GRADO EN COMERCIO

TRABAJO FIN DE GRADO

EL BIG DATA COMO HERRAMIENTA EMPRESARIAL DE VALOR. ESTUDIO DE LAS PERCEPCIONES EN LA POBLACIÓN.

NATALIA CELADA MARTÍN

VALLADOLID, junio 2020

FACULTAD DE COMERCIO
Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID

GRADO EN COMERCIO

CURSO 2019 / 2020

TRABAJO FIN DE GRADO

EL BIG DATA COMO HERRAMIENTA EMPRESARIAL DE VALOR. ESTUDIO DE LAS PERCEPCIONES EN LA POBLACIÓN.

Trabajo presentado por: NATALIA CELADA MARTÍN

Firma:

Tutor: OSCAR M. GONZÁLEZ RODRÍGUEZ

Firma:

Valladolid, junio 2020

INDICE

1. INTRODUCCIÓN

No tenemos más que levantar un poco la vista, para tomar conciencia de la cantidad de información que está a nuestro alrededor, en un mundo en el que la tecnología es otros de los elementos más presentes y aplicables que a nuestra realidad respecta. Es por esto, y por la ambición humana que nos caracteriza, como surge una combinación de ambos elementos, una tecnología de la información.

Si trasladamos esto a un campo de estudio capaz de ordenar, filtrar, tratar y utilizar todos esos datos existentes y potenciales, que en múltiples ocasiones han demostrado tener más valor del que podemos pensar en un primer momento, estamos hablando de Big Data (Datos Masivos).

Acudimos a la definición de referencia de este concepto (Gartner, 2001) *"Big data is high-volume, -velocity and -variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making"*. Es decir, activos de información de gran volumen, velocidad y variedad, que exigen formas rentables e innovadoras de procesamiento de información para una mejor comprensión y toma de decisiones

El fin último de comprender mejor los problemas, y por ende, tomar mejores decisiones es lo que convierte a esta ciencia (si así se le puede considerar) en una de las más interesantes para cualquier ámbito de la vida, siendo el comercio uno de los más destacados. Es por esto, que se está convirtiendo en uno de los términos de imprescindible conocimiento y uso en el mundo empresarial. Tanto es así, que hay quién califica al tiempo que vivimos, como "La era de los datos masivos".

Considero al Big Data como un área de estudio con poca notoriedad entre la población general, o al menos que no recibe toda la atención que merece, esto podría justificarse con la confusión que genera, ya que es un sector en constante y acelerado crecimiento, y es probable que la aceptación y asimilación por parte de un público general, exija de su madurez como área del conocimiento.

Según la publicación del profesor de la London School of Economics and Political Science, (Kallinikos. J, 2017) *"Aparece una nueva realidad derivada de las técnicas y de la forma de interpretar y evaluar problemas y situaciones en las que prevalece la disponibilidad de datos y el análisis de los mismos"*

Y es el descubrimiento de esta "nueva realidad" junto con la sospecha del desconocimiento o falta de atención, los que despiertan mi interés personal y motivación hacia los objetivos del trabajo a continuación planteados:

Trataremos desde un marco teórico esta seudociencia, ofreciendo una visión sencilla pero global acerca de lo que el Big Data es capaz, con el fin de incrementar el grado de comprensión de todos aquellos procesos en los que esta está implicada. Enfocado sobre todo desde un punto de vista empresarial, comprenderemos qué es, cómo funciona, las mejores maneras de emplearlo, exponiendo también casos reales que aporten una visión algo más crítica al lector.

Además completamos esta visión global, con un marco práctico en el que llevamos a cabo una encuesta, en la que aparecerán reflejadas percepciones y nociones reales de la población general, ofreciendo así, un punto de vista más sociológico sobre las consecuencias de esta "nueva realidad" para un entorno cercano.

2. BIG DATA

2.1. ¿QUÉ ES EL BIG DATA?

Para empezar a hablar del Big Data y todo lo relacionado con este, tenemos que empezar por delimitar el término. Se define como Big data al conjunto de cantidades masivas de datos estructurados, semiestructurados y no estructurados que tienen el potencial de ser extraídos para obtener información **(Alcalá, 2019)**.

Esta misma fuente, considera que entra en el concepto del Big Data, cualquier tecnología, disciplina o práctica encargada de la recopilación, almacenamiento o procesamiento de estos datos masivos, para su posterior aprovechamiento.

Desde el punto de vista académico, Big Data se ha venido definiendo y caracterizándolo en base a tres dimensiones *Volumen, Variedad* y *Velocidad*, a estas dimensiones habría que añadir las de *veracidad* y *valor* para comprender la capacidad de crear conocimiento a través del Big Data **(Alcalá, 2019)**.

Veamos a continuación y de forma breve cada una de ellas:

Volumen

Es quizás la característica más asociada al concepto de Big Data. Como ya hemos comentado la cantidad de datos generados hoy en día gracias a la mediación de la tecnología es enorme. Además, los avances tecnológicos han permitido no solo generar todos estos datos, sino también, almacenarlos en clusters o la nube.

Velocidad

De la misma manera, todos estos datos son generados de manera continua e instantánea. Esto supone que los datos tengan ciclos de vida cortos, haciendo obsoletos aquellos que instantes antes eran válidos. Parte de la profesionalidad de un experto en la materia, depende de saber detectar los datos útiles cuyo ciclo de vida es corto. Fundamental a la hora de rentabilizar y optimizar el uso adecuado de los mismos.

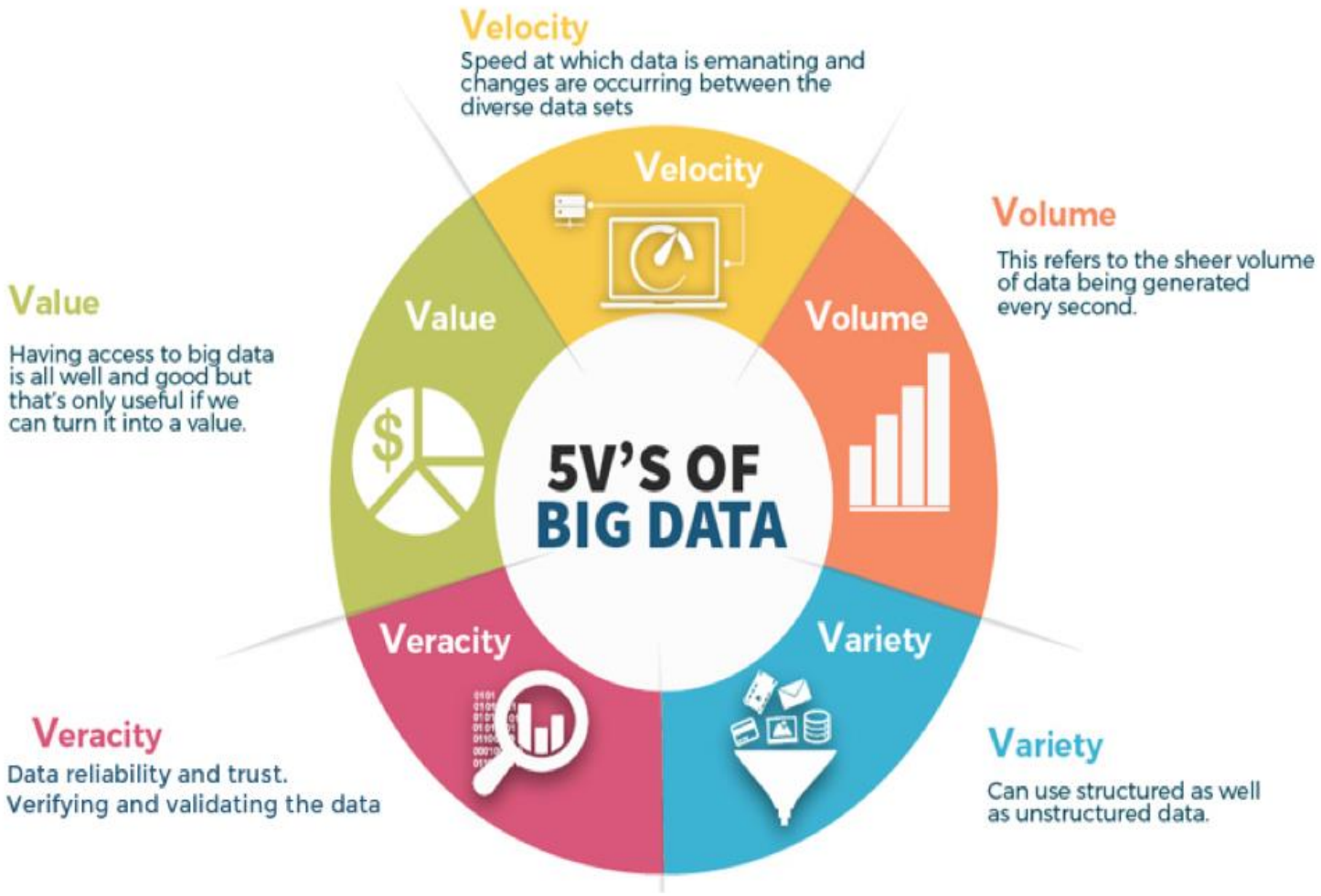

Ilustración 1:"The Data Veracity" Fuente: ***(Nick, 2019)***

Variedad

Estas enormes cantidades de datos son diversos en cuanto a tipología y fuentes de obtención. Esta diversidad es clave para la riqueza de posibilidades del Big Data. Pero a la vez aumenta el grado de complejidad tanto en su almacenamiento como en su procesamiento y análisis.

Veracidad

La veracidad puede entenderse como el grado de confianza que se establece sobre los datos a utilizar y determinará la calidad de los resultados y la confianza en los mismos.

Valor

Fin último del análisis de datos Big Data. Supone el conocimiento e información útil que se puede extraer de estos. Más adelante hablaremos de este verdadero valor capital que suponen a día de hoy para una organización, empresa, incluso figura política la tenencia de estos datos, lo que podría traducirse en poder.

Habiendo citado estas 5 V's que enmarcan el concepto, hagamos ahora un balance de las consecuencias más directas, tanto positivas como negativas de la aplicación de esta ciencia.

2.2. VENTAJAS E IMPLICACIONES

2.2.1. VENTAJAS

Según el Instituto Europeo de Postgrado **(IEP, 2017)** las ventajas que reporta el empleo de estas técnicas de estudio son las siguientes:

Mejora en la toma de decisiones

En la denominada como "Era de los datos", éstos son considerados ya como el nuevo petróleo ¿Qué implica esto? Disponer de un gran volumen de datos estructurados que se puedan interpretar ayuda a las organizaciones a poder tomar una decisión.

