, por la que se aprueban los modelos referidos en la Orden de 24 de abril de 1996 por la que se dictan normas técnicas para la actualización del censo electoral.

Orden EHA/642/2011, del Ministerio de Economía y Hacienda, de 25 de marzo, por la que se dictan normas técnicas para la actualización mensual del Censo Electoral.Instrucción, de 20 de enero de 2004, de la Junta Electoral Central, sobre consulta vía Internet de los datos del censo electoral.

Instrucción 7/2007, de 12 de abril, de la Junta Electoral Central, sobre la certificación censal específica prevista en el artículo 85.1 de la LOREG.

Instrucción 4/2009, de 17 de diciembre, de la Junta Electoral Central, sobre actuaciones de la Oficina del Censo Electoral en relación a la entrega de copias del censo electoral a las candidaturas y al envío de la documentación para ejercer el voto por correo.

ANEXO de

5 – ABUSOS EN EL ÁMBITO LABORAL:

LA VENTA DE LOS DATOS DE LAS PERSONAS EN RÉGIMEN DE AUTÓNOMOS

1. ANÁLISIS DEL DESARROLLO LEGISLATIVO Y ADMINISTRATIVO

Obligaciones de inscripción y actualización de información al Censo de Empresarios, Profesionales y Retenedores de la Agencia Tributaria y en el Registro Mercantil

Las obligaciones de inscripción y actualización de la información de los autónomos se encuentran fijadas en el primer apartado de la disposición adicional quinta de la Ley 58/2003 de la Ley General Tributaria, el artículo 9.1 y 10.1 del Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos, que desarrolla la Ley General Tributaria.

Disposición adicional quinta. Declaraciones censales.
"1. Las personas o entidades que desarrollen o vayan a desarrollar en territorio español actividades empresariales o profesionales o satisfagan rendimientos sujetos a retención deberán comunicar a la Administración tributaria a través de las correspondientes declaraciones censales su alta en el Censo de Empresarios, Profesionales y Retenedores, las modificaciones que se produzcan en su situación tributaria y la baja en dicho censo. El Censo de Empresarios, Profesionales y Retenedores formará parte del Censo de Obligados Tributarios. En este último figurarán la totalidad de personas físicas o jurídicas y entidades a que se refiere el artículo 35 de la Ley General Tributaria, identificadas a efectos fiscales en España.
Las declaraciones censales servirán, asimismo, para comunicar el inicio de las actividades económicas que desarrollen, las modificaciones que les afecten y el cese en las mismas. A efectos de lo dispuesto en este artículo, tendrán la consideración de empresarios o profesionales quienes tuvieran tal condición de acuerdo con las disposiciones propias del Impuesto sobre el Valor Añadido, incluso cuando desarrollen su actividad fuera del territorio de aplicación de este impuesto."

Artículo 9. *Declaración de alta en el Censo de Empresarios, Profesionales y Retenedores*.
"1. Quienes hayan de formar parte del Censo de Empresarios, Profesionales y Retenedores deberán presentar una declaración de alta en dicho censo."

Artículo 10. Declaración de modificación en el Censo de Empresarios, Profesionales y Retenedores.
"1. Cuando se modifique cualquiera de los datos recogidos en la declaración de alta o en cualquier otra declaración de modificación posterior, el obligado tributario deberá comunicar a la Administración tributaria, mediante la correspondiente declaración, dicha modificación."

Los obligados a inscribirse al Censo de Empresarios, Profesionales y Retenedores son los autónomos (para simplificar la redacción del artículo) previstos en el artículo 3.2 del Real Decreto 1065/2007.

El tercer apartado disposición adicional quinta de la Ley 58/2003 de la Ley General Tributaria contiene la información mínima que debe recogerse por parte de la Agencia Tributaria, a la que debe sumarse la información prevista por los artículos 4 a 8 del Real Decreto 1065/2007.

Finalmente, las finalidades de la inscripción y actualización de información se encuentran respectivamente listadas en los artículos 9.3 y 10.2 del Real Decreto 1065/2007.

Estos listados se pueden encontrar respectivamente en las páginas 31 y ss. y 35 y ss. de este informe.

El contenido de estos artículos se encuentra explicado de forma relativamente simplificada en la información general de la Agencia Tributaria proporcionada con los modelos de alta[97] [98] según las cuales están obligados inscribirse, antes del inicio de la actividad profesional, en el Censo de Empresarios.

Profesionales y Retenedores:

"- Empresarios o profesionales que vayan a comenzar el ejercicio de una o varias actividades económicas en territorio español.

– Quienes, no actuando como empresarios o profesionales, abonen rentas sujetas a retención o ingreso a cuenta o realicen entregas o adquisiciones intracomunitarias de bienes sujetas al IVA.

– Los empresarios o profesionales que sean destinatarios de servicios prestados por empresarios o profesionales no establecidos en el territorio de aplicación del Impuesto sobre el Valor Añadido respecto de los cuales sean sujetos pasivos.
-Los empresarios o profesionales que presten servicios que no se localicen en el territorio de aplicación del Impuesto cuando el sujeto pasivo sea el destinatario de los mismos.

– Los no residentes que operen en territorio español mediante establecimiento permanente o satisfagan en dicho territorio rentas sujetas a retención o ingreso a cuenta, así como las entidades en régimen de atribución de rentas constituidas en el extranjero con presencia en territorio español. Asimismo, los establecimientos permanentes en territorio español de las personas jurídicas o entidades no residentes deben presentar declaración de alta en el Censo de empresarios, profesionales y retenedores.

– Los socios, herederos, comuneros, o partícipes de entidades en régimen de atribución de rentas que tengan obligaciones tributarias derivadas de su condición de miembros de tales entidades.

– Los no establecidos en el territorio de aplicación del IVA que sean sujetos pasivos del mismo, excepto que hubieran resultado exonerados del cumplimiento de obligaciones censales por el Departamento de Gestión Tributaria de la Agencia Tributaria.

– En cualquier caso, mediante la declaración censal de alta las personas jurídicas y entidades en general y las personas físicas empresarios o profesionales que no dispongan de él, solicitarán el Número de Identificación Fiscal (NIF)."

La modificación de la información deberá hacerse, en general, en el plazo de un mes, a contar del siguiente en que se produzcan los cambios o antes de iniciar una nueva actividad. También hay previstos supuestos específicos.

[97] Instrucciones relativas al modelo 036 de declaración censal de alta, modificación y baja en el Censo de Empresarios, Profesionales y Retenedores: https://www.agenciatributaria.es/static_files/AEAT/Contenidos_Comunes/La_Agencia_Tributaria/Modelos_y_formularios/Declaraciones/Modelos_01_al_99/036/Instrucciones/instr_mod036.pdf

[98] Instrucciones relativas al modelo 037 de declaración censal simplificada de alta, modificación y baja en el Censo de Empresarios, Profesionales y Retenedores: https://www.agenciatributaria.es/static_files/AEAT/Contenidos_Comunes/La_Agencia_Tributaria/Modelos_y_formularios/Declaraciones/Modelos_01_al_99/037/Instrucciones/instr_mod037.pdf

A esta inscripción que debe realizarse ante la Agencia Tributaria, debe sumarse la inscripción ante el Registro Mercantil establecida por el Real Decreto-Ley 11/2018, de 31 de agosto, de transposición de directivas en materia de protección de los compromisos por pensiones con los trabajadores, prevención del blanqueo de capitales y requisitos de entrada y residencia de nacionales de países terceros y por el que se modifica la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
Deberán inscribirse en el Registro de Prestadores de Servicios, además de cumplir con otras obligaciones según cada caso concreto, los Empresarios personas físicas y a los Profesionales personas físicas, que presten los servicios señalados en el artículo 2.1.o) de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, que son:

• Constituir sociedades u otras personas jurídicas, incluyendo la transmisión de acciones o participaciones de sociedades preconstituidas que no hubieran tenido una actividad económica real.
• Ejercer funciones de dirección, de secretarios no consejeros de un Consejo de Administración, o disponer que los ejerza otra persona, incluyendo, entre otros, Gerentes y Directores Generales.
• Ejercer funciones de asesoría externa de una sociedad,
• Ejercer funciones de socio de una asociación o funciones similares en relación con otras personas jurídicas, o disponer que otra persona ejerza dichas funciones.
• Facilitar un domicilio social o una dirección comercial, postal, administrativa y otros servicios afines a una sociedad, una asociación o cualquier otro instrumento o persona jurídicos (por ejemplo, el gestor o gestora de un espacio de coworking u oficina virtual);
• Ejercer funciones de fiduciario en un fideicomiso (trust) o instrumento jurídico similar, o disponer que otra persona ejerza dichas funciones.
Ejercer funciones de accionista por cuenta de otra persona, exceptuando las sociedades que coticen en un mercado regulado de la Unión Europea y que estén sujetas a requisitos de información acordes con el Derecho de la Unión o a normas internacionales equivalentes que garanticen la adecuada transparencia de la información sobre la propiedad, o disponer que otra persona ejerza dichas funciones.

Como la misión principal del Registro Mercantil es la de dar publicidad los actos y relaciones jurídicas relativas a los sujetos que deben inscribirse en él, el mismo constituye una “fuente de acceso público”.

Este concepto ya estaba presente y bien delimitado en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales (LOPD), pero en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, General de Protección de Datos (en adelante, RGPD) sólo se menciona cuando se establece el deber de información de los responsables cuando no recogen los datos de los interesados. La Agencia Española de Protección de Datos (AEPD) se ha pronunciado al respecto para clarificar que, aunque se trate de datos accesibles por cualquiera, esto no implica necesariamente que el tratamiento sea lícito, debiendo respetarse los demás principios del RGPD[99] y por lo tanto concurrir alguna causa legitimadora del tratamiento. La AEPD, en el informe jurídico relacionado con el tratamiento de datos personales por parte de los partidos políticos[100], también ha establecido que puede aplicarse como criterio interpretativo de este concepto la definición que contenía la antigua LOPD en su artículo 3.j) según la cual eran fuentes de acceso público “aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación”, excluyendo de esta definición las fuentes cuyo

99 Diapositiva nº9 ¿Qué se entiende como fuentes de acceso público? Preguntas de los Asistentes de la 10ª Sesión anual abierta de la AEPD: https://www.aepd.es/agencia/transparencia/jornadas/common/10-sesion/9-preguntas.pdf

100 Informe del Gabinete Jurídico de la AEPD, N/REF: 210070/2018, sobre el tratamiento de datos relativos a opiniones políticas por los partidos políticos al amparo del artículo 58bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, p. 14. https://www.aepd.es/media/informes/2018-0181-tratamiento-datos-opiniones-politicas-por-partidos-polticos.pdf

“acceso está restringido a un círculo determinado, ya sea como “amigo” u otro concepto similar”.

• Apuntes sobre la cesión de datos de la Agencia Tributaria a las Cámaras de Comercio

Tras recoger los datos personales de los autónomos, la Agencia Tributaria debe cumplir no solo con las obligaciones establecidas por el RGPD y la Ley Orgánica de Protección de Datos y garantía de los derechos digitales (en adelante, LOPDGDD), pero también con las establecidas en otras normativas. Un ejemplo es la obligación que le impone el artículo 8 de la Ley 4/2014, de 1 de abril, Básica de las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación de facilitar a las Cámaras de Comercio los datos recogidos para que dichas cámaras elaboren un censo público de las empresas (personas jurídicas y físicas) que se encuentran en su jurisdicción.

