Auditoría Pública nº 74 (2019), pp. 115 - 122

Arantza Martínez de Lagrán Larrauri
Letrada
Tribunal Vasco de Cuentas Públicas

Claves y aspectos prácticos para la adaptación de las ICEX al nuevo marco de la protección de datos personales

RESUMEN/ABSTRACT:

La protección de datos personales debido a los profundos cambios normativos producidos en el último año, es un tema de gran actualidad que conviene tomar en serio. Los datos personales que tratamos no nos pertenecen y por tanto, tenemos la responsabilidad de hacer un tratamiento adecuado de los mismos.

Los recientes cambios legislativos de 2018 han sido de calado, Reglamento Europeo 2016/79 General de Protección de Datos (RGPD) y Ley 3/2018 Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). La nueva normativa ha generado nuevas obligaciones que afectan a las Instituciones de Control Externo (en adelante ICEX) como responsables de tratamientos de datos.

En este trabajo, tomaré como referencia la experiencia del Órgano de control externo vasco, Tribunal Vasco de Cuentas Públicas / Herri-Kontuen Euskal Epaitegia (en adelante TVCP), al cual pertenezco y se repasarán los cambios necesarios para la adaptación. Se analizará también el cambio del planteamiento de la normativa en lo relativo a la comunicación de datos por parte de los fiscalizados a las ICEX.

Y para terminar, un supuesto práctico que aunque no suele ser habitual, en alguna ocasión se ha planteado en la tarea de fiscalización y es aquél en el que algún fiscalizado, con la "excusa" de la protección de los datos personales, se niega a facilitar los datos solicitados por el Órgano de control.

Personal data protection due to profound legislative changes that have taken place in the past year is a highly topical subject that should be taken very seriously. The personal data we process do not belong to us and, therefore, we have the responsibility to process them appropriately.

The recent legislative changes in 2018 have been significant, European Regulation 2016/79 General Data Protection (GDPR) and Organic Law 3/2018 on Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD, in Spanish). The new standards and regulations have created new obligations that affect the External Control Institutions (hereinafter, ICEX) as data controllers.

In this work, I will take the experience of the Basque External Control Body, Basque Court of Auditors / Herri-Kontuen Euskal Epaitegia (hereinafter, TVCP), which I belong to, as reference and will review the necessary changes for adaptation. The change in the regulatory approach regarding data reporting by auditees to the ICEX will also be analysed.

And finally, a case study that, although unusual, on some occasions has been raised in audit tasks is one in which some auditees, using the "excuse" of personal data protection, refuse to provide the data requested by the Control Body.

PALABRAS CLAVE/KEYWORDS:

ICEX, OCEX, PROTECCIÓN DE DATOS, COMUNICACIÓN DE DATOS, TRATAMIENTO DE DATOS, FISCALIZACIÓN, RGPD,LOPDGDD,TVCP
ICEX, OCEX, DATA PROTECTION, DATA REPORTING, TREATMENT OF DATA, AUDITING

INTRODUCCIÓN: EL PORQUÉ DE LA NECESIDAD DE LA PROTECCIÓN DE LOS DATOS

Caer en la cuenta de que la revolución tecnológica, aparentemente silente, está removiendo los cimientos de nuestra forma de ser y de estar en este mundo es un buen punto de partida para entender la necesidad de la protección de los datos personales. Por ilustrativos, cito a continuación unos pasajes del libro que Alessandro Baricco ha publicado este año "The Game"[1] (muy difundido en distintos medios de comunicación):"Caímos en la trampa de que la digitalización era gratis. El precio pagado y el que pagaremos es altísimo: se ha hecho a costa de nuestros datos. Al fin y a la postre de nuestra intimidad, de nuestra dignidad y de nuestros derechos fundamentales. Pero eso es un intangible que a nadie importa. Se trata de violaciones silentes y de efectos retardados. Sólo te darás cuenta cuando nada ya tenga remedio. De paso nos hemos cargado la propiedad intelectual pues quien gana no es quien crea sino quien distribuye"…."y nadie que haya nacido antes de Google va a resolver este problema"…."Los datos son de la persona. Pero resultan un intangible al menos hasta que se hacen operativos y se entrecruzan… el problema real es cómo todo esto terminará afectando a la dignidad de las personas y su patrimonio de derechos y libertades fundamentales, pues los datos mal usados o manejados, tienen una capacidad infinita de irradiar todos y cada uno de los derechos fundamentales de la persona y transformarlos en papel mojado…. ¿por qué no me conceden un crédito hipotecario, un puesto de trabajo o una subvención? Pregúnteselo al algoritmo".