Feedback a tiempo real

Incluso en los momentos en los que es necesario tomar una decisión inmediata, el Big Data es un arma muy poderosa puesto que permite recibir y procesar los datos a tiempo real y contar con la información necesaria rápidamente. El Big Data es por encima de todo una tecnología ágil y veloz que permite por ejemplo obtener información a tiempo real del lanzamiento de un producto o el resultado de una estrategia.

Conocimiento del mercado

El conocimiento del mercado en el que se opera puede ayudar no solo a la toma de decisiones, sino también a la localización de posibles oportunidades mediante el tratamiento de estos datos estructurados y comparables. También

puede ayudar a predecir posibles escenarios e incluso a conocer mejor a los consumidores, mediante un análisis segmentado.

Tecnología del presente y del futuro

La tecnología del Big Data está en constante evolución y todo apunta a que jugará un papel todavía más importante en la toma de decisiones futuras. Por ello, cada vez son más las organizaciones que afrontan el reto de la transformación digital por lo que los profesionales de Business Intelligence se convirtieron en uno de los perfiles más demandados en 2017.

Clara está la abundante utilidad que el Big Data nos puede aportar, y de hecho aporta como empresa, como particulares y usuarios. Ahora contrastemos estas con las implicaciones que esto supone, también en base a las afirmaciones del Instituto Europeo de Postgrado **(IEP, 2017)**.

2.2.2. IMPLICACIONES

Como cualquier materia de la vida, a pesar de las múltiples ventajas y utilidades que ya hemos presentado, esta también tiene una parte negativa, o no tan agradable para quienes recibirían sus consecuencias en caso darse, y formulo esta frase en condicional porque no son implicaciones o desventajas seguras las que el Big Data trae consigo, sino más bien una serie de riesgos que el implicado verá aumentados con el uso de la tecnología, y estos son **(IEP, 2017)**:

Ataques informáticos

Haciendo referencia a las 5 V´s citadas anteriormente, la primera hace referencia a la fiabilidad de estos datos, mientras que la segunda se centra en las ventajas que supone para la empresa u organización disponer de esta recopilación de datos para tomar sus decisiones estratégicas.

Dado el valor de esta información, las empresas que cuentan con un sistema de Big Data disponen igualmente de la tecnología más puntera en seguridad puesto que el hackeo de estos datos puede suponer una importante crisis para su corporación.

Pérdida de privacidad

En todas las discusiones sobre los inconvenientes del Big Data surge la palabra “privacidad”. Si muchos de estos datos provienen de redes sociales, formularios, textos… ¿afecta el Big Data a la privacidad del usuario? Un asunto que abre un complejo debate. ¿Por qué es tan importante?

2.3. LA IMPORTANCIA DEL BIG DATA

Sobre todo por parte de las personas con conocimientos certeros a cerca de la materia, y quienes lo estamos descubriendo y aprendiendo a base de investigación, nace en nuestra cabeza la duda de cuál será el valor real y cuantificable de esos datos, y por ahora me respondo pensando que esto depende de su utilidad y del valor que con esta, los datos sean capaces de generar, es decir, en muchas casos incalculable.

Empezaremos a analizar su importancia y peso en el ámbito más obvio, el sector empresarial y de los negocios, expone VIEWNEXT S.A. en su artículo de la importancia del Big Data "Las inversiones en Big Data Analytics son cada vez más frecuentes, y más a la vista quedan sus beneficios para la empresa" **(IBM, 2019)**.

Por su parte, Forbes y McKinsey desde Teradata realizan en 2015, una encuesta a 300 líderes empresariales que aplicaron estas técnicas obteniendo un resultado, en el que 2/3 de los encuestados aseguraban que el Big Data y las iniciativas de analítica aplicadas en sus organizaciones, han tenido un impacto significativo y cuantificable en sus beneficios, afirma un artículo de Network World España **(Network World, 2015)**.

Chris Twogood, vicepresidente de productos, servicios y marketing de Teradata, afirma que el desarrollo de nuevos modelos de negocio, junto con el descubrimiento de nuevas ofertas de producto y la monetización de datos para compañías externas, son las áreas clave en las que se centran las oportunidades del Big Data y la analítica **(Network World, 2015)**.

En seis sectores económicos diferentes, los ejecutivos han visto en el Big Data un valor potencial diferente, siendo los del sector retail o del comercio los que más importancia le dan, ya que consideran que el Big Data y las analíticas son claves para lograr una ventaja competitiva en esta área.

La mayor parte de las empresas están percibiendo el impacto material como resultado de la inversión en ciencia de datos. Uno de cada cinco participantes en la encuesta (21%) está de acuerdo en que el Big Data Analytics es el mejor camino para logar una ventaja competitiva, mientras que el 38% las considera una de las cinco cuestiones más importantes.

Las compañías que están ganando más terreno con sus iniciativas Big Data están analizando más allá de los datos transaccionales, están explorando todo tipo de datos. Los más citados en la encuesta fueron los datos de localización (usados para identificar la localización de un dispositivo físico), seguidos por datos de texto (datos no estructurados tales como mensajes de correo electrónico, diapositivas, documentos de

Word y mensajes instantáneos). Además de explorar estos nuevos tipos de datos, las empresas líderes están combinando datos estructurados y multi-estructurados en un solo ecosistema analítico, lo que permite adquirir nuevos conocimientos y a su vez conduce a nuevas innovaciones.

"Las compañías ya no invierten en Big Data por mero compromiso. Uno de cada cinco participantes en la encuesta está de acuerdo en que Big Data y Analytics constituyen el mejor camino para logar una ventaja competitiva, mientras que el 38% las considera como una de las cinco más importantes áreas de mejora" **(Twogood. C, 2015)**

Con estos datos y conclusiones extraídas de la encuesta, personalmente me atrevería a afirmar que realmente se trata de una disciplina realmente útil en lo que a negocios respecta, y si estuviera en mi mano, no dudaría de su poder ni escatimaría en su desarrollo aplicado a mi empresa.

2.3.1 BIG DATA COMO HERRAMIENTA ANTE LA CRISIS (COVID-19)

Y del mismo modo que podemos citar los beneficios de esta tecnología para la empresa en el desarrollo normal de una sociedad, me gustaría añadir las utilidades que es capaz de reportarnos el Big Data en estos momentos de crisis que actualmente estamos atravesando. Hablamos de la crisis del Covid-19.

Acudo a un artículo publicado en el periódico InnovaSpain en el que explica las aplicaciones que la recogida de datos masivos ha aportado a la sociedad en su lucha contra el virus **(Calero.J, 2020)**.

"Generamos más datos que nunca en la esfera pública y en el ámbito privado. Muchos de ellos incluyen una variable geográfica que se puede utilizar. Los Sistemas de Información Geográfica (GIS) permiten recopilar, analizar y compartir esos datos, y el Covid-19 no es su primer virus. En 2018 fueron empleados para rastrear la aparición de brotes de virus Zika. Las organizaciones de ayuda humanitaria que trabajaban sobre el terreno pudieron compartir la información con los equipos sanitarios y viceversa" **(Calero.J, 2020)**.

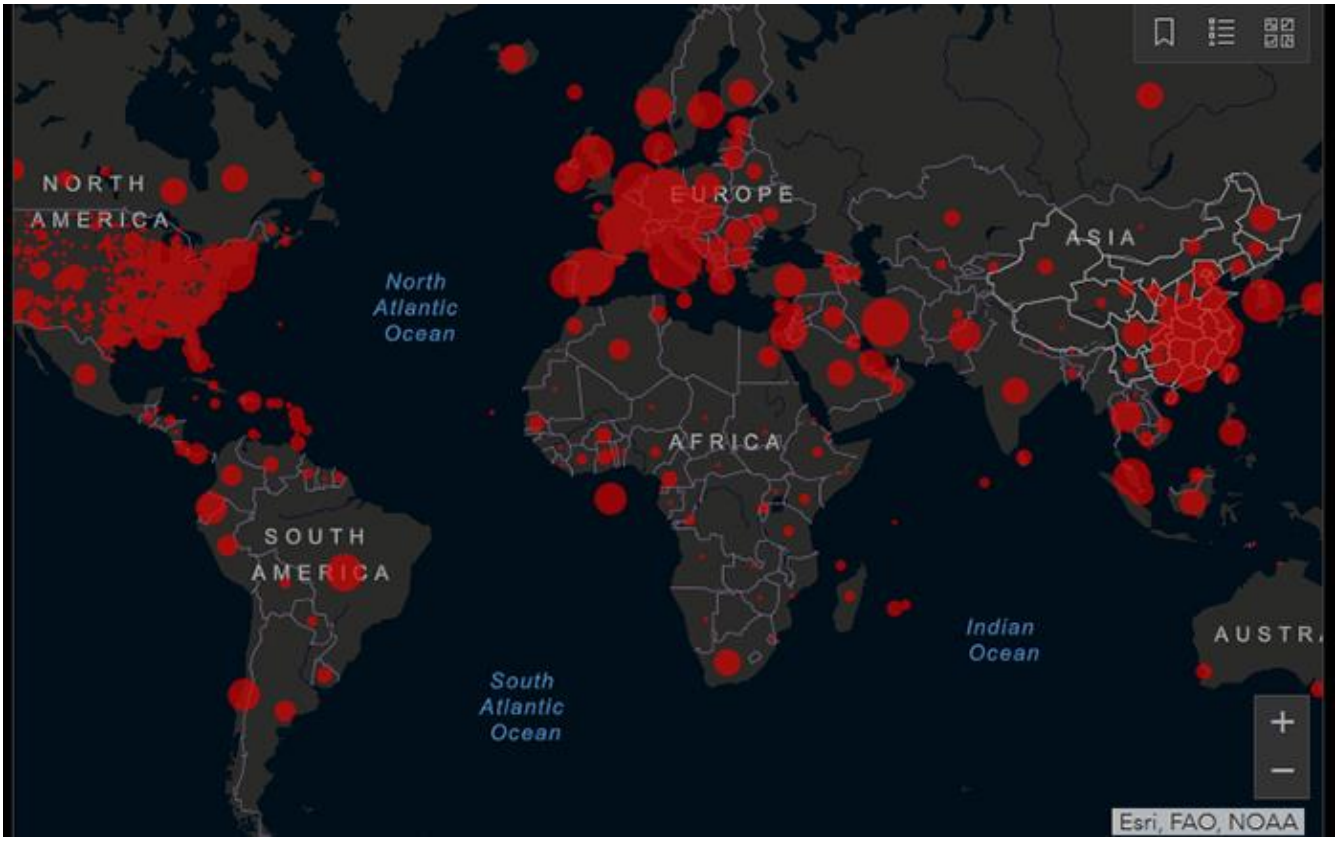

Ilustración 2: Mapa expansión Covid-19 a 12 Mayo 2020. Fuente: imagen de Marca.com.