“Artículo 8. Censo público.
Las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación elaborarán un censo público de empresas del que formarán parte las personas físicas o jurídicas, nacionales o extranjeras, que ejerzan las actividades comerciales, industriales, de servicios y navieras en territorio nacional, para cuya elaboración contarán con la colaboración de la administración tributaria competente así como de otras administraciones que aporten la información necesaria, garantizando, en todo caso, la confidencialidad en el tratamiento y el uso exclusivo de dicha información.
Para la elaboración del censo público de empresas las administraciones tributarias facilitarán a la Cámara Oficial de Comercio, Industria, Servicios y Navegación de España y a las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación los datos del Impuesto sobre Actividades Económicas y los censales de las empresas que sean necesarios.
Únicamente tendrán acceso a la información facilitada por la administración tributaria los empleados de cada Cámara que determine el pleno.
Esta información se empleará para la elaboración del censo público de empresas, para el cumplimiento de las funciones público-administrativas que la presente Ley atribuye a las Cámaras así como para la elaboración del censo electoral a que se hace referencia en el artículo 17 de la misma.
Dicho personal tendrá, con referencia a los indicados datos, el mismo deber de sigilo que los funcionarios de la administración tributaria. El incumplimiento de este deber constituirá, en todo caso, infracción muy grave de conformidad con su régimen disciplinario.”

• Apuntes sobre la legitimación del tratamiento

El artículo 5 del RGPD establece los principios que deben regir todo tratamiento de datos personales, uno de los cuales es el principio de “licitud, lealtad y transparencia” según el cual los datos personales serán “tratados de manera lícita, leal y transparente en relación con el interesado” (artículo 5.1.a), por lo tanto, debe existir una base jurídica que legitime el tratamiento de datos personales.

Legitimación de la Agencia Tributaria para el tratamiento y cesión de datos del censo a las Cámaras de Comercio.

El cumplimiento de obligaciones legales está expresamente previsto en el artículo 6.1.c) del RGPD, desarrollado por el artículo 8.1 de la LOPDGDD, como base jurídica que legitima el tratamiento de datos personales, la noción de tratamiento incluyendo en este caso, tanto la recogida de datos, elaboración del censo público de Empresarios, Profesionales y Retenedores y su posterior comunicación a las Cámaras de Comercio. El tratamiento por parte de la Agencia Tributaria además también estaría legitimado por el cumplimiento de misiones realizadas en interés público o ejercicio de poderes públicos, base jurídica que se encuentra prevista en el artículo 6.1.e) del RGPD y el artículo 8.2 de la LOPDGDD.

Artículo 6. Licitud del tratamiento.
“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
(…) c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
(…) 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;”

Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.
“1. EI tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.
2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.”

Legitimación de las Cámaras de Comercio para el tratamiento y cesión de datos del censo a terceras entidades.

El mismo artículo 8 de la Ley 4/2014 junto con el artículo 6.1.c) del RGPD legitimarían la recepción de los datos, así como elaboración del censo por parte de las Cámaras de Comercio.

Aun así, la cesión posterior a otras entidades, como CAMERDATA, S.A., ya no entraría dentro de este supuesto y para la cesión del censo a terceros debería disponer de otra base jurídica que legitimase dicho tratamiento.

No se encuentran previstas por Ley las comunicaciones de datos a terceras entidades privadas por parte de las Cámaras de Comercio. Así, la comunicación de datos a estas entidades no puede realizarse fundamentándose en el interés público o el ejercicio de poderes públicos de las Cámaras de Comercio (artículo 6.1.e) del RGPD) y se subscribiría dentro de sus intereses privados, debiendo legitimarse mediante otros fundamentos que lo permitan como: el consentimiento del interesado, el cumplimiento de medidas (pre-)contractuales o el interés legítimo del responsable.

Encontramos la disposición adicional décima de la LOPDGDD relativa a las comunicaciones de datos por los sujetos enumerados en el artículo 77.1 (entre los cuales pueden subsumirse las Cámaras de Comercio por ser corporaciones de derecho público, durante el ejercicio de competencias públicas, comprendidas en el artículo 77.1.g)) que dice lo siguiente:

“Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.”

Tanto durante el ejercicio de competencias públicas que le atribuya la Ley, como cuando no las ejerce, la Cámara de Comercio debería disponer del consentimiento de los interesados para ceder los datos a terceros o considerar que prima el interés legítimo de los mismos[101] **sobre los derechos, libertades e intereses de los afectados, siendo su responsabilidad la de**

[101]No nos estamos refiriendo al interés legítimo del responsable del tratamiento, es decir, la Cámara de Comercio en tanto que Administración Pública, porque es de aplicación la exclusión prevista en el último inciso del artículo 6.1 del RGPD: Lo dispuesto en la letra f) no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. De este modo lo explica la AEPD en el Informe 0050/2019

demostrar que prevalecen uno a los otros:

Artículo 6. Licitud del tratamiento.
"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
(…) 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."

Considerando (69) "En los casos en que los datos personales puedan ser tratados lícitamente porque 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 o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado."

Para valorar si prima el interés legítimo de los sujetos de derecho privado por encima de los derechos e intereses de los autónomos, la Cámara de Comercio debe tener en cuenta las previsiones del **artículo 6.1.f), y del considerando 47 del RGPD.**

Considerando (47) "El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo."[102]

Para facilitar la tarea de llevar a cabo la ponderación entre los derechos del interesado y los intereses del responsable, la Information Commissioner's Office (ICO), la Autoridad de Protección de Datos del Reino Unido, publicó un test de tres partes, basándose en la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de mayo de 2017, Rigas C-13/16[103],

(https://www.aepd.es/es/documento/2019-0050.pdf) y 0175/2018 (https://www.aepd.es/es/documento/2018-0175.pdf). Nos referimos al interés legítimo del tercero que se relaciona con ella.

[102] La AEPD analiza los criterios interpretativos del RGPD en relación con el interés legítimo en el caso de comunicaciones comerciales electrónicas en su Informe 0173/2018, disponible en:
https://www.aepd.es/es/documento/2018-0173.pdf

que evalúa[104]:

• *Purpose test*: La finalidad del tratamiento, cuestionándose si hay un interés legítimo que lo ampare.
• *Necessity test*: La necesidad del tratamiento, cuestionándose si el tratamiento de datos personales es necesario para la finalidad prevista
• *Balancing test*: La valoración sobre si el interés legítimo del tratamiento prevalece sobre los intereses, derechos y libertades del interesado.

Para evaluar estas tres partes, y facilitar aún más la tarea, la ICO elaboró un cuestionario[105], [106] en el que se tiene en cuenta, entre otras cosas:

• La existencia de beneficios públicos,
• El impacto si no se realiza el tratamiento,
• Si se cumplen la normativa de protección de datos y otras leyes aplicables,
• Si hay problemas éticos con el tratamiento,
• Si el tratamiento pudiera realizarse de otra manera más obvia o menos intrusiva,
• Si son datos de categorías especiales o datos profesionales,
• Si existe una relación con el interesado o se han obtenido de otra fuente,
• Si hace tiempo que fueron recogidos,
• Si el interesado puede prever que se realizará dicho tratamiento,
• Cuáles pueden ser los posibles impactos del tratamiento,
• Si los interesados perderán el control sobre el uso de sus datos y pueden considerar que el tratamiento es intrusivo.
• Si el responsable del tratamiento estaría dispuesto a explicar el tratamiento de datos que se realiza a los interesados.

En este caso, la Cámara de Comercio parece haber considerado que el interés legítimo de CAMERDATA y otras terceras entidades prima por encima de los derechos e intereses de los autónomos. En nuestra opinión, es lesivo para los derechos fundamentales el uso masivo y no debidamente justificado ni, como se verá más adelante, informado que se está haciendo del concepto de "interés legítimo" incluido en el RGPD. A menudo se utiliza como "cajón de sastre" cuando no saben qué base jurídica es aplicable o cuando ninguna lo es.

En este caso, no podemos estar de acuerdo con la valoración que parece haber hecho la Cámara de Comercio ya que, al inscribirse en el censo de la Agencia Tributaria, los autónomos no pueden prever que sus datos serán comunicados a la Cámara de Comercio y luego a terceras entidades que las utilizaran para su propio beneficio, como se verá más adelante. Por otra parte, si consideramos que algunos de los datos proporcionados a la Agencia Tributaria son, además de profesionales, personales, como direcciones (sobre todo en el caso de los autónomos que trabajan desde casa) o teléfonos, el tratamiento sucesivo por estas entidades y su difusión pública puede considerarse como intrusivo, sobre todo por parte de las terceras empresas que se lucran con la publicación y venta de estos datos. Finalmente, y como se verá más adelante, debe tenerse en cuenta que ni las Cámaras de Comercio, ni los terceros parecen dispuestos a

[103] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1515682033041&uri=CELEX:62016CJ0013

[104] "What is the three-part test?" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/#marketing_activities

[105] https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx

[106] Traducción al español por parte de Marcos Rubiales Olmedo: https://media.licdn.com/dms/document/C4D1FAQE3vKRhZY0DlA/feedshare-document-pdf-analyzed/0?e=1569060000&v=beta&t=9JvxY-fpdF4_rQw7AtFgDR5GOM06YuD1ljg8gohIGOE

informar correctamente a los autónomos de esta comunicación de datos ni para qué son tratados factor que influye en la pérdida de control sobre sus datos. Vemos, por lo tanto, serios problemas éticos con el tratamiento de datos que será realizado por terceras entidades.

Además, debemos recordar el Informe 2018/175 de la AEPD[107], que en el caso de cesiones de datos entre administraciones públicas y citando la jurisprudencia del Tribunal Constitucional concluía que "el acceso deberá ser siempre "específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo e indiscriminado"; "tal acceso sólo podría producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen General que le resulte de aplicación."(STC 19/2013, FJ 7º)", debiendo la cesión de datos entre Administraciones Públicas "regirse por las normas generales previstas en el RGPD, y en concreto cabe fijarse en este momento en los artículos 5.1, letra b); 6.2, 6.3 y 6.4 RGPD."

Legitimación de CAMERDATA

Como hemos visto, CAMERDATA S.A. aparece como referencia directa desde el censo de empresarios de la Cámara de Comercio para obtener más información sobre empresas y autónomos.

En su página web, cuando informa sobre el tratamiento de los datos que no han sido obtenidos del interesado[108], indica en el apartado denominado como "legitimidad del tratamiento":

"Este tratamiento se realiza sobre datos que han sido obtenidos de un Censo oficial elaborado por organismo público, y la persona sujeto pasivo de los datos (el interesado) o ejerce una actividad de las recogidas en el Real Decreto de 2007 (RD 475/ 2007) o ejerce un cargo de responsabilidad que aparece publicado en el registro mercantil, sin la necesidad de obtener su consentimiento previo, en base al interés legítimo en conocer esta información que requieren los Clientes de CAMERDATA, habilitado en el artículo 6.1 f del RGPD, y en el Considerando 47 del RGPD, dado que la finalidad pretendida por nuestros clientes es la realización de campañas de comunicaciones comerciales y de marketing, ofreciendo diferentes bienes o servicios que pudieran ser de su interés. En otros casos, la legitimidad del tratamiento de estos datos por parte de los Clientes de CAMERDATA, puede corresponder a los supuestos previstos en las letras b) o c) del artículo 6.1 del RGPD."