Quizá *a priori*, es esta una visión un tanto crítica del cambio, pero nos ayuda a entender el porqué de la necesidad de la protección de los datos personales, cuya regulación ha sufrido modificaciones profundas en el pasado año.

1.- NUEVAS OBLIGACIONES PARA LAS ICEX EN MATERIA DE PROTECCIÓN DE DATOS

1. A.- Evolución del Marco legal

La base jurídica del derecho a la protección de los datos en origen, lo recoge la **Constitución Española de 1978 en el artículo 18.4** sobre el derecho a la intimidad familiar y personal y el secreto de las comunicaciones, Título I, Capítulo II, Sección 1ª:

"*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***".**

De este modo, nuestra Constitución en 1978, cuando aún no existía ni el correo electrónico, incorporó una nueva garantía constitucional, como forma de respuesta a una nuevo modo de amenaza concreta a la dignidad y a los derechos de la persona, de forma no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales.

De construcción jurisprudencial posterior, ha sido la diferenciación entre el derecho a la intimidad y el derecho a la protección de los datos personales, referido al control de las informaciones personales.

En desarrollo, se aprobó 21 años después, la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD** y su Reglamento, Real Decreto 1720/2007, de 21 de diciembre), que tenía por objeto garantizar y proteger, el tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor, intimidad y privacida d personal y familiar.

En el pasado año, el panorama legislativo cambió, respondiendo a la necesidad de disponer de una regulación más uniforme en el conjunto de la Unión Europea, que evite divergencias y garantice la tenencia de un nivel coherente de protección de derechos y la libre circulación de los datos en el mercado interior. El legislador europeo aprobó en 2016 en el mes de abril, el **Reglamento 2016/79 General de Protección de Datos (RGPD) con entrada en vigor el 25 de mayo de 2018**. Norma que por tratarse de un Reglamento en vez de una Directiva, es de aplicación directa sin necesidad de aprobación de norma interna de trasposición, lo cual es de una importancia capital, pues el legislador europeo ha pasado de la técnica de la Directiva a la del Reglamento que adquiere vigencia, sin necesidad de transposición y sin tan siquiera necesidad de que sea publicado en el BOE.

El Reglamento Europeo, impone un cambio drástico de enfoque en cuanto al tratamiento de los datos personales. Esta norma, además de desplazar a la antigua Ley Orgánica 15/1999, y a su Reglamento de desarrollo, introduce cambios de calado. En líneas generales, se puede decir que en España anteriormente **con la LOPD se articulaba un sistema de responsabilidad de medios**, mientras que **con el nuevo Reglamento el sistema de responsabilidad que se articula es de finalidad**, la finalidad de la regulación ahora, es la de proteger los datos y para ello los responsables deben adoptar las medidas adecuadas y hacer lo razonablemente posible para conseguirlo, función atribuida al Responsable del tratamiento que debe de probar que dicha función se está realizando debidamente, incorporando

[1]Editorial Anagrama, 2019. The Game, Alessandro Baricco

documentos como el análisis de riesgos, y el registro de actividades de tratamiento, novedades a grandes rasgos del Reglamento, de los cuales hablaremos más adelante en profundidad.

Novedad, respecto del sistema anterior con la LOPD, es la supresión de la inscripción de ficheros de datos. Ahora con la nueva regulación, los Responsables deberán configurar el denominado Registro de Actividades de Tratamiento, así como, el contenido del derecho de información que deberá facilitarse a los afectados en la recogida de datos, puesto que se amplía considerablemente. Otra diferencia en lo referente a seguridad, es que el RGPD no parte como la LOPD de una configuración de medidas de seguridad de nivel bajo, medio o alto, en función de los diferentes tipos de tratamiento de datos, ahora, es el análisis de riesgos de los tratamientos, el que determina a partir de los resultados obtenidos del mismo, las medidas de seguridad que se tienen que implementar.

Con posterioridad al Reglamento Europeo, fue aprobada el 5 de diciembre de 2018, con un 93% de apoyo parlamentario, la **Ley 3/2018 Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD)**, esta Ley de la que hablaremos más adelante, no desarrolla el Reglamento Europeo, sólo adapta el derecho español al modelo establecido por el Reglamento General de Protección de Datos (RGPD).