El escenario derivado del Covid-19 es algo excepcional y resulta difícil establecer comparaciones, no obstante, rescatando el famoso caso del Ébola, se pudo constatar la procedencia de la enfermedad, las pautas de distribución y la posible cantidad de contagios existente en áreas aledañas que no disponían de datos oficiales sobre el virus. En la actual crisis del Covid-19 Data Science aporta a la sociedad **(Calero.J, 2020)**:

1. Programa "Geo voluntarios" El programa que ya cuenta con 500 integrantes, pretende tender puentes para que, gracias a la tecnología, no se pierda tiempo, el activo más valioso en una emergencia. El programa conectará a desarrolladores y expertos en el análisis de datos geográficos con empresas y administraciones públicas que están gestionando la crisis.

   Ahora, los GeoVoluntarios, organizados por equipos, buscan soluciones a problemas concretos y generan todo lo necesario: capas de datos abiertos y análisis de los mismos o desarrollo de aplicaciones que, por ejemplo identifiquen zonas desinfectadas. Por otro lado, prestan apoyo a diferentes organizaciones para que puedan disponer de un cuadro de mando que muestre qué barrios presentan mayor riesgo de propagación

del coronavirus. También trabajan en hacer accesibles distintas capas de información que son difíciles de encontrar, como la ubicación de farmacias, supermercados o puestos de Cruz Roja.

2. De lo local a lo global**.** Organismos públicos y privados, ayuntamientos, administraciones autonómicas o equipos de seguridad y emergencias como Guardia Civil o Cruz Roja, ya utilizaban la tecnología de ***Esri***[1] Ahora el objetivo es distinto, los GIS son un aliado clave en determinadas localizaciones de vital importancia. El objetivo es localizar colectivos vulnerables, gestionar recursos y equipos disponibles, tomar datos sobre el terreno y realizar formularios online geolocalizados para evitar el colapso de hospitales y teléfonos habilitados.

   La OMS utiliza GIS para informar a la población mediante mapas de la situación real a través de datos de fuentes oficiales. La Universidad Johns Hopkins también ha lanzado un mapa que actualiza la información prácticamente en tiempo real a nivel global.

3. Cesión de tecnología y conocimiento. Esri también ha anunciado la cesión gratuita y temporal de su tecnología para las administraciones públicas y empresas que lo necesiten. Durante la situación de emergencia, todos los organismos que lo precisen pueden contactar con Esri para adquirir la tecnología que les permita monitorizar, gestionar, planificar y analizar sus acciones.

   La compañía está proporcionando capas de datos sociodemográficos ya tratadas, procedentes del INE y de AIS, con más de 750 variables sociodemográficas, para España y 1.200 a nivel mundial. Esri ha organizado además un grupo de trabajo especial para tratar los datos generados - COVID-19 GIS Hub España- y dotarlos de fiabilidad antes de compartirlos.

   En una línea similar DataCentric, compañía española veterana en gestión inteligente de los datos, ha abierto sus servicios y productos digitales a aquellas instituciones y empresas involucradas de manera directa en la lucha contra el COVID-19.

[1] Empresa dedicada a las soluciones de información geográfica (http://opendata.esri.es/)

4. Alianzas multidisciplinares y llegar a tiempo**.** Se le plantea a De la Llana por la posibilidad de que, al igual que ha ocurrido con el ecosistema de impresores 3D en España, las compañías de Big data se alíen para apoyar a la causa de forma coordinada **(Ceo de DataCentric, 2019)**.

   Para ello necesitaríamos que el Estado prácticamente interviniera nuestras empresas y viera que los datos y la tecnología pueden ser más importantes y estratégicos que las mascarillas. Nos encantaría poder tener un impacto real en la situación".

   Matemáticos, físicos, tecnólogos, científicos de datos… crecen las voces que reclaman al Gobierno enriquecer la gestión de la crisis con un constructivo cruce de materias. "La apuesta por la multidisciplinariedad debe estar presente en la planificación. Si no, cualquier tarea se convierte en un caos", apunta De la Llana. "Es curioso, pero de esto saben mucho los oficios en albañilería. De haber invertido en un mecanismo de comunicación como el que hay para la renta o las elecciones es probable que ahora no estuviéramos tan saturados" **(De la Llana, 2019)**.

5. Evitar el colapso. La importancia de una buena gestión de datos para ayudar a evitar o aminorar colapsos, puede ser ejemplificada con un caso reciente. Supongamos que un cliente compra una empresa, se produce un fallo en la comunicación entre empresa compradora respecto a la comprada, y los millones de clientes de esta última reaccionan al mismo tiempo saturando los servicios de atención al cliente.

   Según CEO de DataCentric, aquel "tsunami de comunicaciones" actúa generando una cadena descontrolada, momento en el que el único modo de gestionarlo, pasa por aplicar técnicas de Big data, pero en sentido figurado. El Big data no deja de ser un procesamiento paralelo, lo vemos en la crisis actual, algunos hoteles ahora son hospitales para dar salida a pacientes con el objetivo de no saturar un servidor central, el trabajo es repartido en lotes abordados individualmente, esta diversificación sólo posible gracias al uso de disciplinas como la del Big Data evita el colapso.

Estas aportaciones y beneficios a favor de la sociedad en situaciones de crisis son demostrables con la historia del Big Data, concretamente sus inicios: **(Bejarano. A, 2017).**

En el año 1.918 un gran virus azotó al mundo, la gripe española considerada la más devastadora de la historia de la humanidad enfermó a más de 150 millones de personas y se estima cobró la vida de al menos entre 40 y 50 millones de ellas en todo el mundo.

En el año 1.999 otro gran virus asoló a nuestro mundo, la gripe aviar, el virus N1H1, los científicos concluyeron que esta enfermedad se propagaría en el mundo en cuestión de semanas debido a la carencia de una vacuna y que se requería ralentizar la propagación, hasta encontrar la vacuna efectiva, para ello era necesario diseñar y ejecutar un plan que pudiera cumplir este objetivo y minimizar al máximo el número de posibles muertes. Este esfuerzo que requería la participación de todos, permitió la intervención en el plan del buscador Google, que disponía de millones de datos por las búsquedas que realizan diariamente sus usuarios, fue con la ayuda de una modelización matemática que se construyó un programa que logró identificar las zonas de mayor propagación de forma casi instantánea y en tiempo real lo cual ayudó inconmensurablemente a las autoridades sanitarias en el control de la propagación de la enfermedad y la mitigación del impacto en la población **(Bejarano. A, 2017).**

A través de ejemplos tan tangibles como la actual situación de crisis, podemos reconocer la utilidad que aporta esta tecnología ante la necesidad global de soluciones para controlar cifras reales, poblaciones inmensas, llevando un control exhaustivo de la masividad de la población, en definitiva las 5 V´s que caracterizan a esta ciencia ya citadas (*Volumen, Variedad, Velocidad, Veracidad y Valor)*. De no contar con estos datos, las decisiones cruciales se tomarían en base al desconocimiento de la realidad global.

2.3.2 ÉXITO EMPRESARIAL A TRAVÉS DEL BIG DATA

Ya hemos insistido de una manera explicativa en el impacto, importancia y presencia del Big Data en la vida diaria, ahora ejemplificaremos la teoría con 5 breves casos reales, ofrecidos por (Juan. C, 2016)

"Te traemos 5 casos de éxito de Big Data aplicado al Marketing que demuestran cómo con esta nueva tecnología se pueden alcanzar los objetivos marcados, conseguir grandes ventajas competitivas o conocer con mayor precisión los hábitos y comportamientos de los clientes" **(Juan. C, 2016).**

Netflix Es la plataforma de series, películas y documentales online más grande del mundo, la cual supo detectar el gran poder del Big Data para conocer los gustos de sus usuarios cuando su éxito se debe, entre otros factores, a las recomendaciones en base a los patrones de consumo de contenido.

¿La evidencia de su éxito? La serie "House of Cards" una producción propia, que Netflix creó en base a los gustos de los usuarios a partir de los patrones de consumo obtenidos de más de 40 millones de consumidores, utilizando estos,

detectó que lo que más atraía eran contenidos que incluyeran drama, política, sensualidad y poder y, en base a ello, crearon la serie.

T-Mobile Esta empresa de telecomunicaciones consiguió reducir el número de portabilidades hasta un 50% gracias a la aplicación del Big Data. Analizando los datos de las quejas y conversaciones que los clientes dejaban en redes sociales, les permitió conocer a cada cliente y de esta manera, enviaron ofertas especiales a cada uno de ellos, para ofrecerles lo que necesitaran específicamente, de esta manera evitaron que se fueran de la compañía.