Así, también CAMERDATA antepone de facto el interés de sus clientes a los derechos, libertades e intereses de los autónomos cuya información personal les vende.
Tanto el considerando 47 del RGPD como la ICO indican que el tratamiento relativo al marketing directo puede estar legitimado por los intereses legítimos[109], pero no siempre el marketing directo constituirá un interés legítimo, dependiendo de las circunstancias del caso concreto. Deberá realizarse una ponderación entre los derechos del interesado y los intereses del responsable para determinar si el tratamiento por parte de los clientes en este caso está, o no, legitimado.
Si respecto a la comunicación de datos de la Cámara de Comercio a CAMERDATA hemos considerado que el interés legítimo no se encontraba justificado, en este caso tampoco.

---

[107] AEPD. Informe 2018/0175, página 19. Disponible en: https://www.aepd.es/es/documento/2018-0175.pdf

[108] "En Camerdata cumplimos con el RGPD" https://www.camerdata.es/faq

[109] "Can we use legitimate interests for our marketing activities?" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/#marketing_activities

También la ICO, cuando considera el contacto entre contactos de empresas dice claramente que es posible que el interés legítimo pueda justificar el tratamiento pero que no hay una regla absoluta, y deberá también realizarse una ponderación.

En lo que respecta al tratamiento por parte de los clientes de CAMERDATA, además de la manca de interés legítimo para el tratamiento de los datos que realicen y haciendo referencia a la mención por CAMERDATA de campañas de marketing, si las mismas se realizan a través de medios electrónicos, también deberá tenerse en cuenta el artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE):

Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes
"1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.
2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.
En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija. (…)"

Adicionalmente, cabe destacar el artículo 19 de la actual LOPDGDD, en la que se establece la facultad de tratar datos personales relativos a empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición, se limiten a los datos mínimos e imprescindibles para su localización profesional (en cumplimiento del principio de minimización) y no se traten para entablar una relación con los mismos como personas físicas, sino sólo para mantener relaciones jurídicas en el entorno profesional, requisitos que en el caso del tratamiento por parte de terceras entidades que obtienen los datos del Registro Mercantil y de la Agencia Tributaria no están reflejados en la ley, al no estar incluida la difusión de estos datos.

Artículo 19. Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.
"1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:
a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.
b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.
2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas."

Este artículo ha sido introducido en la LOPDGDD para mantener el statu quo del artículo 2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que fue el fundamento de diversas resoluciones de la AEPD[110], pero no se fundamenta en ninguna disposición prevista en el RGPD, el cual NO excluye de su ámbito de aplicación los datos

[110] Un ejemplo de resolución de la AEPD en que desestima el ejercicio de derechos en base al artículo 2.2 del RDLOPD porque "los datos publicados se refieren a la reclamante en su calidad de médico, es decir, en su actividad profesional, consistente únicamente en su nombre y apellidos, las

profesionales.

Artículo 2 (Real Decreto 1720/2007). Ámbito objetivo de aplicación
"(…) 2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal. (…)"

Artículo 2 (RGPD). Ámbito de aplicación material
"1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:
a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención. (…)"

Artículo 2 (LOPDGDD). Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94
"(…) 2. Esta ley orgánica no será de aplicación:
a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.
b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.
c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas. (…)"

• Apuntes sobre la finalidad del tratamiento

El artículo 5 del RGPD sobre los principios que deben regir todo tratamiento de datos personales, establece, además del principio de "licitud, lealtad y transparencia" el principio de "limitación de la finalidad" según el cual los datos personales serán "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1 del RGPD, "el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se

funciones o puestos desempeñados en su actividad profesional de una empresa, es decir respecto de la que no se aplica la normativa de protección de datos", aún tratarse de un caso en que los datos a los que se hacía referencia eran erróneos:
https://www.aepd.es/resoluciones/REPOSICION-TD-00546-2018_ORI.pdf

considerará incompatible con los fines iniciales” **(artículo 5.1.b) RGPD)**. De acuerdo con este principio, **los datos podrán recabarse para cumplir cualquier finalidad que no pudiese realizarse sin recabarlos, debiendo tratarse de una finalidad determinada y no genérica, explícita y no confusa, y legítima**.

Como hemos podido observar, la finalidad de tratamiento de los datos de los autónomos por parte de la Agencia Tributaria, la finalidad de la cesión de estos datos a las Cámaras de Comercio y el posterior tratamiento por parte de estas últimas se encuentran establecidas por ley:

• En el primer caso, la Agencia Tributaria recoge los datos de los autónomos para elaborar el Censo de Empresarios, Profesionales y Retenedores que forma parte del Censo de Obligados Tributarios.
• En el segundo y tercer casos, la finalidad de la cesión y las distintas finalidades de tratamiento de los datos se encuentran recogidas en el artículo 8 de la Ley 4/2014:

“Para la elaboración del censo público de empresas las administraciones tributarias facilitarán a la Cámara Oficial de Comercio, Industria, Servicios y Navegación de España y a las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación los datos del Impuesto sobre Actividades Económicas y los censales de las empresas que sean necesarios. Únicamente tendrán acceso a la información facilitada por la administración tributaria los empleados de cada Cámara que determine el pleno.
Esta información se empleará para la elaboración del censo público de empresas, para el cumplimiento de las funciones público-administrativas que la presente Ley atribuye a las Cámaras así como para la elaboración del censo electoral a que se hace referencia en el artículo 17 de la misma.”

Así, siguiendo las indicaciones del artículo 6.3 y considerando 45 del RGPD y del artículo 8.2 de la LOPDGDD las finalidades del tratamiento por parte de la Agencia Tributaria y de las Cámaras de Comercio se encuentran establecidas por ley, pero no se encuentran previstas por Ley las comunicaciones de datos a terceras entidades privadas por parte de las Cámaras de Comercio. Así, las Cámaras de Comercio realizan un tratamiento de datos cuya finalidad es distinta de la que inicialmente está prevista.

El tratamiento posterior de los datos con otras finalidades está previsto por el RGPD el cual indica que no pueden utilizarse los datos para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. Al respecto, el Tribunal Constitucional ya utilizaba como equivalente al término ”incompatible” el término “distinto”, en la STC 94/1998, de 4 de mayo[111], citando la STC 254/1993, de 20 de julio[112], según las cuales:

STC 94/1998, de 4 de mayo, FJ 4º:
“La STC 254/1993 declaró que el art. 18.4 C.E. incorpora un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad. La garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (fundamento jurídico 7.o).

STC 254/1993, de 20 de julio, FJ 7º:
“ (…) En este sentido, las pautas interpretativas que nacen del convenio de protección de datos personales de 1981 conducen a una respuesta inequívocamente favorable a las tesis del demandante de amparo. La realidad de los problemas a los que se enfrentó la elaboración y la ratificación de dicho tratado internacional, así como la experiencia de los países del Consejo de Europa que ha sido condensada en su articulado, llevan a la conclusión de que la

[111] http://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1998-13334.pdf

[112] http://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1993-21425.pdf

protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones Públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades.
Los argumentos que esgrime el Abogado del Estado en contra de este juicio no son convincentes. Si, como acepta dialécticamente en sus alegaciones, el derecho fundamental a la intimidad puede justificar en determinados casos que un ciudadano se niegue a suministrar a las autoridades determinados datos personales, no se ve la razón por la que no podría justificar igualmente que ese mismo ciudadano se oponga a que esos mismos datos sean conservados una vez satisfecho o desaparecido el legítimo fin que justificó su obtención por parte de la Administración o a que sean utilizados o difundidos para fines distintos, y aun ilegales o fraudulentos, o incluso a que esos datos personales que tiene derecho a negar a la Administración sean suministrados por terceros no autorizados para ello.
Toda la información que las Administraciones Públicas recogen y archivan ha de ser necesaria para el ejercicio de las potestades que les atribuye la Ley, y ha de ser adecuada para las legítimas finalidades previstas por ella, como indicamos en la STC 110/1984, especialmente fundamentos 3º y 8º, pues las instituciones públicas, a diferencia de los ciudadanos, no gozan del derecho fundamental a la libertad de expresión que proclama el art. 20 C.E. (…).”

En concreto, el artículo 6.4 y el considerando 50 del RGPD establecen que sólo podrán tratarse los datos cuando el tratamiento posterior de los mismos sea compatible con los fines de su recogida inicial, teniendo en cuenta el contexto de recogida de los datos y la naturaleza de los mismos, la relación del interesado con el responsable del tratamiento y las expectativas razonables del interesado respecto al tratamiento de sus datos. **Así, si el interesado no puede prever que sus datos serán tratados más tarde para cumplir con una finalidad distinta el tratamiento posterior de sus datos no sería compatible con los fines de la recogida inicial, como en el caso de los autónomos, y no debería llevarse a cabo**, y más teniendo en cuenta que una vez que el tratamiento ha perdido su finalidad originaria, los datos deben ser devueltos o destruidos y no está permitida su reutilización o tratamiento para otras actividades.

Artículo 6. Licitud del tratamiento.
“4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.”

Considerando (50) “El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si 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, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación

científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.
Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.”

La finalidad del tratamiento de los datos personales debe ser específica pero también conocida por el interesado al momento de proporcionar sus datos o, como veremos, al momento en que sus datos lleguen a manos de un tercero que deba tratarlos, o en el momento en que el responsable quiera tratarlos para fines distintos de los iniciales. El interesado, en este caso el autónomo, sólo podrá conocer la finalidad específica, o las finalidades específicas, del tratamiento de los datos que proporciona mediante la información que le sea proporcionada por el responsable del tratamiento.

• Apuntes sobre la información que debe proporcionarse a los interesados

Un tratamiento no debe cumplir solamente con los principios y obligaciones analizados hasta el momento, sino que es necesario cumplir con el resto de requisitos establecidos en la normativa de protección de datos. Como se ha visto, el artículo 5 del RGPD sobre los principios que deben regir todo tratamiento de datos personales, establece, además del principio de “licitud, lealtad y transparencia”. **La vertiente de transparencia de este principio se refiere en gran parte a la información de qué deben disponer los interesados cuando sus datos personales van a ser objeto de tratamiento**, a la cual hacía ya referencia, en relación con el tratamiento por parte de Administraciones Públicas, **la Sentencia del Tribunal Constitucional 254/1999, de 20 de julio, en su Fundamento Jurídico 7º**[113]:

“(…) Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 C.E., y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente (STC 11/1981, fundamento jurídico 8º, y 101/1991, fundamento jurídico 2º).”

113 http://hj.tribunalconstitucional.es/docs/BOE/BOE-T-1993-21425.pdf

El artículo 12 y considerandos 39 y 58 del RGPD concretan este principio y establecen que esta información debe permitir que el interesado sepa y comprenda cual es la finalidad del tratamiento y los datos que se recogen, además de informar sobre la identidad del responsable. La información a los interesados, como cuando se informa a consumidores y usuarios, debe ser gratuita, clara, transparente, accesible y fácil de entender, utilizando un lenguaje sencillo, pudiendo utilizar incluso iconos, y el RGPD incide en ello.

Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.
"1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.
(…) 5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito.
(…) 7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. (…)"

Considerando (39) "Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento."

Considerando (58) "El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en

línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender."

Los artículos 13 y 14 del RGPD establecen respectivamente la información mínima que debe proporcionarse a los interesados según si los datos personales los proporciona directamente el interesado (artículo 13) o si los datos son obtenidos de terceras fuentes (artículo 14), siendo precisados por los considerandos 60, 61 y 62 del mismo RGPD.

ARTÍCULO 13	AMBOS	ARTÍCULO 14
El motivo por el que el interesado debe facilitar los datos: requisito legal o (pre-)contractual, si está obligado a facilitarlos y las consecuencias en caso de no facilitarlos.	La identidad y datos de contacto del responsable del tratamiento, y su representante si corresponde. Los datos de contacto del delegado de protección de datos si el responsable debe nombrarlo. La finalidad o finalidades del tratamiento. La base o bases jurídicas que legitiman el tratamiento. Si la base jurídica sean los intereses legítimos del responsable o de un tercero deberán explicarse también. Los destinatarios de los datos o categorías de destinatarios de los datos recogidos. La intención de realizar transferencias de datos a terceros países u organizaciones fuera de la Unión Europea y las garantías de seguridad de dicha transferencia: si existe o no decisión de adecuación de la Comisión o si se han tomado garantías adecuadas o apropiadas. El plazo de conservación de los datos personales o los criterios utilizados para determinarlo. Los derechos de qué dispone el interesado respecto sus datos personales: acceso, rectificación, supresión, oposición, limitación y portabilidad, así como el derecho a retirar el consentimiento en caso de fundamentarse el tratamiento de los datos en este y el derecho a presentar una reclamación ante la autoridad de protección de datos que corresponda. Si el tratamiento consiste a tomar decisiones automatizadas o la elaboración de perfiles, debe informarse sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.	Las categorías de datos personales de que se trate. La fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

El artículo 11 de la LOPDGDD permite reducir la información que se proporciona y aplicar un modelo de "información por capas" que las Agencias y Autoridades de Protección de Datos de España ya han concretado mediante una "guía para el cumplimiento del deber de informar"[114].

Artículo 11. Transparencia e información al afectado
"1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

[114] https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:
a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquél la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
En estos supuestos, la información básica incluirá también:
a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos."

El objetivo de este modelo es proporcionar sólo información considerada como básica en un primer lugar para dirigir al interesado que quiera más información a un segundo nivel de información dónde pueda encontrar la información requerida por el RGPD.

La guía de las Autoridades y Agencias lo expone del siguiente modo en su página 5:

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

En cuanto al momento en que debe proporcionarse la información, varía según las circunstancias de la recogida de la información y de utilización de los datos:

ARTÍCULO 13	AMBOS	ARTÍCULO 14
Debe facilitarse la información en el momento de obtener los datos personales.		Debe facilitarse la información dentro de un "plazo razonable" desde la obtención de los datos, y como máximo en el plazo de un mes, o cuando los datos tengan que utilizarse para comunicarse con el interesado, a más tardar en el momento de la primera comunicación con el mismo, o si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que se comuniquen por primera vez.
	La información no deberá facilitarse si el interesado ya dispone de la misma.	La información no deberá facilitarse cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado. Por ejemplo, cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas. La información no deberá facilitarse cuando informar pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. El responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información. La información no deberá facilitarse cuando la obtención o la comunicación de los datos esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado. La información no deberá facilitarse cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.
	Deberá informarse ulteriormente al interesado cuando quieran tratarse los datos recogidos para un fin distinto de las previstas, y antes de llevarlo a cabo, proporcionándole información sobre dicha finalidad y otra información adicional que el responsable considere pertinente.	

Tras conocer los requisitos informativos que deben cumplir los responsables del tratamiento en cada caso, es preciso analizar si se

cumplen dichas obligaciones en el caso de las sucesivas transmisiones de los datos personales de los autónomos desde que se inscriben en el Censo de Empresarios, Profesionales y Retenedores de la Agencia Tributaria hasta que su información es divulgada por terceras entidades privadas que puede que ni conozcan e indexada por los motores de búsqueda.

Información proporcionada por la Agencia Tributaria

La Agencia Tributaria es quien recoge los datos de las y los autónomos, y, por lo tanto, **debe informar** según lo previsto en el artículo 13 del RGPD en el momento mismo de la recogida de los datos, es decir, **en el momento en que se realiza la declaración de alta en el Censo** de Empresarios, Profesionales y Retenedores mediante los formularios 036 y 037 disponibles en el siguiente enlace:
https://www.agenciatributaria.gob.es/AEAT.sede/procedimientoini/G322.shtml

En el mismo encontramos más enlaces que nos dirigen, entre otras, a las páginas que seguramente consultan más los autónomos cuando realizan este trámite:

• de ayuda para la cumplimentación del formulario de forma telemática.
• de cumplimentación del formulario 036[115] y 037[116] para su posterior impresión.
• de información general sobre la presentación de los formularios[117], donde a su vez se encuentran:

◦ las instrucciones para realizar la declaración censal mediante el modelo 036[118].
◦ las instrucciones para realizar la declaración censal mediante el modelo 037[119].

• de información sobre la normativa aplicable, guías y manuales[120] para hacer la declaración censal, donde a su vez se encuentran:

◦ la orden HAC/1416/2018, de 28 de diciembre, por la que modifica (…) la Orden EHA/1274/2007, de 26 de abril, por la que se aprueban los modelos 036 de Declaración censal de alta, modificación y baja en el censo de empresarios, profesionales y retenedores y 037 de Declaración censal simplificada de alta, modificación y baja en el censo de empresarios, profesionales y retenedores (…)[121].
◦ la guía práctica de la declaración censal de alta, modificación y baja en el censo de empresarios, profesionales y retenedores, actualizada el mes de enero de 2019.[122]

En ninguno de los enlaces consultados encontramos información relacionada con la protección de los datos personales de quienes se inscriben en el mencionado censo.

[115] https://www2.agenciatributaria.gob.es/static_files/common/internet/dep/aplicaciones/ov/i903600b.html

[116] https://www2.agenciatributaria.gob.es/static_files/common/internet/dep/aplicaciones/ov/i803700b.html

[117] https://www.agenciatributaria.es/AEAT.internet/G322/informacion.shtml

[118] https://www.agenciatributaria.es/static_files/Sede/Procedimiento_ayuda/G322/instr_mod036.pdf

[119] https://www.agenciatributaria.es/static_files/Sede/Procedimiento_ayuda/G322/instr_mod037.pdf

[120] https://www.agenciatributaria.es/AEAT.internet/G322/normativa.shtml

[121] https://www.boe.es/buscar/doc.php?id=BOE-A-2018-17996

[122] https://www.agenciatributaria.es/static_files/Sede/Procedimiento_ayuda/G322/Guia_censal.pdf

La información sobre protección de datos personales se encuentra dividida en distintos sitios de la página web:

– **El** aviso legal, el cual contiene la política de privacidad, remite a otro enlace que denomina "ayuda tratamiento de datos personales"[123]– dónde se proporciona acceso a información general sobre protección de datos y a normativa, guías y manuales.

Es en la información general[124] sobre protección de datos donde a su vez, encontramos la "información al interesado sobre protección de datos[125]". Es aquí donde los autónomos podrán encontrar información sobre el tratamiento de sus datos personales una vez que los proporcionan a la Agencia Tributaria, concretamente, una vez entren en el apartado de "información detallada", **y aún más concretamente en el "5. Registro de las actividades de tratamiento"**[126] (accesible desde los puntos 3.3, 3.4, 3.5, 3.6 y 3.7 de la página de "información detallada"), **que dedica su punto 5.42. al Censo de actividades económicas**[127], donde indica como destinatarios de los datos, entre otros, las "Cámaras de comercio, industria y navegación".

– También encontramos un apartado denominado "datos personales"[128] en el pie de la página web, que contiene información muy genérica sobre el tratamiento de datos por parte de la Agencia Tributaria. Para mayor concreción, debe accederse al enlace "información al interesado sobre protección de datos"[129], que dirige al mismo enlace que el accesible desde la "ayuda tratamiento de datos personales" del aviso legal, o directamente al registro de las actividades de tratamiento.

En conclusión, **no se cumple debidamente con el deber de información de acuerdo con el artículo 13 del RGPD en lo referido al tratamiento de datos personales de los autónomos , al encontrarse la información esparcida por la página** web y al hecho de que no encontramos cláusulas informativas específicas sobre este tratamiento, ni incluso información básica en una primera capa que nos dirija a información más concreta, y tenemos que dirigirnos hasta el Registro de Actividades de Tratamiento para poder acceder a dicha información.

Información proporcionada por la Cámara de Comercio de España

El artículo 8 de la Ley 4/2014 establece que las administraciones tributarias facilitaran los datos del Impuesto sobre Actividades Económicas y los censales que sean necesarios para que las Cámaras de Comercio elaboren un censo público de empresas que ejerzan actividades comerciales, industriales, de servicios y navieras en territorio nacional. **Al estar la comunicación de datos prevista por Ley, las Cámaras de Comercio pueden aplicar la excepción al deber de**

[123] https://www.agenciatributaria.gob.es/AEAT.sede/Ayuda/FZ08.shtml

[124] https://www.agenciatributaria.es/AEAT.internet/FZ08/informacion.shtml

[125] https://www.agenciatributaria.es/AEAT.internet/FZ08/informacion/interesado.shtml

[126] https://www.agenciatributaria.es/AEAT.internet/Inicio/Ayuda/Modelos__Procedimientos_y_Servicios/Ayuda_P_FZ08___Tratamiento_de_datos_personales/Informacion_general/_Ayuda_Informacion_al_interesado_sobre_proteccion_de_datos/5__Registro_de_las_actividades_de_tratamient/5__Registro_de_las_actividades_de_tratamiento.html

[127] https://www.agenciatributaria.es/AEAT.internet/Inicio/Ayuda/Modelos__Procedimientos_y_Servicios/Ayuda_P_FZ08___Tratamiento_de_datos_personales/Informacion_general/_Ayuda_Informacion_al_interesado_sobre_proteccion_de_datos/5__Registro_de_las_actividades_de_tratamiento/5_42__Censo_de_actividades_economicas/5_42__Censo_de_actividades_economicas.html

[128] https://www.agenciatributaria.gob.es/AEAT.sede/Inicio/_pie_/_Datos_personales_/_Datos_personales_.shtml

[129] https://www.agenciatributaria.es/AEAT.internet/FZ08/informacion/interesado.shtml

información prevista por el artículo 14 del RGPD según la cual no deben informar a los interesados cuando la obtención o la comunicación de los datos que no recogen de los interesados está expresamente establecida por el Derecho de los Estados Miembros. Siguiendo este precepto, **la Cámara de Comercio de España no informa ni en el** Censo Nacional de Empresas[130] ni en su política de privacidad[131] sobre el tratamiento de datos personales de los autónomos.