1. B.- Conceptos clave del RGPD

Los conceptos básicos que el RGPD incorpora, son de necesaria y previa comprensión para la implantación del mismo:

Dato de carácter personal, es toda información sobre una persona física identificada o identificable («el afectado»). Se considerará persona física identificable, aquélla **cuya identidad pueda determinarse, directa o indirectamente** mediante un identificador, como un nombre, un número, localización, un identificador en línea o a través de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

La web oficial de la Comisión europea[2] cita como ejemplos, además del nombre y apellidos y domicilio, la dirección de correo electrónico del tipo nombre. apellido@empresa.com, el número de DNI, datos de localización (como la función de los datos de localización de un teléfono móvil), dirección de protocolo de internet (IP), el identificador de una *cookie*, el identificador de la publicidad del teléfono, los datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona. Y no considera datos personales, por ejemplo: el número de registro mercantil, la dirección de correo electrónico, del tipo info@empresa.com, o los datos anonimizados.

Tratamiento de datos de carácter personal: Cualquier actividad que contenga datos de carácter personal, ya se realice de manera manual o automatizada, total o parcialmente.

Responsable del tratamiento de datos: El Responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que determine los fines y medios del tratamiento.

Encargado del tratamiento: Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos por cuenta del Responsable del tratamiento. En el caso de los poderes públicos, algunos ejemplos pueden ser el encargo a una empresa de la elaboración de las nóminas de su personal, la destrucción de documentación o el control de las cámaras de video vigilancia. La relación entre Responsable y Encargado deberá estar regulada en instrumento jurídico.

Delegado de protección de datos: Figura de nueva creación del RGPD, obligatoria para la Administración y también para las ICEX. Será el sujeto especialista en materia de protección de datos, con carácter independiente. La persona que desempeñe dicha función, deberá contar con un perfil jurídico y con sólidos conocimientos en materia de protección de datos y de la organización interna de la ICEX.

1. C.- Nuevos principios aplicables al tratamiento de datos personales

El RGPD regula en sus artículos 5 a 11 los principios que en general rigen en materia de protección de datos: 1) **Licitud, lealtad y transparencia:** los datos deben ser tratados de manera lícita, leal y transparente en relación con el afectado. 2) **Limitación de la finalidad**: serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con dichos fines. 3) **Minimización de datos**: serán adecuados, pertinentes y limitados a lo necesario, en relación con los fines. 4) **Exactitud**: serán exactos y actualizados, debiendo adoptar medidas razonables para suprimir o rectificar los que sean inexactos. 5) **Limitación del plazo de conservación**: serán mantenidos no más tiempo del necesario para los fines del tratamiento, excepto con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos. 6) **Integridad y seguridad**: serán tratados garantizando su adecuada seguridad, protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño

[2]https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es#ejemplos-de-datos-personales

accidental. En el caso de la Administración Pública, con arreglo al Esquema Nacional de Seguridad que regula el Real Decreto 3/2010. Por último, 7) la **Responsabilidad proactiva**: el responsable del tratamiento además de cumplir, debe ser capaz de proporcionar evidencias del cumplimiento, artículo 5 RGPD.

La LOPDGDD ya citada, adapta el Reglamento europeo y en esa línea introduce algunas novedades: facilita el ejercicio de derechos a los ciudadanos, reconoce específicamente el derecho de acceso, rectificación o supresión por parte de quienes tuvieran vinculación con **personas fallecidas** salvo que el fallecido lo hubiera prohibido, en cuanto a los **menores**, la Ley fija en 14 años la edad a partir de la cual se puede prestar consentimiento de manera autónoma. También regula el derecho a solicitar la supresión de los datos facilitados a redes sociales y refuerza, las obligaciones del **sistema educativo** en el uso seguro y adecuado de internet, regula el **derecho al olvido** en redes sociales y servicios de la sociedad de la información equivalentes, establece **sistemas de denuncias internas anónimas**, modifica la regulación de los **sistemas de información crediticia** (los conocidos como ficheros de morosos), reduciendo de 6 a 5 años el periodo máximo de inclusión de las deudas por importe superior a 50 euros, actualiza las garantías del derecho a la intimidad frente al uso de dispositivos de video vigilancia y de grabación de sonidos en el lugar de trabajo y refuerza las garantías del derecho a la intimidad en relación con el uso de dispositivos digitales puestos a disposición de los empleados, complementando la regulación del derecho a la intimidad ante la utilización de sistemas de geolocalización en el **ámbito laboral**, de los que deberán ser informados. En el ámbito del empleo público, es la LOPDGDD la que añade un **nuevo derecho individual** para los empleados públicos, con el artículo 14, apartado j bis) al **Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público**: Derecho "A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de video-vigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