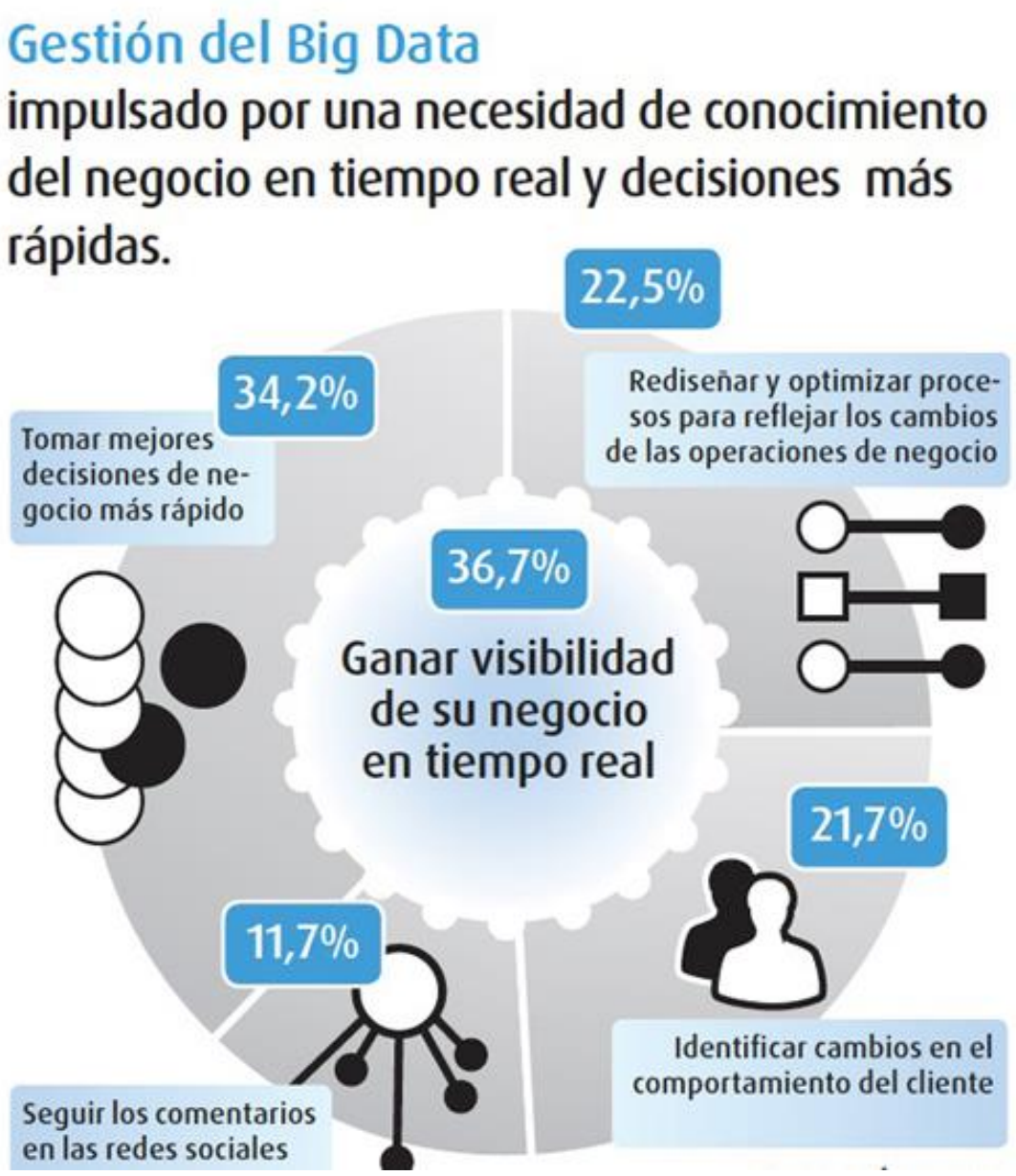

Ilustración 3: Gestión de Big Data; Fuente: ***(Juan.C, 2016)***

Amazon Es otro de los grandes casos de éxito en el uso del Big Data, esta gran empresa sabe perfectamente qué le gusta leer a los consumidores. Gracias a la predicciones en base a búsquedas anteriores, la app ya te habrá ofrecido ese libro que tanto te gusta pero aún no lo sabías. Para conocer los gustos de los clientes, la compañía no sólo se basa en los datos del usuario o búsquedas, sino también en las tendencias que este genera a partir de los amplios catálogos de datos que recopila. Uno de los elementos con los que Amazon ha logrado su éxito es con las recomendaciones que ofrece con cada producto, basadas en las pautas de comportamiento de otros compradores similares al propio usuario.

Target La cadena de distribución Target fue capaz de predecir cuándo sus clientes esperaban un bebé. ¿Y cómo lo han hecho? asignando un ID único a cada cliente, asociado a su tarjeta de crédito para analizar el historial de compra y después generar cupones de descuento.

La compañía se dio cuenta de que las mujeres en su primer trimestre de embarazo repetían ciertos movimientos (como comprar suplementos de magnesio o bolsas grandes como para guardar pañales), lo que les llevó a poder construir un algoritmo capaz de predecir el comportamiento de compra de mujeres embarazadas y, de esta manera, enviarles ofertas específicas para ellas.

Nike La gran empresa de equipación deportiva ahora se está convirtiendo también en una empresa pionera en tecnología e innovación. Con la creación del wearables (dispositivo que permite aplicar inteligencia artificial a objetos como relojes o pulsómetros) la compañía cada vez recopila más información sobre sus clientes y sus hábitos deportivos. Esta valiosa información puede utilizarse para abrir nuevos nichos de mercado.

Estos casos demuestran una vez más que los datos implican conocimiento acerca de una realidad (cualquiera que se quiera o necesite conocer).

Y con la posibilidad, dado el mundo competitivo que nos respecta, nace la necesidad por supervivencia, y con esta, el ingenio que establezca la diferencia.

Teniendo el Big Data como herramienta, con todas las posibilidades que este ofrece ¿Dónde encontramos el límite de este avance, aprovechamiento de recursos, e incremento de la eficiencia? A continuación exponemos un caso de claro éxito empresarial, gracias al aprovechamiento de esta ciencia, en dimensiones que tal vez no habían sido exploradas anteriormente por ninguna otra.

2.3.3. ¿DÓNDE ESTÁ EL LÍMITE DEL PROGRESO? (CASO UBER).

Los casos de éxito expuestos anteriormente ejemplifican la clara ventaja competitiva que supone el empleo del Big Data en la gestión empresarial de una manera explícita y detallada. Sin embargo encontramos otros menos convencionales, aunque muy a la orden del día, pero de los que probablemente no tengamos toda la información acerca su funcionamiento, exponemos el caso la app Uber.

Un artículo del periodista Pablo del Pozo **(Del Pozo, 2017)** nos explica el funcionamiento de esta app para obtener de ella, el máximo rendimiento:

"Como toda empresa grande, maneja una base de datos bastante numerosa y tiene información de valor que le permite brindar un mejor servicio a los conductores y a los clientes" **(Del Pozo, 2017).** Uber maneja dos tipos de información según su destinatario:

1. Para los conductores:

   - Ofrece datos de los clientes de la ciudad en la que se encuentra, utiliza un mapa de calor en que este puede aprovechar las mejores tarifas disponibles a través del conocimiento de las zonas de la ciudad en la que el cliente está dispuesto a pagar un precio superior.

   - También con el fin de rentabilizar su trabajo, le ofrece un mapa del tráfico de la ciudad a tiempo real, así puede detectar las concentraciones, esquivarlas, y ahorrar tiempo de conducción. Asimismo también puede localizar las vías de mejor acceso a su destino.

   - Le permite ver las valoraciones de sus clientes, y de esta manera conocer sus errores más frecuentes y los servicios de mayor valor para sus usuarios.

2. Para el usuario solicitante/ cliente:

   - El vehículo que más cerca está de su ubicación.

   - El menor precio de su zona.

   - La ubicación exacta del vehículo a tiempo real.

"El uso que Uber le da al Big Data es genial porque todas las partes involucradas pueden obtener información de valor" ***(Del Pozo, 2017).***

Uber recopila todos estos datos, los analiza, ordena y procesa, con lo que después lanza un resultado predictivo para cada caso. Esta predicción realizada por el propio sistema, funciona a través de Inteligencia Artificial, que junto con el ***Machine Learning***[2], son áreas de estudio muy conexas con el Big Data, pero en lo que a este trabajo nos respecta, no entraremos en su conocimiento en profundidad, aunque son buenos temas para trabajos futuros.

En definitiva, los datos ofrecidos por la app a través de Big Data, mejoran la oferta y la demanda de ambas partes de la transacción. Uber es un gran ejemplo de éxito del uso del Big Data, no solo por su magnífica optimización del servicio, sino también por la velocidad en que lo hace.

Hasta ahora la explicación del proceso que lleva a cabo la app, no resulta inquietante pues el empleo del algoritmo de búsqueda de Uber (uno de los más interesantes en cuanto al aprovechamiento de Big Data) utiliza datos de proximidad, disponibilidad…

El problema podría plantearse cuando además de estos, la empresa utiliza como herramientas de optimización, datos de los que el usuario ni siquiera sabe que podrían ser extraídos por la app, como: su nivel de batería, la distancia respecto a su casa en combinación con la hora del día en que lo solicita, la zona en la que vive o la disponibilidades de otros medios para llegar su destino, son algunos de los parámetro que Uber podría estar utilizando para obtener como resultado, el nivel de desesperación de un usuario por un vehículo y su capacidad económica en función de la zona en la que vive. Teniendo estos dos como determinantes a la hora de establecer el precio, pudiendo así obtener esta máxima rentabilidad de la que hablábamos anteriormente.

Desde un punto de vista empresarial es perfecto:

- El conductor puede saber que cliente pagará más por sus servicios cuando se encuentre en la situación de elegir. Asegurando otros clientes que tal vez consideren esas tarifas demasiado caras.

- Y el cliente se asegura de que cuando su necesidad de vehículo sea urgente, la obtendrá en el menor tiempo posible.

[2] Aprendizaje automático, disciplina científica del campo de la inteligencia artificial, que crea sistemas capaces de aprender en base a la experiencia, de forma automática.

Este último planteamiento acerca del funcionamiento "oculto" de la app, es extraído de lo que podría considerase una fuente menos fiable, obtenemos este recurso del programa de radio "Si sí o si no" de la cadena SER, protagonizado por Jorge Ponce, aunque no se trata de un programa académico sino uno de entretenimiento, estos datos son contrastados con la periodista especializada en privacidad y datos personales Marta Peirano.

Pese a esta falta de exactitud y evidencia probada, la información aportada por el programa, personalmente no me resulta extraña ni especialmente desconfiable ya que la empresa ha demostrado la capacidad necesaria para llevarlo a cabo, y dentro de unos marcos legales que a continuación se especificarán (3.2. Reglamento General de Protección de Datos) este tipo de acciones por parte de las empresas, son totalmente probables.

Añadiendo al caso de Uber, otros usos de Big Data por parte de las grandes empresas, de esta misma fuente obtenemos información menos detallada pero en mi opinión igual de interesante de conocer, como el caso de Twitter, dónde se planteaban la intencionalidad de las recomendaciones que la app hace, en cuanto a noticias, artículos y demás lecturas recomendadas. Planteándose a partir de esos datos, la intencionalidad o influencia que esto podía tener entre los usuarios. Siendo estas posibles intencionalidades:

- Reforzar el pensamiento o creencias del usuario, con lecturas de opiniones semejantes a la suya, obteniendo así una autoafirmación en su creencia.

- Mostrarle a al usuarios noticias o artículos en los que se le muestren evidencias de su confusión.

- Recomendarle tweets de usuarios que tienen una opinión muy contraria a la suya, y de esta manera hacerle conocedor de varios puntos de vita para un realidad más amplia.

La respuesta en cuanto a la intencionalidad de las recomendaciones automáticas, o su influencia en nuestro pensamiento no es algo que quedara esclarecido del todo, dependiendo de casos, cada persona puede interpretar la información recibida de una manera u otra, lo que una vez más vuelve a quedar sobre la mesa y tras ejemplos podemos afirmar inequívocamente es *EL PODER DE LOS DATOS.*

2.4. ORIGEN, EVOLUCIÓN Y FUTURO DEL BIG DATA.

Suele ser concebido como una disciplina relativamente nueva, aunque ya muy presente en la vida diaria de todos los que vivimos en esta sociedad informatizada y utilizamos diariamente nuestro Smartphone. Y es cierto que el verdadero avance de la misma es cosa del presente y sobre todo del futuro, pero podemos remontarnos muy atrás para hablar del nacimiento del Big Data.