Aun así, el legislador debió cuestionarse la constitucionalidad de la previsión de esta cesión porque la redacción del artículo 14.5.c) del RGPD es la siguiente:

"5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:
(…) c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, (…)"

El derecho nacional, cuando establece una comunicación de datos personales debe prever las medidas adecuadas aplicables para proteger los intereses legítimos del interesado[132], pero el artículo 8 de la Ley 4/2014 prevé como única medida para proteger los intereses de los interesados guardar la confidencialidad de los datos y que el personal de las Cámaras de Comercio que tenga acceso a la información facilitada por la Agencia Tributaria tendrá el mismo deber de sigilo que los funcionarios de esta administración.

Viendo que los datos personales comunicados a las Cámaras de Comercio, recogidos para el cumplimiento por parte de los autónomos de obligaciones legales, constituyen el negocio de algunas entidades privadas mediante su publicación y difusión, parece que nos encontramos ante un posible incumplimiento de las condiciones de confidencialidad establecidas por la Ley. El legislador debería limitar estas posibilidades de negocio por parte de las Cámaras de Comercio y de terceros modificando la Ley 4/2014 para incluir la aplicación de más garantías con el objetivo de proteger los derechos e intereses de los autónomos cuyos datos son vendidos sin que puedan tener control sobre su difusión, sobre todo en el caso de aquellos autónomos cuyos datos profesionales coinciden con los personales, cuya información personal, como la dirección de su domicilio, no debería ser objeto de difusión sin su consentimiento ni conocimiento.

Información proporcionada por CAMERDATA

La excepción anterior no se aplica a CAMERDATA, S.A ni a terceras entidades que reciban los datos tratados por la Cámara de Comercio, por lo tanto, **estas empresas deberían cumplir con lo establecido en el artículo 14 del RGPD, es decir, informar del tratamiento de sus datos a los autónomos dentro de un plazo razonable desde que los obtienen y como máximo en el plazo de un mes.**

Para informar a los autónomos cuyos datos son vendidos, CAMERDATA lo hace a través de su aviso legal[133], en cuyo apartado sexto incluye toda la "información sobre el tratamiento de los datos (FEE y productos comercializados) no

[130] https://censo.camara.es/

[131] https://www.camara.es/legal-y-privacidad

[132] Fue uno de los principales argumentos de inconstitucionalidad del apartado 1 del artículo 58bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado a esta por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, se encuentra en el fundamento jurídico nº8 de la Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo:
"Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales. (…) "

[133] https://www.camerdata.es/avisoLegal

obtenidos del interesado, relativos a marketing y publicidad", indicando como base jurídica una vez más el interés legítimo de sus clientes de conocer la información para realizar "campañas de comunicaciones comerciales y marketing", siendo la finalidad la misma.

La información no se proporciona entonces individualmente a cada autónomo porque CAMERDATA debe haber considerado que proporcionar la información a través del aviso legal constituye una medida adecuada para proteger los derechos, libertades e intereses de los interesados y es de aplicación la excepción al deber de información del **artículo 14.5.b) del RGPD y del considerando 62** según los cuales:

Artículo 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.
"(…) 5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:
(…) b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;"

Considerando (62) "Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas."

El principal problema que nos encontramos con la aplicación del apartado 5 del artículo 14 del RGPD es que no hay aún interpretación expresa por parte de la AEPD, de acuerdo con el RGPD, de la aplicación de esta excepción y de lo que considera como "esfuerzo desproporcionado". Sin embargo, la AEPD sancionó la Mancomunidad de Pamplona por incumplir el artículo 14 del RGPD, obligándola al envío a las personas afectadas de comunicaciones informativas sobre protección de datos personales[134]. La ICO ha establecido que el responsable debe realizar y documentar una evaluación de la situación analizando si el esfuerzo que implica proveer a los individuos con la información es proporcional con las consecuencias que el tratamiento por parte del responsable, CAMERDATA en este caso, puede tener sobre ellos. Cuanto más significantes son las consecuencias menos puede confiarse en la aplicación de esta excepción, que debe ser interpretada de forma restrictiva para que no se convierta en la norma general.[135]

No podemos compartir la interpretación supuestamente realizada por CAMERDATA ya que disponiendo de las direcciones de los autónomos no consideramos un esfuerzo desproporcionado comunicarles que sus datos son objeto de tratamiento y que disponen de ciertos derechos, como el derecho de oposición, supresión y limitación del tratamiento (artículos 17, 18, 21 del RGPD y 15,16, 18 de la LOPDGDD) para que los mismos puedan controlar el uso de sus datos por parte de terceros a quienes no les han proporcionado dichos datos.

Además, el considerando 70 del RGPD establece claramente que debe comunicarse explícitamente al interesado, al margen de cualquier otra información, que tiene derecho de oponerse al tratamiento de sus datos personales cuando

[134] Resolución Procedimiento Nº: PS/00201/2019 de 4 de junio de 2020, disponible en: https://www.aepd.es/es/documento/ps-00201-2019.pdf

[135] When can we rely on disproportionate effort?
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/#id4

sean tratados con fines de mercadotecnia directa (finalidad indicada en el aviso legal de CAMERDATA cuanto a la justificación del interés legítimo del tratamiento de los datos: “la finalidad pretendida por nuestros clientes es la realización de campañas de comunicaciones comerciales y de marketing, ofreciendo diferentes bienes o servicios que pudieran ser de su interés”):

Considerando (70) “Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información.”

En este sentido, cabe recordar que el responsable del tratamiento está obligado a eliminar los datos y conceder el derecho de oposición a los interesados, salvo cuando acredite motivos legítimos imperiosos que prevalezcan sobre los intereses, derechos y libertades de los interesados, y que toda rectificación, supresión o limitación deberá comunicarse a cada uno de los destinatarios a los que se hayan comunicado los datos para que realicen la misma acción que el responsable de acuerdo con el artículo 19 del RGPD:

Artículo 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.
El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

• Conclusión

Tradicionalmente, el derecho a la protección de datos se ha configurado como un derecho de control sobre el uso y destino de los datos personales,[136]que debe ser respetado tanto por entes privados como públicos. Además, el RGPD establece en su artículo 25 el **principio de privacidad desde el diseño y por defecto**, que debe tenerse en cuenta, tanto en la concepción de un tratamiento de datos personales como en su desarrollo.

En el presente informe hemos constatado que los datos que los autónomos deben proporcionar obligatoriamente a las administraciones pasan a formar parte de “fuentes de acceso público”, tales como el Registro Mercantil cuya misión principal es dar publicidad los actos y relaciones jurídicas relativas a los sujetos que deben inscribirse en él y el Censo Público de empresas elaborado por parte de las Cámaras de Comercio.

Xnet entiende que para el bien de la transparencia deban proporcionarse estos datos pero no está conforme con la posterior publicación y venta de los mismos cuando estos coinciden con los datos personales del interesado y circunstancia donde no dispone de una sede diferente de su domicilio para llevar a cabo la actividad profesional, muchas veces porque no dispone de los ingresos suficientes para tenerlos.

Además, para que las y los autónomos recuperen el poder de control sobre sus datos personales ab initio y no deban

[136] STC 292/2000, en su Fundamento Jurídico 6º define el derecho a la protección de datos como aquel derecho que “garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen y con qué fin.”

ejercer los derechos de oposición y supresión de forma constante, **es necesario que por defecto** no **se realicen las comunicaciones de datos a las terceras entidades que se han descrito** y que solo puedan llevarse a cabo cuando los autónomos decidan, de forma expresa en el momento en que proporcionan la información a la Agencia Tributaria, si quieren que estos datos puedan ser objeto de venta en un futuro.

Finalmente, como se ha comentado en informes anteriores, es imperativo que se respeten los principios esenciales previstos por la normativa de protección de datos, tales como el deber de información y el principio de licitud, concretando en qué casos concretos y restrictivos se aplican las excepciones al primero, y prever cuando los intereses legítimos de las empresas constituyen un fundamento válido para el tratamiento de datos personales.

2. LISTADO DE LEGISLACIÓN Y ARTÍCULOS RELEVANTES

Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional quinta. Declaraciones censales.
1. Las personas o entidades que desarrollen o vayan a desarrollar en territorio español actividades empresariales o profesionales o satisfagan rendimientos sujetos a retención deberán comunicar a la Administración tributaria a través de las correspondientes declaraciones censales su alta en el Censo de Empresarios, Profesionales y Retenedores, las modificaciones que se produzcan en su situación tributaria y la baja en dicho censo. El Censo de Empresarios, Profesionales y Retenedores formará parte del Censo de Obligados Tributarios. En este último figurarán la totalidad de personas físicas o jurídicas y entidades a que se refiere el artículo 35 de la Ley General Tributaria, identificadas a efectos fiscales en España.

Las declaraciones censales servirán, asimismo, para comunicar el inicio de las actividades económicas que desarrollen, las modificaciones que les afecten y el cese en las mismas. A efectos de lo dispuesto en este artículo, tendrán la consideración de empresarios o profesionales quienes tuvieran tal condición de acuerdo con las disposiciones propias del Impuesto sobre el Valor Añadido, incluso cuando desarrollen su actividad fuera del territorio de aplicación de este impuesto.

2. Reglamentariamente se regulará el contenido, la forma y los plazos para la presentación de estas declaraciones censales.

3. La declaración censal de alta en el Censo de Empresarios, Profesionales y Retenedores contendrá, al menos la siguiente información:
a) El nombre y apellidos o razón social del declarante.
b) El número de identificación fiscal si se trata de una persona física que lo tenga atribuido. Si se trata de personas jurídicas o entidades del apartado 4 del artículo 35 de la Ley General Tributaria, la declaración de alta servirá para solicitar este número, para lo cual deberán aportar la documentación que se establezca reglamentariamente y completar el resto de la información que se relaciona en este apartado. De igual forma procederán las personas físicas sin número de identificación fiscal que resulten obligadas a la presentación de la declaración censal de alta, porque vayan a realizar actividades económicas o vayan a satisfacer rendimientos sujetos a retención.
c) El domicilio fiscal, y su domicilio social, cuando sea distinto de aquél.
d) La relación de establecimientos y locales en los que vaya a desarrollar actividades económicas, con identificación de la comunidad autónoma, provincia, municipio, y dirección completa de cada uno de ellos.
e) La clasificación de las actividades económicas que vaya a desarrollar según la codificación de actividades establecida a efectos del Impuesto sobre Actividades Económicas.

f) El ámbito territorial en el que vaya a desarrollar sus actividades económicas, distinguiendo si se trata de ámbito nacional, de la Unión Europea o internacional. A estos efectos, el contribuyente que vaya a operar en la Unión Europea solicitará su alta en el Registro de operadores intracomunitarios en los términos que se definan reglamentariamente.
g) La condición de persona o entidad residente o no residente. En este último caso, se especificará si cuenta o no con establecimientos permanentes, identificándose todos ellos, con independencia de que éstos deban darse de alta individualmente. Si se trata de un establecimiento permanente, en la declaración de alta se identificará la persona o entidad no residente de la que dependa, así como el resto de los establecimientos permanentes de dicha persona o entidad que se hayan dado de alta en el Censo de Empresarios, Profesionales y Retenedores.
h) El régimen de tributación en el Impuesto sobre Sociedades, en el Impuesto sobre la Renta de las Personas Físicas o en el Impuesto sobre la Renta de no Residentes, según corresponda, con mención expresa de los regímenes y modalidades de tributación que le resulten de aplicación y los pagos a cuenta que le incumban.
i) El régimen de tributación en el Impuesto sobre el Valor Añadido, con referencia a las obligaciones periódicas derivadas de dicho impuesto que le correspondan y el plazo previsto para el inicio de la actividad, distinguiendo el previsto para el inicio de las adquisiciones e importaciones de bienes y servicios del previsto para las entregas de bienes y prestaciones de servicios que constituyen el objeto de su actividad, en el caso de que uno y otro sean diferentes.
j) El régimen de tributación en los impuestos que se determinen reglamentariamente.
k) En el caso en que se trate de entidades en constitución, la declaración de alta contendrá, al menos, los datos identificativos y domicilio completo de las personas o entidades que promuevan su constitución.