2.- TRATAMIENTO DE LOS DATOS COMUNICADOS POR LOS FISCALIZADOS A LAS ICEX

Entre las múltiples formas de tratamiento de datos personales que llevan a cabo los poderes públicos, y en especial las ICEX, uno de los más relevantes y con mayor impacto potencial, es el que contiene datos comunicados, lo que el RGPD califica como "**comunicación por transmisión**" a terceros y que, como toda modalidad de tratamiento, debe ampararse en alguno de los criterios de licitud previstos en el art. 6 del Reglamento.

Tan frecuente como la comunicación de datos personales entre Administraciones, basada en el consentimiento previo y expreso de su titular, lo es aquella comunicación amparada en "el cumplimiento de una obligación legal aplicable al Responsable del tratamiento" (art.6.1c) RGPD) y en "el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al Responsable del tratamiento" (art.6.1 e) RGPD).

En los dos últimos casos mencionados, el RGPD exige la existencia de una determinada base jurídica (el Derecho de la Unión o el Derecho del Estado miembro aplicable al Responsable del tratamiento). Además dicha base jurídica preceptiva, ha de cumplir un objetivo de interés público y ser proporcional al fin legítimo perseguido.

Entre los contenidos que habrá de especificar el Derecho de la Unión y el Derecho de los Estados miembros, se encuentra el relativo a la determinación de "las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación" (art.6.3, párrafo segundo, RGPD); no en vano, una de las facultades que integran el derecho de acceso de los interesados, es la de conocer "los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales" (art. 15.1 c) RGPD), siendo ésta una de las informaciones objeto del "registro de las actividades de tratamiento".

La comunicación de datos, por parte de las Administraciones fiscalizadas a las ICEX, con la anterior LOPD se encontraba prevista expresamente en el artículo 11, como excepción al previo consentimiento, que era regla general para la comunicación de datos:

"Comunicación de datos: 1. Los datos de carácter personal objeto del tratamiento *sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.*

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.……

….d) Cuando la comunicación que deba efectuarse

tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas".

Ahora sin embargo, el artículo de la derogada Ley Orgánica no tiene equivalente en la nueva Ley, ni en el Reglamento Europeo. En el Reglamento Europeo la comunicación de datos no es ya una excepción al consentimiento, sino que tanto el consentimiento como las restantes bases jurídicas, son requisitos equivalentes e independientes para que el tratamiento no resulte ilícito, es decir, ya no existen excepciones, sino únicamente requisitos, siendo el consentimiento un requisito más y no la regla general como lo era antes.

Por tanto, las comunicaciones de datos de los fiscalizados, están amparadas en "*el cumplimiento de una obligación legal aplicable al responsable del tratamiento*" (art.6.1c) RGPD) y en "*el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*" (art.6.1 e) RGPD).

La LOPDGDD, expresamente establece en el artículo 8.2, que 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, cuando derive de una competencia atribuida por una **norma con rango de ley**. Por tanto, establece como lícitos los tratamientos, para cumplimiento de obligaciones impuestas por norma con rango de Ley. En el caso de las ICEX y en concreto en el del TVCP, nuestra Ley autonómica 1/1988, de 5 de febrero, del «Tribunal Vasco de Cuentas Públicas» / «Herri-Kontuen Euskal Epaitegia», es la que impone la obligación para el fiscalizado y reconoce la competencia para la fiscalización al OCEX autonómico.

3.- ADECUACIÓN AL RGDP EN LAS ICEX

Se cumple algo más de un año de la entrada en vigor del Reglamento y son muchas las Administraciones e ICEX que se han adaptado el cambio. Sin embargo, algunos expertos apuntan a que quizá la **exención de sanciones para la Administración**, a diferencia con la empresa privada, ha supuesto una relajación para los Responsables.