Existen dos factores principales que han permitido la evolución del Big Data, en primer lugar, los datos de los ya se disponía antes de esta revolución, por supuesto el gran volumen que se está generando de manera continua, y la velocidad de procesamiento a la que es posible analizarlos.

Adquiere Alan Turing el nombre de "Padre de la computación". En los años 30, Alan soñaba con una máquina capaz de realizar tareas de manera autónoma, y de trasladar estas a otras máquinas. Es conocido como el padre de la computación por su investigación durante la II Guerra Mundial, junto a su equipo de inteligencia en Bletchley Park, con el fin de descifrar Enigma, una de las máquinas de cifrado del ejército nazi.

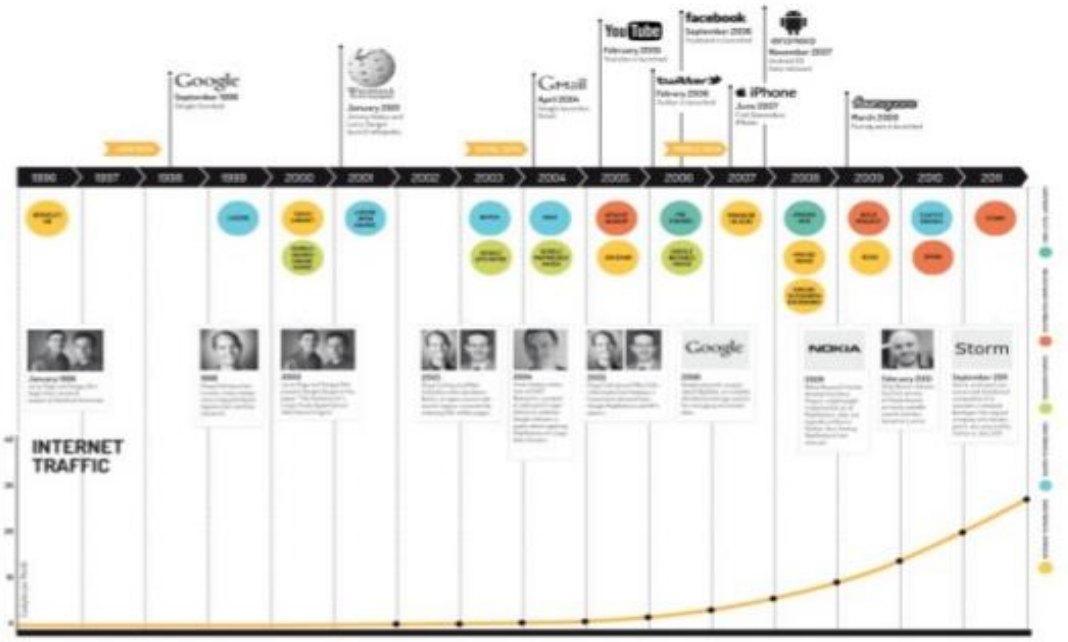

Ilustración 4: Big Data a brief history; Fuente: SlideShare.net

Hagamos ahora un breve repaso del recorrido a través de la historia de Big Data creado a partir de la información obtenida de una fuente anteriormente mencionada **(Alcalá, 2019)**.

Estos son los hechos fundamentales, ordenados cronológicamente desde los inicios de esta ciencia:

1956→ El físico Fritz Rudolf Güntsch crea la primera Memoria Virtual.

1962→ William C. Dersch crea el primer sistema capaz de comprender la voz humana, "Shoebox".

1966→ Se avanza en la sofisticación de los sistemas de computación, suponiendo la posibilidad de automatizar los sistemas de inventario en las empresas.

1989→ Erik Larson menciona el Big Data en el significado actual de la palabra. En este año se popularizan las herramientas de business intelligence para analizar la actividad comercial y el rendimiento de las operaciones. Y con el nacimiento de la WWW (World Wide Web) e Internet se abren los caminos hacia esta era de los Datos masivos.

1992→ Con el aumento exponencial de la cantidad de datos se hace necesaria su gestión, y así aparecen los primeros sistemas de gestión de datos..

En los años comprendidos entre 2009 y 2011 aparecen empresas como Cloudera y Hortonworks. Cuyas principales actividades de empresa, y misión se basan en una mejor gestión de los datos. Con la oferta de estos servicios en el mercado, se abre para las empresas un mundo de posibilidades para mejorar su rendimiento y consecución de objetivos.

2012 → Empleo del poder Big Data para fines políticos. Barack Obama lo usó en su campaña, a fin de conocer las opiniones de los votantes más indecisos e identificar sus canales más utilizados, de esta manera pudo lanzar unos mensajes con un impacto más personalizado.

2016→ El Big Data alcanza un puesto importante en la sociedad. Se generaliza la contratación de expertos en Big Data, el Machine Learning llega a las fábricas y el Internet de las Cosas comienza a abarcar diferentes sectores.

2017→ Los datos llegarían a las masas. La gente puede conocer sus patrones de descanso, su gasto de dinero y se informa de, por ejemplo, sobre la posesión de balón de su equipo de fútbol. Los datos están en todas partes y la población ya se encuentra dispuesta a usarlos.

2.5. DESCUBRIMIENTO DEL CONOCIMIENTO EN LAS BASES DE DATOS (PROCESO KDD).

La sigla KDD es el acrónimo de Knowledge Discovery in Databases (Descubrimiento de Conocimiento en Bases de Datos) designa el conjunto de procesos, técnicas y abordajes que propician el contexto en el cual la minería de datos tendrá lugar **(Landa.J 2016)**.

Dicho proceso tiene como fin extraer conclusiones, que pueden utilizarse en beneficio de la empresa o la persona que lo lleva a cabo, con este proceso se recogen también evidencias y explicaciones que pueden eventualmente llevar a la construcción de un modelo básico de actuación.

Aunque cada proceso dependiendo de la empresa o persona que lo aplique, variará adaptándose a las circunstancias requeridas, podríamos esquematizar su procedimiento básico en 5 pasos:

1º Selección de datos → En esta etapa los datos importantes son extraídos de las fuentes o bases de datos de donde proviene la información.

2º Pre-procesamiento → Se limpian datos inconsistentes o en blanco, obteniendo una estructura de datos adecuada para su transformación.

3º Transformación → Aquí se realizan operaciones de normalización o agregación para consolidar los datos para la fase siguiente.

4º Data mining → En esta fase se aplican modelos para identificar patrones en los datos ya transformados.

5º Interpretación y evaluación → Se identifican patrones obtenidos basados en algunas medidas y se realiza una evaluación de resultados.

Según el experto Javier Landa, KDD (Knowledge Discovery in Databases) es un proceso metodológico y además secuencial, con el fin de encontrar conocimiento en un conjunto de datos en bruto.

Los pasos de este proceso son 9, los enumeramos a continuación:

- Abstracción del escenario
- Selección de datos
- Limpieza y pre-procesamiento
- Transformación de los datos
- Elección de tareas de Minería de Datos
- Elección del algoritmo
- Aplicación del algoritmo
- Evaluación e interpretación
- Entendimiento del conocimiento.

Antes de esto definamos el conjunto de datos, como una colección de información (cuantitativa o cualitativa) compuesta por variables o atributos (columnas) que representan las propiedades de un fenómeno o suceso, y casos (filas) que identifican los diferentes sucesos que se presentaron en el escenario. Una vez contextualizado el proceso KDD, como un conjunto actuaciones sobre cierta información en bruto, explicamos sus fases de una manera más detallada:

1 – Abstracción del escenario.

No todo es matemática y estadística, sino entender la problemática a la que nos vamos a enfrentar y tener contexto para proponer soluciones viables y reales, ya que me ha tocado ver propuestas absurdas. Es importante conocer las propiedades, limitaciones y reglas del escenario en estudio, para posteriormente definir las metas a alcanzar.

2 – Selección de los datos.

Del conjunto de datos recolectados y ya definidos los objetivos a alcanzar, se deben elegir los disponibles para realizar el estudio, e integrarlos en uno solo que puedan favorecer al alcance de los objetivos del análisis. Muchas veces esta información puede encontrarse en una misma fuente (estudio centralizado) o pueden estar distribuidos.

3 – Limpieza y pre-procesamiento.

En esta etapa se determina la confiabilidad de la información, es decir, realizar tareas que garanticen la utilidad de los datos. Para esto se hace la limpieza de datos (tratamiento de datos perdidos o remover valores atípicos). Esto implica eliminar variables o atributos con datos faltantes o eliminar información no útil para este tipo de tareas como el texto (aunque puede utilizarse para hacer Minería de Texto, que es otro asunto).

4 – Transformación de los datos.

En esta etapa se mejora la calidad de los datos con transformaciones que involucran ya sea reducción de dimensionalidad (disminuir la cantidad de variables del conjunto de datos) o bien transformaciones como por ejemplo convertir los valores que son números a categóricos (discretización).

5 – Selección de la apropiada tarea de Minería de Datos.

Fase en la que se refiere a elegir el paradigma apropiado de Minería de Datos, ya sea la clasificación, regresión o agrupación, según los objetivos que se haya planteado para la investigación (predicción o descripción), la primera ocupada para encontrar un modelo que sea utilizada para casos futuros y desconocidos; mientras que la segunda solo para observar su comportamiento.

6 – Elección del algoritmo de Minería de Datos.

Posteriormente se procede a seleccionar la técnica o algoritmo, o incluso más de uno para la búsqueda del patrón y obtener conocimiento. El meta-aprendizaje se enfoca en explicar la razón por la que un algoritmo funciona mejor en determinadas problemáticas, y para cada técnica existen diferentes posibilidades de cómo seleccionarlas. Cada algoritmo tiene su propia esencia, su propia manera de trabajar y obtener los resultados, por lo que es recomendable conocer las propiedades de aquellos candidatos a utilizar y ver cual se ajusta mejor a los datos. En 2015 se publicó un artículo que intenta abordar justamente este problema, realizando una comparación entre diferentes clasificadores en distintas problemáticas. Puedes verlo dando clic aquí.

7 – Aplicación del algoritmo.

Por fin, una vez seleccionado las técnicas el paso siguiente es aplicarlo a los datos ya seleccionados, limpiados y procesados. Es posible que la ejecución de los algoritmos sean varias intentando ajustar los parámetros que optimicen los resultados. Estos parámetros varían de acuerdo al método seleccionado.