4. La declaración censal de modificación contendrá cualquier variación que afecte a los datos consignados en la declaración de alta o en cualquier otra declaración de modificación anterior, en los términos que se establezcan reglamentariamente.

5. La declaración censal de baja se presentará cuando se produzca el cese efectivo en todas las actividades a que se refiere este artículo, de acuerdo con lo que se disponga reglamentariamente.

6. La Administración tributaria llevará conjuntamente con el Censo de Empresarios, Profesionales y Retenedores un Registro de operadores intracomunitarios en el que se darán de alta los sujetos pasivos del Impuesto sobre el Valor Añadido que realicen entregas y adquisiciones intracomunitarias de bienes, así como determinadas prestaciones de servicios en los términos que se establezcan reglamentariamente.

7. Las personas o entidades a que se refiere el apartado uno de este artículo podrán resultar exoneradas reglamentariamente de presentar otras declaraciones de contenido o finalidad censal establecidas por las normas propias de cada tributo.

8. Las sociedades en constitución y los empresarios individuales que presenten el documento único electrónico para realizar telemáticamente sus trámites de constitución e inicio de actividad, de acuerdo con lo previsto en la Ley 14/2013 de Apoyo a los Emprendedores y su Internacionalización, quedarán exoneradas de la obligación de presentar la declaración censal de alta, pero quedarán obligadas a la presentación posterior de las declaraciones de modificación o de baja que correspondan en la medida en que varíe o deba ampliarse la información y circunstancias contenidas en dicho documento único electrónico en caso de que el emprendedor no realice estos trámites a través de dicho documento.

Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.

Artículo 3. Formación de los censos tributarios en el ámbito de competencias del Estado.

2. El Censo de Empresarios, Profesionales y Retenedores estará formado por las personas o entidades que desarrollen o vayan a desarrollar en territorio español alguna de las actividades u operaciones que se mencionan a continuación:
a) Actividades empresariales o profesionales. Se entenderá por tales aquellas cuya realización confiera la condición de empresario o profesional, incluidas las agrícolas, forestales, ganaderas o pesqueras.
No se incluirán en el Censo de Empresarios, Profesionales y Retenedores quienes efectúen exclusivamente arrendamientos de inmuebles exentos del Impuesto sobre el Valor Añadido, conforme al artículo 20.uno.23.º de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido, siempre que su realización no constituya el desarrollo de una actividad empresarial de acuerdo con lo dispuesto en la normativa reguladora del Impuesto sobre la Renta de las Personas Físicas. Tampoco se incluirán en este censo quienes efectúen entregas a título ocasional de medios de transporte nuevos exentas del Impuesto sobre el Valor Añadido en virtud de lo dispuesto en el artículo 25.uno y dos de su ley reguladora, y adquisiciones intracomunitarias de bienes exentas en virtud de lo dispuesto en el artículo 26.tres de la misma ley.
b) Abono de rentas sujetas a retención o ingreso a cuenta.
c) Adquisiciones intracomunitarias de bienes sujetas al Impuesto sobre el Valor Añadido efectuadas por quienes no actúen como empresarios o profesionales.
También se integrarán en este censo las personas o entidades no residentes en España de acuerdo con lo dispuesto en el artículo 6 del texto refundido de la Ley del Impuesto sobre la Renta de no Residentes, aprobado por Real Decreto Legislativo 5/2004, de 5 de marzo, que operen en territorio español mediante establecimiento permanente o satisfagan en dicho territorio rentas sujetas a retención o ingreso a cuenta, y las entidades a las que se refiere el párrafo c) del artículo 5 de la citada ley.

De igual forma, las personas o entidades no establecidas en el territorio de aplicación del Impuesto sobre el Valor Añadido quedarán integradas en este censo cuando sean sujetos pasivos de dicho impuesto.
Asimismo, formarán parte de este censo las personas o entidades que no cumplan ninguno de los requisitos previstos en este apartado pero sean socios, herederos, comuneros o partícipes de entidades en régimen de atribución de rentas que desarrollen actividades empresariales o profesionales y tengan obligaciones tributarias derivadas de su condición de miembros de tales entidades.
El Censo de Empresarios, Profesionales y Retenedores formará parte del Censo de Obligados Tributarios.”

Artículo 4. Contenido del Censo de Obligados Tributarios.
1. Los datos que se incluirán en el Censo de Obligados Tributarios serán para las personas físicas los siguientes:
a) Nombre y apellidos, sexo, fecha de nacimiento, lugar de nacimiento, estado civil y fecha del estado civil.
b) Número de identificación fiscal español.
c) Número de identificación fiscal de otros países, en su caso, para los residentes.
d) Código de identificación fiscal del Estado de residencia, en su caso, para no residentes.
e) Número de pasaporte, en su caso.
f) Condición de residente o no residente en territorio español.
g) Domicilio fiscal en España y la referencia catastral del inmueble, salvo que no esté obligado a ello de acuerdo con la normativa que le sea de aplicación.
h) En su caso, domicilio en el extranjero.
i) Nombre y apellidos o razón social o denominación completa y número de identificación fiscal de los representantes legales para las personas que carezcan de capacidad de obrar en el orden tributario.

2. Los datos que se incluirán en el Censo de Obligados Tributarios serán para las personas jurídicas y demás entidades los siguientes:
a) Razón social o denominación completa, así como el anagrama, si lo tuviera.

b) Número de identificación fiscal español.
c) Número de identificación fiscal de otros países, en su caso, para los residentes.
d) Código de identificación fiscal del Estado de residencia, en su caso, para no residentes.
e) Condición de persona jurídica o entidad residentes o no residentes en territorio español.
f) Constitución en España o en el extranjero. En este último caso incluirá el país de constitución.
g) Fecha de constitución y, en su caso, fecha del acuerdo de voluntades a que se refiere el artículo 24.2 y fecha de inscripción en el registro público correspondiente.
h) Capital social de constitución.
i) Domicilio fiscal en España y la referencia catastral del inmueble, salvo que no esté obligado a ello de acuerdo con la normativa que le sea de aplicación.
j) En su caso, domicilio en el extranjero.
k) Nombre y apellidos o razón social o denominación completa y número de identificación fiscal de los representantes legales.
l) La declaración de que la entidad se constituye con la finalidad específica de la posterior transmisión a terceros de sus participaciones, acciones y demás títulos representativos de los fondos propios, y de que no realizará actividad económica hasta dicha transmisión.
Hasta ese momento estas entidades no formarán parte de los registros a que se refieren los apartados 3, 4, 5 y 6 del artículo 3.

Artículo 5. Contenido del Censo de Empresarios, Profesionales y Retenedores.
En el Censo de Empresarios, Profesionales y Retenedores, además de los datos mencionados en el artículo 4 de este reglamento, para cada persona o entidad constará la siguiente información:
a) Las declaraciones o autoliquidaciones que deba presentar periódicamente por razón de sus actividades empresariales o profesionales, o por satisfacer rentas sujetas a retención o ingreso a cuenta, en los términos previstos en la orden a que se refiere el artículo 13 de este reglamento.
b) Su situación tributaria en relación con los siguientes extremos:

1.º La condición de entidad total o parcialmente exenta a efectos del Impuesto sobre Sociedades, de acuerdo con el artículo 9 del texto refundido de la Ley del Impuesto sobre Sociedades, aprobado por Real Decreto Legislativo 4/2004, de 5 de marzo.
2.º La opción o la renuncia al régimen fiscal especial previsto en el título II de la Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo.
3.º El método de determinación del rendimiento neto de las actividades económicas que desarrolle y, en su caso, la modalidad aplicada en el Impuesto sobre la Renta de las Personas Físicas.
4.º La inclusión, renuncia, revocación de la renuncia o exclusión del método de estimación objetiva o de la modalidad simplificada del régimen de estimación directa en el Impuesto sobre la Renta de las Personas Físicas.
5.º La sujeción del obligado tributario al régimen general o a algún régimen especial en el Impuesto sobre el Valor Añadido.
6.º La inclusión, renuncia, revocación de la renuncia o exclusión del régimen simplificado, del régimen especial de la agricultura, ganadería y pesca y del régimen especial del criterio de caja del Impuesto sobre el Valor Añadido.
7.º La inclusión o baja en el Registro de operadores intracomunitarios.
8.º La inclusión o baja en el Registro de exportadores y otros operadores económicos en régimen comercial a que se refiere el artículo 30 del Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre.
9.º La inclusión o baja en el Registro de grandes empresas.
10.º La clasificación de las actividades económicas desarrolladas de acuerdo con la codificación prevista en el Real

Decreto 475/2007, de 13 de abril, por el que se aprueba la Clasificación Nacional de Actividades Económicas 2009 (CNAE-2009).
11.º La relación, en su caso, de los establecimientos o locales en los que desarrolle sus actividades económicas, con identificación de la comunidad autónoma, provincia, municipio, dirección completa y la referencia catastral de cada uno de ellos.
c) El número de teléfono y, en su caso, la dirección de correo electrónico y el nombre de dominio o dirección de Internet, mediante el cual desarrolle, total o parcialmente, sus actividades.

Artículo 6. Información censal complementaria respecto de las personas físicas residentes en España incluidas en el Censo de Empresarios, Profesionales y Retenedores.
Respecto de las personas físicas residentes en España, constarán en el Censo de Empresarios, Profesionales y Retenedores, además de su domicilio fiscal, el lugar donde tengan efectivamente centralizada la gestión administrativa y la dirección de sus negocios en territorio español, cuando sea distinto del domicilio fiscal.