A continuación se hace un repaso de los **pasos imprescindibles** para lograr la adecuación a la nueva normativa de protección de datos:

1.- En primer lugar se debe establecer un **registro de actividades de tratamiento** que sustituye en parte a los ficheros que establecía la LOPD. El RGPD establece un contenido mínimo de ese registro, que perfectamente puede organizarse sobre la base de los ficheros existentes. Ese registro debe mantenerse actualizado y a disposición de las autoridades de protección de datos. La LOPDGDD en el artículo 31 en relación con el 77.1 establece la obligatoriedad de su elaboración y publicación para las ICEX:

"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".*

El artículo 77.1 incluye, entre otros: "a) ***Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos***."

Por tanto, las ICEX para dar cumplimiento a este requisito han de elaborar y publicar el Registro de Actividades de Tratamiento.

A continuación, a modo de ejemplo, los tratamientos de datos más habituales en un OCEX[3]:

[3]http://web.tvcp.org/2019/03/18/registro-de-tratamientos/
"Código de protección de datos". José Luis Piñar Mañas. Editorial La Ley 2019
https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf
https://www.avpd.euskadi.eus/s04-5213/es/

2. En segundo lugar se debe Identificar la **legitimación de los tratamientos finalidades y la base jurídica.** En el ámbito de los poderes públicos, y en especial en la mayor parte de los tratamientos de datos de las ICEX, la base jurídica que en general legitima los tratamientos no es el consentimiento (hay supuestos en que sí), es el cumplimiento de una tarea en interés público o el ejercicio de poderes o funciones públicas, así como el cumplimiento de una obligación legal. En ambos casos como ya se ha dicho, debe existir una previsión normativa **con rango de ley**. A continuación se exponen como ejemplo, las bases jurídicas del ejemplo de tratamiento antes expuesto, haciendo concreta referencia a la legislación autonómica que afecta al TVCP:

TRATAMIENTO	BASE JURÍDICA DEL TRATAMIENTO
Gestión Económica Presupuestaria y Contable	Cumplimiento de la legislación aplicable al tratamiento (D. L 2/2017, de 19 de octubre, por el que se aprueba el texto refundido de la Ley de Control Económico y Contabilidad de la Comunidad Autónoma de Euskadi) Cumplimiento de la legislación aplicable al tratamiento (Ley 9/2017 de 8 de noviembre de Contratos del Sector Público)
Registro de Entrada y Salida	Cumplimiento de la legislación aplicable al tratamiento (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas)
Agenda de Comunicación y Relaciones Institucionales	Tratamiento necesario para el cumplimiento de una misión realizada en interés público (Ley 1/1988, de 5 de febrero, del TVCP).
Grabación de sesiones de Plenos	Ejercicio de funciones públicas conferidas al responsable del tratamiento (Ley 1/1988, de 5 de febrero, del TVCP). Cumplimiento de la legislación aplicable al tratamiento (Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público).
Recursos Humanos y Nómina	Cumplimiento de la legislación aplicable al tratamiento (Ley 6/1989 de 6 de julio de la Función Pública Vasca. Real Decreto Legislativo 5/2015 de 30 de octubre por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. Ley 1/1988, de 5 de febrero, del TVCP)
Fiscalización	Ejercicio de funciones públicas conferidas al responsable del tratamiento (Ley 1/1988, de 5 de febrero, del TVCP)
Contabilidades Electorales	Ejercicio de funciones públicas conferidas al responsable del tratamiento (Ley 1/1988, de 5 de febrero, del TVCP)

Añadir un **inciso referido a la regulación del tratamiento de categorías especiales de datos**, como las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los que revelen el origen racial o étnico, y los relativos a la salud o a la vida u orientación sexual de una persona, incluso los datos genéticos y los datos biométricos, para estos la **regla general** en el Reglamento es la **prohibición del tratamiento**, salvo las excepciones que recoge el propio artículo 9.

3.- Siguiendo con la hoja de ruta para la adaptación, también se debe **revisar la información que se ofrece a los interesados**, cuando se recogen sus datos. Que esta información se proporcione de forma "concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

4. Deberán **establecerse procedimientos de ejercicio de derechos** que permitan responder en los plazos previstos por el RGPD y mecanismos visibles, accesibles

y sencillos**,** incluidos los medios electrónicos, para su ejercicio, cuando se trate del ejercicio por medios electrónicos, deben incorporar procedimientos para verificar la identidad de los interesados que los utilizan.

5. Se deben **revisar los contratos con los encargados de tratamiento,** para ver si ofrecen garantías de cumplimiento del RGPD. La relación entre Responsables y Encargados deberá formalizarse mediante acto jurídico que vincule al Encargado.