8 – Evaluación.

Una vez aplicado los algoritmos al conjunto de datos, procedemos a evaluar los patrones que se generaron y el rendimiento que se obtuvo para verificar que cumpla con las metas planteadas en las primeras fases. Para realizar esta evaluación existe una técnica que se llama Validación Cruzada (también abordado en el artículo anterior), el cual realiza una partición de los datos dividiéndose en entrenamiento (que servirán para crear el modelo) y prueba

(que serán utilizados para ver que en verdad funciona el algoritmo y realiza su trabajo bien).

9 – Aplicación

Si todos los pasos se siguen correctamente y los resultados de la evaluación se satisfacen, la última etapa es simplemente aplicar el conocimiento encontrado al contexto y comenzar a resolver sus problemáticas. Si de lo contrario, los resultados no son satisfactorios entonces es necesario regresar a las anteriores etapas a realizar algún ajuste, analizando desde la selección de los datos hasta en la etapa de evaluación **(Landa.J, 2018).**

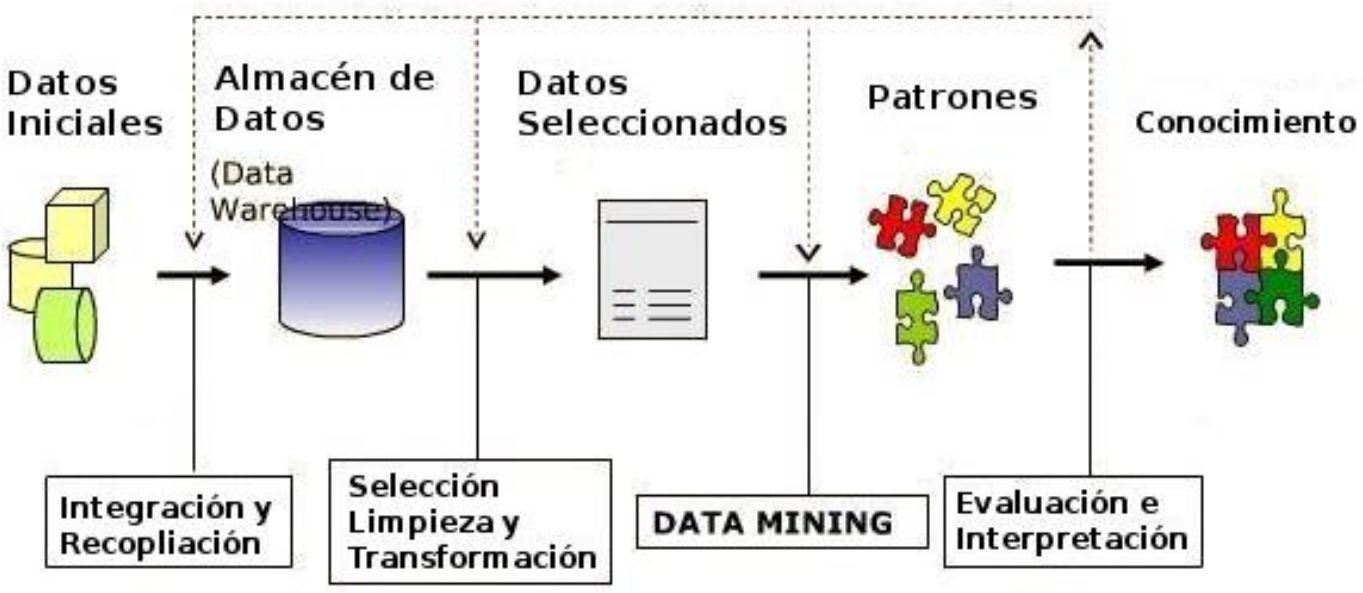

Ilustración 5: Proceso KDD; Fuente: **(Camino a las TIC, 2017).**

Como hemos hecho visible en esta explicación, el proceso KDD engloba al conjunto de procesos previos y posteriores al verdadero tratamiento de los datos, es decir las tareas nucleares del proceso, nos referimos al data mining o minería de datos.

Este proceso equivale a las fases 5, 6 y 7 del KDD, sin embargo cada una de las fases mencionadas tiene su complejidad y especialidad. Hablar de Minería de Datos implica familiarización de las matemáticas y no solamente en su aplicación, va más allá de su entendimiento, pues hasta una medida tan simple como un promedio, tiene un gran significado en esta metodología, por lo que consideramos conveniente el siguiente apartado.

2.5.1. EL NÚCELO DEL PROCESO KADD - LA MINERÍA DE DATOS (DATA MINING)

El concepto de minería de datos se refiere al proceso de extraer información, y de entre esta, obtener patrones del gran conjunto de datos, normalmente heterogéneos. Se denomina así por una analogía con el proceso de extracción de minerales como el diamante, algo sin duda muy valioso.

La experta en Cloud y Big Data, Marta Benedet, nos explica este proceso de extracción en su artículo en Mediacloud, diferenciándolo en 4 etapas **(Benedet. M, 2018).**

1. Creación de conjuntos de datos. En función del destino seleccionando y qué tipo de datos se necesitan.

2. Exploración de los datos. Este pre-procesamiento es la base para las operaciones siguientes.

3. Preparación de los datos. Se crean las reglas de segmentación, se procede a la limpieza de los datos, la gestión de valores perdidos y la verificación de anomalías. Esta etapa también puede incluir una exploración de datos adicional.

4. Combinación de algoritmos de aprendizaje automático**.** En este momento es cuando realmente la minería de datos comienza a funcionar.

Explica también en su artículo, Marta Benedet, que las técnicas de minería de datos o algoritmos, se eligen en base al tipo de datos a analizar, el tipo de conocimiento o patrones a extraer de los datos, y la forma en la que se utilizará el conocimiento.

Esto nos lleva al aprendizaje de que en un proceso de minería de datos, entran en juego de manera muy influyente, los diferentes tipos de algoritmos de aprendizaje automático. Y una vez más esta explicación nos lleva al siguiente apartado en el que trataremos de comprender, o por lo menos apreciar la complejidad de las metodologías necesarias relacionadas con esta ciencia.

2.5.2. ALGORITMOS DE APRENDIZAJE AUTOMÁTICO

La ya conocida experta en Cloud y Big Data **(Benevet. M, 2018)** hace una diferenciación también entre los procesos de aprendizaje automático, clasificándolos en 4 tipos atendiendo al tipo de dato que tratan, y nos explica brevemente sus respectivos procesos:

1. Algoritmos supervisados. Estos se utilizan para clasificar los datos estructurados de la siguiente manera:

   En la clasificación se generalizan patrones conocidos a la nueva información (por ejemplo, clasificar algunos correos electrónicos como correo no deseado). Mediante la regresión se predicen ciertos valores (precios, temperaturas o tasas). Y con una normalización de los datos, se homogenizan las variables independientes de los conjuntos de datos y reestructuran la información de forma más cohesiva.

2. Algoritmos no supervisados**.** Estos se utilizan para la exploración de datos no etiquetados:

   Se agrupan los datos para detectar patrones distintos. Se establecen reglas de asociación, para identificar la relación entre las variables del conjunto total de datos. (Por ejemplo, qué tipo de acciones se realizan con mayor frecuencia) Y por último, para una visualización e informe posterior, se realiza un resumen.

3. Algoritmos semi-supervisados. Que son una combinación de las metodologías mencionadas anteriormente.

4. Redes neuronales. Se trata de sistemas complejos, necesarios para operaciones de elevado nivel de dificultad, pero estas no las tocaremos ya que el nivel de dificultad de sus acciones no nos respecta.

   Existe una amplia gama de técnicas de minería de datos (algoritmos), que pueden aplicarse en todo tipo de dominios donde se requiere el análisis de datos. Algunos ejemplos de aplicaciones de minería de datos son la detección de fraude, la predicción del precio del mercado de valores o el análisis del comportamiento de los clientes, entre otros.

2.6 ¿CÓMO SE OBTIENEN LOS DATOS?

Hemos hablado de los procesos de extracción, procesamiento, predicción y posterior creación de datos en base a dichos patrones, pero si prestásemos más a tención al proceso de extracción de dichos datos, es posible que nos venga a la mente una cuestión fundamental, y es *¿De dónde se obtienen esos datos? ¿Cuáles son sus fuentes?*

En este sentido podemos dar respuesta a la cuestión, haciendo una clasificación de los datos atendiendo a su fuente de extracción. Aunque no existe un criterio único para categorizar los tipos de datos atendiendo a su origen, una manera de hacerlo muy aceptada, es la que nos expone el profesor **(Rayo. A, 2016).** Esta consta de 5 categorías.

- Web y Redes Sociales
  - Información sobre clicks en vínculos y elementos
  - Búsquedas en Google
  - RRSS (fuentes de datos de Twitter, publicaciones en Facebook, otras RRSS)
  - Contenido Web (páginas, imágenes, enlaces, etc.)

- Comunicación entre máquinas
  - Lecturas RFID
  - Señales GPS
  - Otros sensores (parquímetros, máquinas expendedoras… etc.)

- Transacciones
  - Registros de comunicaciones (llamadas, mensajería, VoIP, etc.)
  - Registros de facturación (pagos con tarjeta, pago online, etc.)

- Biométricos
  - Reconocimiento facial
  - Información genética (ADN)

- Generados por personas
  - Grabaciones a operadores de atención al cliente
  - E-mail
  - Registros médicos electrónicos

Esta clasificación nos muestra las múltiples fuentes de obtención de datos, normalmente de carácter personal, que son recogidos por los diferentes sistemas de extracción.

Al verlos, se nos pueden plantear dos pensamientos:

- *La masividad de los datos*. Aunque esto ya ha sido comentado previamente, hacernos conscientes de la cantidad de motores informáticos que hay extrayendo datos de cada individuo que lo utiliza, activa o pasivamente, personalmente me genera un sentimiento de inmensidad al pensar en la cantidad de datos que existen y se generan cada día.
- *La información personal que es extraída de cada uno:* probablemente muchos nos reconozcamos en la cotidianidad realizando dichas acciones, y pensando más individualmente, nos planteemos la cantidad de datos de todo tipo que están ya registrados, aportando información de todo tipo a cerca nuestra persona, pudiendo generar un sentimiento de vulnerabilidad o falta de intimidad.

Y aludiendo a este último pensamiento, me gustaría conocer más acerca los datos personales que se generan, su alcance, fines y temas referentes a estas metodologías, examinada desde un punto de más personal, relacionado esta vez, con la intimidad de los usuarios.

3. BIG DATA VS. INTIMIDAD (LOS DATOS PERSONALES)

3.1. ¿QUÉ SON LOS DATOS PERSONALES?