Artículo 7. Información censal complementaria respecto de las entidades residentes o constituidas en España incluidas en el Censo de Empresarios, Profesionales y Retenedores.
Respecto de las entidades residentes o constituidas en España, constarán en el Censo de Empresarios, Profesionales y Retenedores los siguientes datos adicionales:
a) El domicilio social, cuando exista y sea distinto al domicilio fiscal, y la referencia catastral del inmueble.
b) La fecha de cierre del ejercicio económico.
c) La forma jurídica o clase de entidad de que se trate.
d) El nombre y apellidos o razón social o denominación completa, número de identificación fiscal y domicilio fiscal de cada uno de los socios, miembros o partícipes fundadores o que promuevan su constitución. También se harán constar esos mismos datos, excepto para las entidades que tengan la condición de comunidades de propietarios constituidas en régimen de propiedad horizontal, para cada uno de los miembros o partícipes que formen parte, en cada momento, de las entidades a que se refiere el artículo 35.4 de la Ley 58/2003, de 17 de diciembre, General Tributaria, con indicación de su cuota de participación y de atribución en caso de que dichas cuotas no coincidan. En el caso de que los socios, miembros o partícipes no sean residentes en España, se deberá hacer constar su residencia fiscal y la identificación de su representante fiscal en España si lo hubiera.
e) El nombre y apellidos o razón social o denominación completa, número de identificación fiscal de los sucesores de entidades extintas ya sea por trasformación o en los supuestos mencionados en el artículo 40 de la Ley 58/2003, del 17 de diciembre, General Tributaria.

Artículo 8. Información censal complementaria respecto de las personas o entidades no residentes o no establecidas, así como de las no constituidas en España, incluidas en el Censo de Empresarios, Profesionales y Retenedores.
1. En el caso de personas o entidades no residentes o no establecidas, así como en el de las no constituidas en España, que hayan de formar parte del Censo de Empresarios, Profesionales y Retenedores constarán en dicho censo los siguientes datos complementarios:
a) El Estado o territorio de residencia.
b) La nacionalidad y la forma jurídica o clase de entidad sin personalidad jurídica de que se trate, de acuerdo con su derecho nacional.
c) En su caso, nombre y apellidos o razón social o denominación completa, con el anagrama, si lo hubiera, número de identificación fiscal, domicilio fiscal y nacionalidad de su representante en España.

2. Cuando una persona o entidad no residente opere en territorio español por medio de uno o varios establecimientos

permanentes que realicen actividades claramente diferentes y cuya gestión se lleve de modo separado, de acuerdo con lo dispuesto en el artículo 17 del texto refundido de la Ley del Impuesto sobre la Renta de no Residentes, aprobado por Real Decreto Legislativo 5/2004, de 5 de marzo, cada establecimiento deberá inscribirse individualmente en el Censo de Empresarios, Profesionales y Retenedores, con los mismos datos y en las mismas condiciones que las personas o entidades residentes y, además, cada uno de ellos deberá identificar la persona o entidad no residente de la que dependan y comunicar los datos relativos a aquella relacionados en el apartado anterior.
Cada establecimiento permanente se identificará con una denominación específica que, en cualquier caso, comprenderá una referencia a la persona o entidad no residente de la que dependa y un número de identificación fiscal propio e independiente del asignado, en su caso, a esta última y la referencia catastral del inmueble donde esté situado el establecimiento permanente.
Asimismo, deberá especificarse la forma de determinación de la base imponible del establecimiento permanente que se constituye en España, de acuerdo con lo dispuesto en el artículo 18 del texto refundido de la Ley del Impuesto sobre la Renta de no Residentes, aprobado por Real Decreto Legislativo 5/2004, de 5 de marzo.

3. En el caso de que una persona o entidad no residente opere en territorio español por sí misma y por medio de uno o varios establecimientos permanentes, la inclusión en el Censo de Empresarios, Profesionales y Retenedores deberá realizarse tanto por la persona o entidad no residente como por sus establecimientos permanentes.
En todas estas inclusiones, además de los datos exigidos con carácter general en este reglamento, se comunicarán los relacionados en el apartado 1 de este artículo referentes a la persona o entidad no residente.
Asimismo, cada establecimiento permanente se identificará e indicará la clase de establecimiento que constituya de acuerdo con lo dispuesto en el apartado anterior y la referencia catastral del inmueble.

4. En el caso de entidades en régimen de atribución de rentas con presencia en territorio español, de acuerdo con lo dispuesto en el artículo 38.2 del texto refundido de la Ley del Impuesto sobre la Renta de no Residentes, aprobado por Real Decreto Legislativo 5/2004, de 5 de marzo, en el Censo de Empresarios, Profesionales y Retenedores deberán constar el nombre y apellidos o razón social o denominación completa, número de identificación fiscal, domicilio fiscal y nacionalidad de cada uno de los miembros o partícipes de aquella, con indicación de su cuota de participación y de atribución.

Artículo 9. Declaración de alta en el Censo de Empresarios, Profesionales y Retenedores.
1. Quienes hayan de formar parte del Censo de Empresarios, Profesionales y Retenedores deberán presentar una declaración de alta en dicho censo.

2. La declaración de alta deberá incluir los datos recogidos en los artículos 4 a 8 de este reglamento, ambos inclusive.

3. Asimismo, esta declaración servirá para los siguientes fines:
a) Solicitar la asignación del número de identificación fiscal provisional o definitivo, con independencia de que la persona jurídica o entidad solicitante no esté obligada, por aplicación de lo dispuesto en el apartado 1 anterior, a la presentación de la declaración censal de alta en el Censo de Empresarios, Profesionales y Retenedores. La asignación del número de identificación fiscal, a solicitud del interesado o de oficio, determinará la inclusión automática en el Censo de Obligados Tributarios de la persona o entidad de que se trate.
b) Comunicar el régimen general o especial aplicable en el Impuesto sobre el Valor Añadido.
c) Renunciar al método de estimación objetiva y a la modalidad simplificada del método de estimación directa en el Impuesto sobre la Renta de las Personas Físicas o a los regímenes especiales simplificado, y de la agricultura, ganadería y pesca del Impuesto sobre el Valor Añadido.
d) Indicar, a efectos del Impuesto sobre el Valor Añadido, si el inicio de la realización habitual de las entregas de bienes o prestaciones de servicios que constituyen el objeto de la actividad será posterior al comienzo de la adquisición o

importación de bienes o servicios destinados al desarrollo de la actividad empresarial o profesional.
e) Proponer a la Agencia Estatal de Administración Tributaria el porcentaje provisional de deducción a que se refiere el artículo 111.dos de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
f) Optar por la determinación de la base imponible mediante el margen de beneficio global en el régimen especial de los bienes usados, objetos de arte, antigüedades y objetos de colección a que se refiere el apartado dos del artículo 137 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
g) Solicitar la inclusión en el Registro de operadores intracomunitarios.
h) Optar por la no sujeción al Impuesto sobre el Valor Añadido de las entregas de bienes a que se refiere el artículo 68.cuatro de la ley de dicho impuesto.
i) Comunicar la sujeción al Impuesto sobre el Valor Añadido de las entregas de bienes a que se refieren el artículo 68. tres y cinco de la ley de dicho impuesto, siempre que el declarante no se encuentre ya registrado en el censo.
j) Optar por la aplicación de la regla de prorrata especial en el Impuesto sobre el Valor Añadido, prevista en el artículo 103.dos.1.º de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
k) Optar por la determinación del pago fraccionado del Impuesto sobre Sociedades, de acuerdo con la modalidad prevista en el artículo 45.3 del texto refundido de la Ley del Impuesto sobre Sociedades, aprobado por Real Decreto Legislativo 4/2004, de 5 de marzo.
l) Comunicar el periodo de liquidación de las autoliquidaciones de retenciones e ingresos a cuenta del Impuesto sobre la Renta de las Personas Físicas, del Impuesto sobre la Renta de no Residentes y del Impuesto sobre Sociedades, en atención a la cuantía de su último presupuesto aprobado cuando se trate de retenedores u obligados a ingresar a cuenta que tengan la consideración de Administraciones públicas, incluida la Seguridad Social.
m) Optar por la aplicación del régimen general previsto para los establecimientos permanentes, en los términos del artículo 18.5.b) del texto refundido de la Ley del Impuesto sobre la Renta de no Residentes, aprobado por Real Decreto Legislativo 5/2004, de 5 de marzo, para aquellos establecimientos permanentes cuya actividad en territorio español consista en obras de construcción, instalación o montaje cuya duración exceda de seis meses, actividades o explotaciones económicas de temporada o estacionales, o actividades de exploración de recursos naturales.
n) Optar por el régimen fiscal especial previsto en el título II de la Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo.
ñ) Comunicar aquellos otros hechos y circunstancias de carácter censal previstos en la normativa tributaria o que determine el Ministro de Economía y Hacienda.
o) Comunicar la condición de empresario o profesional revendedor de los bienes a que se refiere el artículo 84.Uno.2.ºg) de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
p) Optar por la aplicación del diferimiento del ingreso de las cuotas de Impuesto sobre el Valor Añadido en las operaciones de importación liquidadas por la Aduana, a que se refiere el artículo 167.Dos de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
q) Optar por la llevanza de los libros registro del Impuesto sobre el Valor Añadido a través de la Sede electrónica de la Agencia Estatal de Administración Tributaria de acuerdo con lo previsto en el artículo 62.6 del Reglamento del Impuesto sobre el Valor Añadido.
r) Comunicar la opción por el cumplimiento de la obligación de expedir factura por los destinatarios de las operaciones o por terceros, en los términos del artículo 5.1 del Reglamento por el que se aprueban las obligaciones de facturación, aprobado por el Real Decreto 1619/2012, de 30 de noviembre, en el caso de las personas y entidades a que se refiere el artículo 62.6 del Reglamento del Impuesto sobre el Valor Añadido.
s) Optar por la no sujeción al Impuesto sobre el Valor Añadido de las prestaciones de servicios a que se refiere el artículo 70.Uno.8.º de la ley de dicho impuesto.
t) Comunicar la sujeción al Impuesto sobre el Valor Añadido de las prestaciones de servicios a que se refiere el artículo 70.Uno.4.ºa) de la ley de dicho impuesto, siempre que el declarante no se encuentre ya registrado en el censo.

4. Esta declaración deberá presentarse, según los casos, con anterioridad al inicio de las correspondientes actividades, a

la realización de las operaciones, al nacimiento de la obligación de retener o ingresar a cuenta sobre las rentas que se satisfagan, abonen o adeuden o a la concurrencia de las circunstancias previstas en este artículo.
A efectos de lo dispuesto en este reglamento, se entenderá producido el comienzo de una actividad empresarial o profesional desde el momento que se realicen cualesquiera entregas, prestaciones o adquisiciones de bienes o servicios, se efectúen cobros o pagos o se contrate personal laboral, con la finalidad de intervenir en la producción o distribución de bienes o servicios.

Artículo 10. Declaración de modificación en el Censo de Empresarios, Profesionales y Retenedores.
1. Cuando se modifique cualquiera de los datos recogidos en la declaración de alta o en cualquier otra declaración de modificación posterior, el obligado tributario deberá comunicar a la Administración tributaria, mediante la correspondiente declaración, dicha modificación.