6. Se debe realizar un **análisis de riesgo** para los derechos y libertades de los ciudadanos de todos los tratamientos. En el contexto de la Administración Pública, debe incluir riesgos asociados al incumplimiento de las disposiciones del RGPD y **revisar las medidas de seguridad** que se aplican a los tratamientos, a **la luz de los resultados del análisis de riesgo**, no atendiendo al nivel de los datos tratados, como hasta ahora se hacía con la LOPD.

En el caso de las Administraciones Públicas, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad (ENS) ya citado, pues tienen obligación de estar certificadas contra esquema, en el caso de las ICEX como órgano parlamentario no están obligadas pero me consta que la mayoría sí lo hacen.

7. Se deben **establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas**, para evaluar el riesgo que puedan suponer y para notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados, con obligación de mantener un registro de todos los incidentes de seguridad.

8. Se debe designar un **delegado de protección de datos (DPD).** El Delegado de Protección de Datos (DPD) es una figura prevista en el RGPD, que no existía en nuestra LOPD y cuyo nombramiento es obligado para todas las "autoridades u organismos públicos", incluidas las ICEX. Puede nombrarse un único DPD para varias entidades y puede también ser externo. Su designación debe comunicarse a las autoridades de control.

El Reglamento, establece los criterios para su designación (cualidades profesionales, conocimientos en derecho y práctica en protección de datos), su posición independiente en la organización y sus funciones las define el artículo 39 del RGPD: a) informar y asesorar al Responsable, al Encargado y a los empleados que se ocupen del tratamiento, de las obligaciones que les incumben; b) supervisar el cumplimiento de lo dispuesto en el Reglamento y legislación en general, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; c) cooperar con la autoridad de control y actuar con ella como punto de contacto.

4.- ¿LA PROTECCIÓN DE DATOS PERSONALES COMO "EXCUSA" PARA NO FACILITAR LA INFORMACIÓN SOLICITADA POR LAS ICEX?

No es que resulte habitual, pero en alguna ocasión se ha presentado el supuesto en el que algún fiscalizado se niega a facilitar datos alegando la legislación de protección de datos. La protección de datos, lamentablemente se puede convertir a veces, en una buena excusa para no dar información.

Como ya se ha apuntado, con la nueva regulación, **la base legitimadora de la comunicación de los datos, es la Ley de creación del respectivo ICEX** que establece sus funciones y la obligación de los fiscalizados de facilitar la información solicitada para la fiscalización. La finalidad para la que se comunican los datos, es la del cumplimiento de la función fiscalizadora, función de interés público que ya por sí misma legitima la comunicación de datos, siempre siendo proporcional al fin perseguido. Así pues, desde la óptica del RGPD, en el ámbito de la fiscalización, casi siempre las comunicaciones de datos están amparadas en "*el cumplimiento de una obligación legal aplicable* (art.6.1 c) RGPD) y en "*el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*" (art.6.1 e) RGPD).

Ahora bien, los datos personales que se utilicen por la ICEX, deben ser los estrictamente necesarios, adecuados y pertinentes para poder cumplir la finalidad a la que va orientada. Y lo relevante **es que a nuestro juicio, es la ICEX y no el fiscalizado, la que debe ponderar el equilibrio y la necesidad del uso de los datos personales.** Con el deber, eso sí, de adoptar las medidas necesarias para la correcta tutela del derecho fundamental a la protección de datos de carácter personal.

Así lo declaró la **Agencia Vasca de Protección de datos** en 2006, en una consulta realizada por parte de una Diputación Foral Vasca que planteó **la siguiente consulta**: "*Como vemos, la normativa tributaria prevé la colaboración con el Tribunal Vasco de Cuentas Públicas, como no podía ser de otra forma, en relación exclusivamente con la función fiscalizadora del mismo y que debe limitarse por su propia naturaleza a analizar la actuación por acción u omisión de los órganos de la Administración tributaria en el ejercicio de sus funciones, sin que deba llegar a ocuparse de analizar la concreta situación tributaria de los contribuyentes, ya que la competencia exclusiva al respecto corresponde a la Diputación Foral de Bizkaia*

de conformidad con lo dispuesto en el Concierto económico". En la consulta, la Diputación además sugirió que la publicidad de los informes de obligación legal para el Tribunal, podría tener repercusiones negativas en relación con la protección de datos.