El artículo 4 del ***RGPD***[3] recoge en su apartado primero la definición de datos personales. Según dicho artículo, se consideran datos personales *"toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, número de identificación, datos de localización, un identificador en línea, o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*

Es decir, se considera dato personal a aquel que aporta información que permita conocer la identidad de una persona física viva identificada o identificable, es decir "de carne y hueso". Por lo tanto, esta definición excluye a las personas jurídicas y sociedades limitadas o anónimas por definición, salvo excepciones.

También existe un concepto parecido, con el que puede llegar a confundirse, es el concepto de datos relativos a las personas (person-related data) que son lo capaces de identificar a una persona solo en compañía de otros datos relevantes (datos seudonimizados). Cuando los datos personales se anonimizan, de manera irreversible, impide que la persona sea identificable convirtiendo al dato, en no personal.

Antes de la aprobación del actual reglamento, la principal ley aplicable en España era la Ley Orgánica de Protección de Datos (LOPD), pero desde el 25 de mayo de 2018 es el Reglamento General de Protección de Datos o RGPD el que se aplica en todos los estados de la Unión Europea como ley de protección de datos oficial y, por lo tanto, superior a la legislación nacional. Los cambios solo hacen referencia a pequeños detalles. Los principios ya existentes se mantienen, pero el nuevo reglamento los reformula y los amplia claramente, por ejemplo, con obligaciones de información más estrictas en caso de robo de datos o nuevas directrices para la protección de datos en tecnologías innovadoras aún por desarrollar **(Derecho Digital, 2018).**

[3] Reglamento General de Protección de Datos.

3.2. MARCO JURÍDICO DE LA PROTECCIÓN DE DATOS.

Habiendo enmarcado un poco la situación actual, y con una idea de la cantidad de actividades que realizamos al día de manera rutinaria, suponiendo esto una serie de aportaciones a bases de datos, de las que por norma general desconocemos fines, capacidades de alcance, derechos de tratamiento con su respectivo cumplimiento, y demás actividades o usos en los que nos veamos involucrados por error o desconocimiento, veamos qué está establecido legalmente al respecto de su uso, por parte de las empresas entidades u otros usuarios que puedan disponer de los mismos, y utilizar dentro del cumplimiento del marco legal.

La legislación consolidada al respecto, a día de hoy, versa en *la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* Disponible en el Anexo que se encuentra al final del TFG.

A modo de resumen, esta ley, otorga derechos a los ciudadanos, e impone obligaciones a todos aquellos usuarios que tengan como objetivo el trato de datos (empresas, autónomos o personas físicas que ejercen algún tipo de actividad comercial). La nueva ley de protección de datos se diferencia de versiones anteriores en la adición de algo que se conoce como "responsabilidad proactiva", lo que quiere decir que, que se hace necesaria la aplicación de ciertas acciones para la protección de los datos periódicas y de una manera constante e para acogerse con legalidad a este reglamento, digamos que las política con el tiempo se han ido endureciendo para las empresas que los manipulan.

Anteriormente, sólo bastaba con inscribir los datos en cuestión, en un fichero organizado para la agencia española de protección de datos detallando en este, los datos que la empresa posee de sus clientes, trabajadores o terceros, detallando además las finalidades empresariales de dichos datos, en cambio ahora con el nuevo reglamento, los empresarios están obligados a llevar un registro periódico de actividad de sus clientes. Y con este registro, añado las obligaciones que este conlleva:

- Validar sus datos (datos actualizados, previo consentimiento expreso de los usuarios para el tratamiento de sus datos, habiendo sido informados de las finalidades de dichos datos, y con el derecho de una exigibilidad de acceso siempre que este quiera.

- Trazabilidad**.** La empresa tiene la obligación de llevar un registro de todos los datos recogidos y a quién se ceden, por si el afectado ejerce sus derechos de cancelación de datos o el de oposición, en cuyo caso la

empresa tendría la obligación de rastrear hasta dónde han sido cedidos estos datos, para recuperarlos.

- Los fines empresariales en cuestión, deben estar concretados.

- Cesión de datos. En caso de que para los objetivos establecidos, sea necesaria la cesión de datos a terceros, esto debe ser comunicado y registrado en el informe para la agencia española de protección de datos, determinándose los periodos de tenencia de los mismo, los países en lo que se encuentran dichos terceros en caso de que sean cesiones internacionales.

- Las medidas de seguridad tomadas para que esos datos no sean robados, manipulados o enajenados por terceros, deben ser constatadas.

- Permiso expreso**. A**nteriormente bastaba con el consentimiento tácito de quiénes generaban estos datos, pero siguiendo con el principio proactivo de la nueva legislación esto ha cambiado, los clientes y terceros deben ser informados a su vez de: persona responsables de los datos, a quién deben dirigirse, y de qué manera para ejercer sus derechos de cancelación u oposición de tratamiento de datos, el derechos de acceso…También deberán saber en caso de cesión quién manipulará o tendrá acceso a dichos datos especificando el periodo de posesión, e informar de sus propios derechos como consumidores, de la base jurídica de la actividad empresarial desarrollada que justifique dicha tenencia, y de su procedencia o fuente de obtención.

La aplicación de esta nueva normativa, no es obligatoria para todas las empresas, sino que sólo para las que cuentan con más de 250 trabajadores y aquellas que utilizan datos personales de carácter sensible (raza, orientación sexual, datos penales, de salud.)

No obstante su aplicación sí que es recomendable para todas las empresas, ya que este registro de actividad, podría ser relacionado posteriormente con el resto de obligaciones necesarias para cualquier empresa.

En cada empresa debe haber un responsable de datos, cuya función sea el contacto con la agencia española de protección de datos, en caso de infracción por cualquiera de las partes, o en caso de inspección. También cada empresa deberá contar con un delegado certificado de protección de datos, cuya función es el cumplimiento estricto de la normativa vigente.

Otra figura que aparece en una empresa que utiliza los datos de terceros para sus fines empresariales, es el encargado de tratamiento de datos, cuya responsabilidad no está en la tenencia, o posesión de estos datos, ni en su recolección, sin embargo si es el encargado de su uso y tratamiento.

Es decir, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se basa en la obligación empresarial de aquellos que trabajan con los datos, en la transparencia en sus operaciones y fines.

Pero, ¿Por qué y cómo deben protegerse los datos personales? Analicemos ambas cuestiones a continuación.

Todo el mundo debería saber que actualmente, en su totalidad, las grandes empresas de Internet como Google y Facebook, recopilan datos personales de los usuarios a gran escala **(Derecho Digital, 2018)**.

En la mayoría de los casos, los utilizan para colocar publicidad individualizada y, de esta forma, generar beneficios económicos. Pero el Big Data no es un mero factor competitivo, sino el factor considerado más importante por parte de la mayoría de las empresas presentes en el mercado.

Esto contrasta con un consumidor cada vez más maduro y mejor informado que teme, motivadamente, convertirse en una "persona totalmente transparente" mediante la creación de perfiles de usuario detallados. Esta desconfianza hacia las empresas (y también hacia las autoridades) se muestra en los resultados de un estudio que exponemos más adelante.

Los casos recurrentes de robo y abuso de datos a través de correos de ***phishing***[4] y el uso de troyanos alimentan, aún más, este temor porque, cuanto más sensible es la información que circula sobre un individuo, mayor es el peligro asociado para su supervivencia financiera y social.

Por lo tanto, la normativa de protección de datos obliga a las empresas y las autoridades a garantizar la protección de la información de sus usuarios y clientes. **(Derecho Digital, 2018).**

[4] Uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Lo cual implica el cumplimiento de los siguientes principios y prácticas establecidos en el RGPD:

- Legalidad del tratamiento de datos: la recogida, el almacenamiento, la utilización y la transmisión de datos personales a terceros solo está permitida con el consentimiento expreso del interesado.

- Transparencia: las empresas y autoridades públicas están sujetas a una completa rendición de cuentas, documentación y pruebas. A petición del interesado, deberá informar sobre todos los procedimientos de tratamiento de sus datos personales.

- Uso limitado: el empleo de datos deberá estar restringido a objetivos específicos y no ser arbitrario.

- Minimización de datos: las organizaciones están obligadas a recopilar solo los datos que sean estrictamente necesarios para el cumplimiento de sus objetivos y a garantizar que el volumen de información almacenada esté, siempre y en todo caso, lo más minimizada posible.

- Corrección del procesamiento de datos: los datos almacenados deben ser siempre correctos y estar actualizados en caso de que sea necesario.

- Limitación del almacenamiento: existe una obligación de eliminar datos con regularidad y desde el momento en que ya no sean necesarios para los objetivos de una organización, si se han almacenado ilegalmente o si ha expirado un período predeterminado para conceder dichos datos.

- Integridad y confidencialidad: las empresas y las autoridades deben tomar amplias medidas para la protección interna de datos personales. Además del uso de programas de encriptación y software de seguridad, esto también incluye la formación detallada de los empleados encargados del procesamiento de datos. (Derecho Digital, 2018).

3.3. TIPOS DE DATOS PERSONALES

Hacer una lista con los tipos de datos que pueden recogerse acerca de una persona es una tarea prácticamente imposible, por eso para distinguirlos un poco dependiendo de su naturaleza acudimos a esta clasificación que hace la redacción de Digital Guide que obtenemos de la web de IONOS by 1&1.