2. Esta declaración, en particular, servirá para:
a) Comunicar el cambio de domicilio fiscal, de acuerdo con lo previsto en el artículo 48.3 de la Ley 58/2003, de 17 de diciembre, General Tributaria, por las personas jurídicas y demás entidades, así como por las personas físicas incluidas en el Censo de Empresarios, Profesionales y Retenedores.
b) Comunicar la variación de cualquiera de los datos y situaciones tributarias recogidas en los artículos 4 a 9 de este reglamento, ambos inclusive.
c) Comunicar el inicio de la realización habitual de las entregas de bienes o prestaciones de servicios correspondientes a actividades empresariales o profesionales, cuando la declaración de alta se hubiese formulado indicando que el inicio de la realización de dichas entregas de bienes o prestaciones de servicios se produciría con posterioridad al comienzo de la adquisición o importación de bienes o servicios destinados a la actividad.
Asimismo, la declaración de modificación servirá para comunicar el comienzo de la realización habitual de las entregas de bienes o prestaciones de servicios correspondientes a una nueva actividad constitutiva de un sector diferenciado a efectos del Impuesto sobre el Valor Añadido, cuando se haya presentado previamente una declaración censal mediante la que se comunique que el inicio de la realización de las entregas de bienes y prestaciones de servicios en desarrollo de dicha nueva actividad se produciría con posterioridad al comienzo de la adquisición o importación de bienes o servicios destinados a aquella.
d) Optar por la determinación de la base imponible mediante el margen de beneficio global en el régimen especial de los bienes usados, objetos de arte, antigüedades y objetos de colección a que se refiere el apartado dos del artículo 137 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
e) Solicitar la inclusión en el Registro de operadores intracomunitarios cuando se vayan a producir, una vez presentada la declaración censal de alta, las circunstancias que lo requieran previstas en el artículo 3.3 de este reglamento.
Los sujetos pasivos del Impuesto sobre el Valor Añadido que cesen en el desarrollo de las actividades sujetas al mismo sin que ello determine su baja en el Censo de Empresarios, Profesionales y Retenedores, y las personas o entidades que durante los 12 meses anteriores no hayan realizado entregas o adquisiciones intracomunitarias de bienes sujetas al Impuesto sobre el Valor Añadido o no hayan prestado o sido destinatarios de las prestaciones de servicios a que se refieren los párrafos c) y d) del artículo 3.3 de este reglamento, deberán presentar, asimismo, una declaración censal de modificación solicitando la baja en el Registro de operadores intracomunitarios.
f) Optar por la no sujeción al Impuesto sobre el Valor Añadido de las entregas de bienes a que se refiere el artículo 68.cuatro de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
g) Comunicar la sujeción al Impuesto sobre el Valor Añadido de las entregas a que se refieren el artículo 68.tres y cinco de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.
h) Revocar las opciones o modificar las solicitudes a que se refieren los párrafos d), e), f), p), q) y r) de este apartado y los párrafos f), h), q), r) y s) del artículo 9.3 de este Reglamento, así como la comunicación de los cambios de las situaciones a que se refieren el párrafo g) de este apartado y los párrafos i), o) y t) del artículo 9.3 de este Reglamento.

i) (Suprimida)
j) En el caso de aquellos que, teniendo ya la condición de empresarios o profesionales por venir realizando actividades de tal naturaleza, inicien una nueva actividad empresarial o profesional constituya o no, a efectos del Impuesto sobre el Valor Añadido, un sector diferenciado respecto de las actividades que venían desarrollando con anterioridad, y se encuentren en cualesquiera de las circunstancias que se indican a continuación, para comunicar a la Administración su concurrencia:

1.º Que ejercen la opción por la regla de prorrata especial prevista en el artículo 103.dos.1.º de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.

2.º Que en los casos de inicio de actividad que constituya un sector diferenciado, el comienzo de la realización habitual de las entregas de bienes o prestaciones de servicios correspondientes a la nueva actividad se producirá con posterioridad al comienzo de la adquisición o importación de bienes o servicios destinados a su desarrollo y resulte aplicable el régimen de deducción previsto en los artículos 111, 112 y 113 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido. En este caso, la declaración contendrá también la propuesta del porcentaje provisional de deducción a que se refiere el citado artículo 111.dos de dicha ley.
k) Solicitar la inclusión en el Registro de exportadores y otros operadores económicos en régimen comercial, así como la baja en dicho registro, de acuerdo con el artículo 30 del Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre.
l) Comunicar a la Administración tributaria el cambio de periodo de liquidación en el Impuesto sobre el Valor Añadido y a efectos de las autoliquidaciones de retenciones e ingresos a cuenta del Impuesto sobre la Renta de las Personas Físicas, Impuesto sobre la Renta de no Residentes y del Impuesto sobre Sociedades por estar incluidos en el Registro de grandes empresas regulado en el artículo 3 de este reglamento, o en atención a la cuantía de su último presupuesto aprobado cuando se trate de retenedores u obligados a ingresar a cuenta que tengan la consideración de Administraciones públicas, incluida la Seguridad Social.
m) Optar o renunciar a la opción para determinar el pago fraccionado del Impuesto sobre Sociedades, de acuerdo con la modalidad prevista en el artículo 45.3 del texto refundido de la Ley del Impuesto sobre Sociedades, aprobado por Real Decreto Legislativo 4/2004, de 5 de marzo.
n) Renunciar a la aplicación del régimen de consolidación fiscal en el caso de los grupos fiscales que hayan ejercitado esta opción.
ñ) Optar o renunciar al régimen fiscal especial previsto en el título II de la Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo.
o) Solicitar la rectificación de datos personales a que se refiere el artículo 2.5 de este reglamento.
p) Optar por la llevanza de los libros registro del Impuesto sobre el Valor Añadido a través de la Sede electrónica de la Agencia Estatal de Administración Tributaria de acuerdo con lo previsto en el artículo 62.6 del Reglamento del Impuesto sobre el Valor Añadido.
q) Comunicar la opción del cumplimiento de la obligación de expedir factura por los destinatarios de las operaciones o por terceros, en los términos del artículo 5.1 del Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1619/2012, de 30 de noviembre, en el caso de las personas y entidades a que se refiere el artículo 62.6 del Reglamento del Impuesto sobre el Valor Añadido.
r) Optar por la no sujeción al Impuesto sobre el Valor Añadido de las prestaciones de servicios a que se refiere el artículo 70.uno.8.º de la Ley de dicho impuesto.
s) Comunicar otros hechos y circunstancias de carácter censal previstos en las normas tributarias o que determine el Ministro de Hacienda.

3. Esta declaración no será necesaria cuando la modificación de uno de los datos que figuren en el censo se haya producido por iniciativa de un órgano de la Agencia Estatal de Administración Tributaria.

4. La declaración deberá presentarse en el plazo de un mes desde que se hayan producido los hechos que determinan su presentación, salvo en los casos que se indican a continuación:
a) En los supuestos en que la normativa propia de cada tributo o la del régimen fiscal aplicable establezca plazos específicos, la declaración se presentará de conformidad con estos.
b) Las declaraciones a que se refiere el apartado 2.j).1.º de este artículo, deberán presentarse con anterioridad al momento en que se inicie la nueva actividad empresarial que vaya a constituir, a efectos del Impuesto sobre el Valor Añadido, un sector diferenciado de actividad respecto de las que se venían desarrollando con anterioridad.
c) La comunicación prevista en el apartado 2.l) de este artículo se formulará en el plazo general y, en cualquier caso, antes del vencimiento del plazo para la presentación de la primera declaración periódica afectada por la variación puesta en conocimiento de la Administración tributaria o que hubiese debido presentarse de no haberse producido dicha variación.
d) La solicitud a que se refiere el primer párrafo del apartado 2.e) de este artículo deberá presentarse con anterioridad al momento en el que se produzcan las circunstancias previstas en el artículo 3.3 de este reglamento.
e) Cuando el Ministro de Economía y Hacienda establezca un plazo especial atendiendo a las circunstancias que concurran en cada caso.

Ley 4/2014, de 1 de abril, Básica de las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación

Artículo 8. *Censo público*.
Las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación elaborarán un censo público de empresas del que formarán parte las personas físicas o jurídicas, nacionales o extranjeras, que ejerzan las actividades comerciales, industriales, de servicios y navieras en territorio nacional, para cuya elaboración contarán con la colaboración de la administración tributaria competente así como de otras administraciones que aporten la información necesaria, garantizando, en todo caso, la confidencialidad en el tratamiento y el uso exclusivo de dicha información.
Para la elaboración del censo público de empresas las administraciones tributarias facilitarán a la Cámara Oficial de Comercio, Industria, Servicios y Navegación de España y a las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación los datos del Impuesto sobre Actividades Económicas y los censales de las empresas que sean necesarios. Únicamente tendrán acceso a la información facilitada por la administración tributaria los empleados de cada Cámara que determine el pleno.
Esta información se empleará para la elaboración del censo público de empresas, para el cumplimiento de las funciones público-administrativas que la presente Ley atribuye a las Cámaras así como para la elaboración del censo electoral a que se hace referencia en el artículo 17 de la misma.
Dicho personal tendrá, con referencia a los indicados datos, el mismo deber de sigilo que los funcionarios de la administración tributaria. El incumplimiento de este deber constituirá, en todo caso, infracción muy grave de conformidad con su régimen disciplinario.

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)

Artículo 5. *Principios relativos al tratamiento*
1.Los datos personales serán:
a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará

incompatible con los fines iniciales («limitación de la finalidad»);
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Considerando (39)
Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

Artículo 6. *Licitud del tratamiento*
1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
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. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2.Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3.La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:
a) el Derecho de la Unión, o
b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.
La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Considerando (40)
Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro

Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

Considerando (45)
Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

Considerando (31)
Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

Considerando (47)
El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del

interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

Considerando (50)
El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si 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, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista. Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

Artículo 12. *Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado*
1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:
a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o
b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. 8.La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Considerando (58)
El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

Artículo 13. *Información que deberá facilitarse cuando los datos personales se obtengan del interesado*

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:
a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. *Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado*
1.Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
d) las categorías de datos personales de que se trate;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:
a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
e) el derecho a presentar una reclamación ante una autoridad de control;
f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:
a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:
a) el interesado ya disponga de la información;
b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de

naturaleza estatutaria.

Considerando (60)
Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.

Considerando (61)
Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

Considerando (62)
Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas.

Artículo 25. *Protección de datos desde el diseño y por defecto*
1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas

físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Considerando (78)
La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Artículo 5. *Deber de confidencialidad.*
1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Artículo 8. *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.*
1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo

6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 77. *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.*
1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:
a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 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 sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.
Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la

publicidad de estas resoluciones, a lo que disponga su normativa específica.

Disposición adicional décima. *Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.*
Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.

Artículo 11. *Transparencia e información al afectado*.
1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:
a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
En estos supuestos, la información básica incluirá también:
a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

Artículo 19. *Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.*
1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:
a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.
b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea

necesario para el ejercicio de sus competencias.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Artículo 2. Ámbito objetivo de aplicación
1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.
1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.
En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.
Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Proyecto de Xnet coordinado por Simona Levi con Míriam Carles y con la colaboración de los investigadores del Posgrado dirigido por Simona Levi y Cristina Ribas sobre Tecnopolítica y Derechos en la Era Digital, Rubén Bujalance, César Manso-Sayao y otras

participantes que han pedido no hacer públicos sus nombres.

**Título propuesto durante el Posgrado en Tecnopolítica y Derechos en la Era Digital por Víctor Pérez Berruezo.*

Versión actualizada a diciembre de 2022.

Ninguna publicación de versiones anteriores es autorizada por las y los autores.

Investigación realizada en parte con el apoyo de la Agència de Transparència del Àrea Metropolitana de Barcelona (AMB) y del Ajuntament de Barcelona (En ambos casos, subvenciones).

Parte de la investigación se incorporará y continuará en el proyecto Gavius de la UIA.