La Agencia Vasca en su informe concluyó que la comunicación de datos al Tribunal, estaba amparada entonces por la antigua LOPD (artículo 11.2d), y que los datos personales que el Tribunal utilice, deben ser los estrictamente necesarios, adecuados y pertinentes para poder cumplir la finalidad a la que va orientada, y en éste punto remarcó que **es el Tribunal y no el fiscalizado el que debe ponderar el equilibrio y la necesidad del uso de los datos personales y que es también éste, quien deberá adoptar las medidas necesarias para la correcta tutela del derecho fundamental a la protección de datos de carácter personal**, pues es responsabilidad del órgano de control externo, conservar debidamente custodiados en sus archivos los papeles de trabajo y borradores que constituyan el soporte de su trabajo y que contengan datos personales, estableciendo para ello los procedimientos necesarios que garanticen su protección y conservación.

CONCLUSIONES

La Constitución Española de 1978 en su artículo 18.4, incorporó la protección al Derecho de la intimidad familiar y personal y el secreto de las comunicaciones. De construcción jurisprudencial posterior, ha sido la diferenciación entre el derecho a la intimidad y el derecho a la protección de los datos personales, que en pocas palabras puede resumirse como el control de las informaciones personales. En desarrollo se aprobó la Ley 15/1999 Orgánica de Protección de Datos Personales, vigente junto con su Reglamento de desarrollo hasta la entrada en vigor el día 25 de mayo de 2018, del nuevo Reglamento Europeo 2016/79, de aplicación directa sin necesidad de transposición ni desarrollo. Finalmente el 5 de diciembre del pasado año se aprobó la Ley Orgánica Ley 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

La principal novedad de la actual legislación reguladora es que mientras la LOPD del año 99, articulaba un sistema de responsabilidad de medios, con el nuevo Reglamento Europeo, el sistema de responsabilidad es de finalidad. Se reemplazan los antiguos ficheros de datos, por el registro de actividades de tratamiento que deben elaborar los responsables, entre ellos las ICEX. Novedad importante es también para las ICEX, la obligatoriedad de contar con una persona delegada en protección de datos que conozca a fondo la organización interna de la ICEX, con sólidos conocimientos jurídicos y que sea especialista en la materia y de carácter independiente.

El tratamiento de datos personales más relevante que lleva a cabo la ICEX, es el relacionado con la actividad fiscalizadora, en la cual se tratan datos comunicados por los Entes fiscalizados. Con la anterior LOPD, dicha comunicación se planteaba como una excepción a la obligación de requerir el consentimiento de los afectados. Actualmente, la nueva regulación lo califica como una comunicación por transmisión a terceros, que debe ampararse en alguno de los criterios de licitud del artículo 6 del Reglamento. En el supuesto de la fiscalización, la comunicación de los datos está basada en el cumplimiento de una obligación legal aplicable al responsable del tratamiento, artículo 6.1c) RGPD.

Para la adaptación a las nuevas obligaciones, los ICEX como responsables de tratamientos de datos, han tenido que cumplir unos mínimos imprescindibles: aprobar y publicar el registro de los tratamientos, (LOPDGDD artículo 31 en relación con el 77.1), que ha sustituido a los ficheros de datos que la antigua LOPD establecía como obligatorios. Se ha tenido que identificar la legitimación de cada uno de los tratamientos de datos, su finalidad y su base jurídica. Además, se ha tenido que revisar tanto la información que se ofrece a los interesados, como las cláusulas de los contratos que se formalicen con terceros encargados de tratamiento y establecer procedimientos de ejercicio de derechos, y también ha sido necesario realizar un análisis de riesgos. Finalmente destacar como novedad importante que las ICEX han tenido que designar una persona delegada de protección de datos.

En el tratamiento de datos para la fiscalización, no con habitualidad pero si ocasionalmente, se presentan supuestos en los que el fiscalizado se opone a facilitar información al OCEX alegando su deber de proteger los datos personales. En estos casos hay que transmitir claramente a los fiscalizados que la comunicación de datos a las ICEX está amparada en el cumplimiento de una obligación legal, a fin de que éstas puedan llevar a cabo la misión de interés público encomendada por Ley. Y es la ICEX y no el fiscalizado quien debe ponderar el equilibrio y la necesidad del uso de los datos personales, debiendo, eso sí, utilizar los datos estrictamente necesarios, adecuados y pertinentes para poder cumplir su finalidad y adoptar las medidas necesarias para la correcta tutela del derecho a la protección de datos.