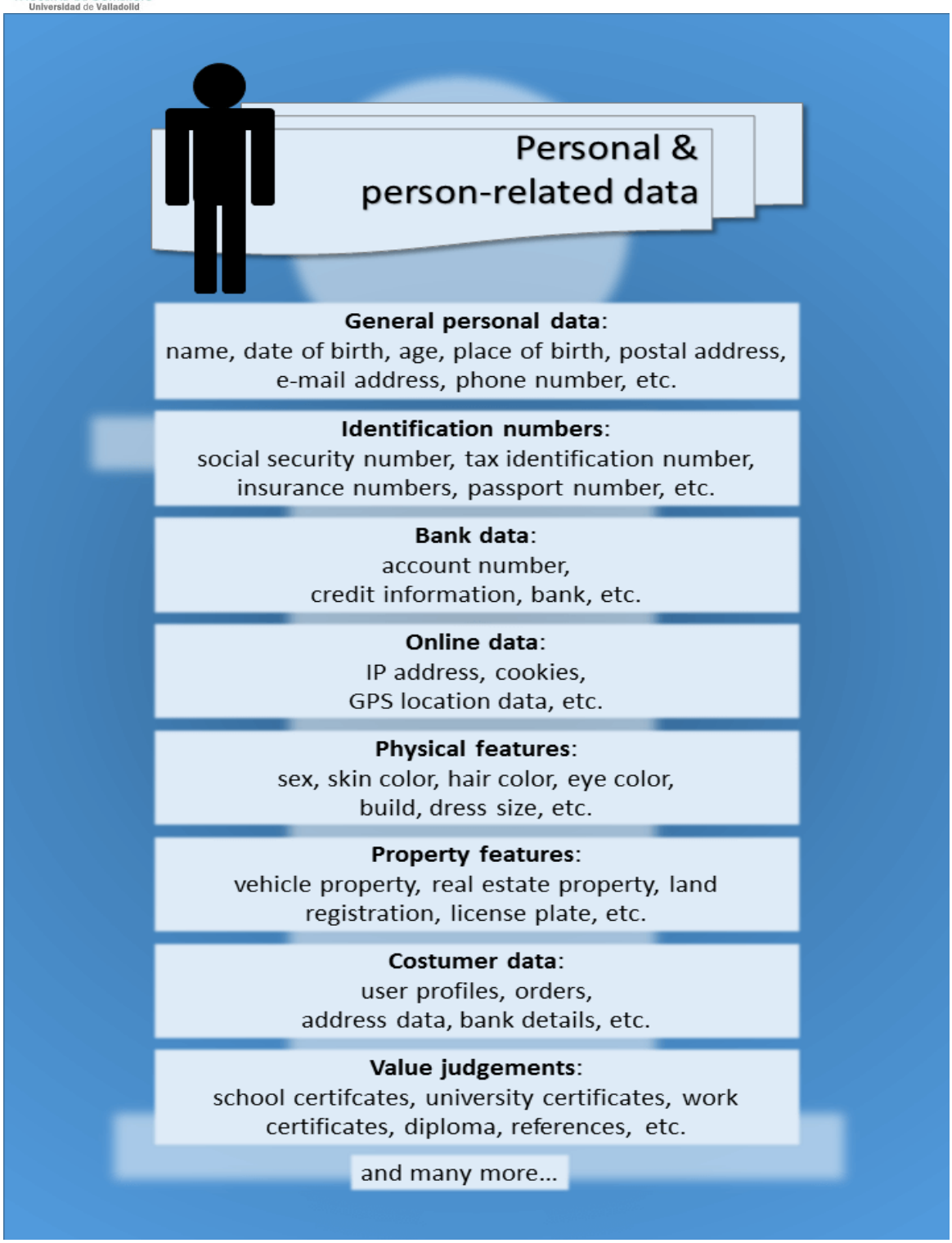

Ilustración 6: "Esquema de datos personales", Fuente: **(Redacción de Digital Guide, 2018)**

Los datos de carácter personal no se limitan únicamente a nombres y apellidos, sino que son una lista amplia y abierta, que va creciendo, y que incluye datos como nuestra voz, número de la Seguridad Social, nuestra dirección o datos económicos. Pero también son datos de carácter personal nuestros «likes» en Facebook, nuestro ADN o nuestra forma de caminar. Ni siquiera nosotros mismos somos conscientes de las formas en las que nuestro propio día a día nos hace identificables.

Ejemplo: Aunque no nos hayamos registrado en un sitio web, éste puede utilizar técnicas analíticas para rastrear las huellas digitales que nuestras actividades han ido dejando hasta terminar identificándonos.

Mención señalada merecen los llamados datos especialmente protegidos (Gil. E, 2015) puesto que son aquellos datos que, de divulgarse de manera indebida, podrían afectar a la esfera más íntima del ser humano, tales como ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud y orientación sexual. Estos datos requieren un nivel de protección mayor y la Ley les reserva un tratamiento especial.

Además de los ejemplos de datos personales mencionados anteriormente, la ley de protección de datos recoge un grupo de datos definidos como especiales relativos a personas físicas. Se trata, en particular, de estos:

- Datos de origen étnico o cultural
- Opiniones políticas, religiosas y filosóficas
- Datos relativos a la salud
- Orientación sexual
- Afiliación sindical
- Además, de conformidad con lo establecido en el artículo 9 del RGPD, también se incluye información genética (análisis de ADN, por ejemplo) y datos biométricos (fotografías y huellas dactilares).

Debido a que se trata de información especialmente sensible, las normas relativas a protegerla, son mucho más estrictas. Por lo tanto, el procesamiento de estos datos sensibles está en principio prohibido, con arreglo a lo establecido en el apartado primero del artículo 9 del RGPD. Esta prohibición solo se exime en dos casos específicos: que la persona a la que se refieren dichos datos haya dado su consentimiento expreso (no basta con una declaración de consentimiento para el tratamiento de datos personales generales) o exista un interés público legítimo en dicha información, por ejemplo, en el contexto de un proceso penal. Si bien el nombramiento de los delegados de protección de datos suele ser una cuestión a considerar por parte del gerente de la empresa, es obligatorio en el caso de que se usen datos personales especiales **(Derecho Digital, 2018)**.

3.4. CONOCIMIENTO Y VALOR QUE LOS USUARIOS DAN A SUS DATOS.

Los medios de comunicación actuales, especialmente las redes sociales, facilitan el intercambio de información y el acceso por parte de terceros a imágenes y datos sobre nuestros gustos, preferencias, hábitos, nuestras relaciones y, en general, aspectos de nuestra vida privada que deben ser garantizados y tutelados en virtud del derecho a la protección de datos.

Este derecho a la protección de datos ha sido definido por nuestros tribunales, modificado y actualizado con el paso del tiempo, estableciendo que «*consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, permitiendo también al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o su uso. Su carácter de derecho fundamental le otorga determinadas características, como la de ser irrenunciable y el hecho de prevalecer sobre otros derechos no fundamentales*»

Tal y como está establecido en esta ley, personalmente y a primer juicio, pensaría que la mayor parte de las personas y usuarios de internet, no disfrutan de este derecho en su totalidad, pues muchas veces tendemos a regalar nuestra información a cambio de lo que queremos en el momento de esa web, o dispositivo sin preocuparnos a penas por quién recibirá dichos datos, y que hará con ellos… Este pensamiento proviene de mi reciente preocupación al respecto al ver y observar toda esta información antes detallada.

La llegada de un relativamente nuevo Reglamento General de Protección de Datos (RGPD) para la Unión Europea, (2018) ha hecho a los usuarios y consumidores más conscientes y documentados que nunca acerca de esta recopilación y utilización de su información personal.

Hallamos un informe de Privacidad de datos en el mundo (Lo que realmente piensan los consumidores) de la Global Alliance of Data-Driven Marketing Associations (GDMA), impulsado en España por ICEMD, el Insituto de la Economía Digital de ESIC Business & Marketing School **(GDMA, 2018).**

Como ha explicado el fundador y presidente de ***ICEMD***[5] "El tratamiento e intercambio de datos es fundamental para el buen funcionamiento de una economía moderna" **(Marketing Directo, 2018).**

Este estudio realizado con una muestra de población Europea, muestra la existencia de 3 tipos de consumidores diferentes:

- Los pragmáticos (51%) dispuestos a compartir sus datos, siempre y cuando reciban algo a cambio.
- Los consumidores despreocupados (26%).
- Los consumidores fundamentalistas (23%) no están dispuestos a intercambiar ningún tipo de datos personal.

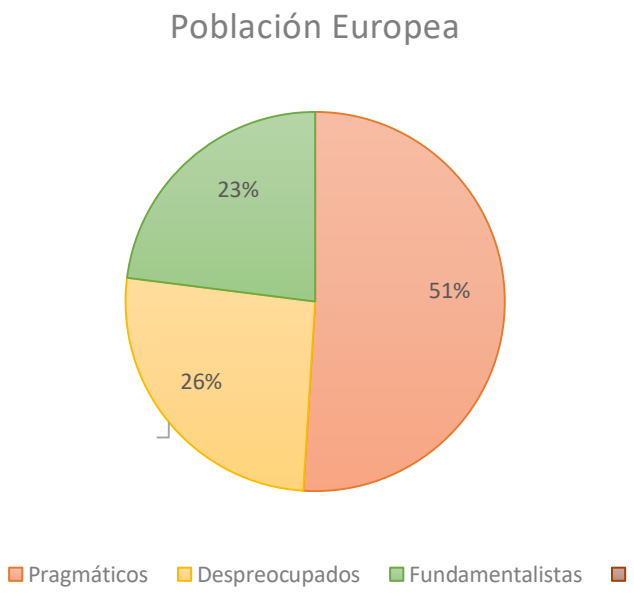

Ilustración 7: Mentalidad europea frente a Big Data, Fuente: elaboración propia.

En base a este mismo informe, también se realiza una investigación para conocer los tres factores más importantes para el consumidor europeo a la hora de intercambiar sin reservas sus datos personales, y el resultado obtenido es el siguiente:

- Tan solo un 26% de los encuestados reclama productos o servicios a cambio de sus datos personales.
- Un 51% exige un nivel de confianza en la organización que la recoge.

[5] Escuela de negocios líder en marketing y economía digital.

- Y la gran mayoría de la población (un 86% de los encuestados) requiere de la trasparencia institucional de quienes recolectarán sus datos, de manera que, lo propios usuarios tengan conocimiento de los fines, responsables y demás datos exigibles a las empresas.

Esto quiere decir que la transparencia es algo que los consumidores sí tenemos muy en cuenta a la hora de tomar nuestras decisiones de confianza y ponencia de datos. Nos importa conocer más de lo que a simple vista se muestra acerca de una empresa cuando esta solicita los datos, o pide permiso de una manera indirecta para hacerlo automáticamente.

Estos resultados a priori, personalmente me sorprenden, pues en un primer momento habría apostado por que el mayor porcentaje de la población encuestada, se reconocería en una situación de desconocimiento a cerca de los tratamientos de datos, certificados de protección de datos por parte de quienes las piden, confusión y desconfianza general, pese a una conducta comportamental que pudiera interpretarse como todo lo contrario, plena confianza. Con esto pretendo hacer alusión a las situaciones en las que seguro muchos nos hemos encontrado más de una vez:

Un momento en el que por ejemplo te encuentras navegando por la red, y para seguir avanzando en tu cometido, es necesario aceptar cierta política de privacidad de datos, incluso introducir directamente algún dato personal en la página.

En ese momento se nos plantean tres opciones, confiar, no confiar en la página, o tratar de averiguar algo más acerca de lo que estaríamos cediendo en caso de aceptar su política de privacidad, para ello podemos leer los mensajes en la ventanas que en un principio pretenden informarte de ello. ¿Cuál sería la opción más acertada? ¿Cuál es la reacción más común de la población española? ¿Cuánto conocimiento tiene la población acerca de los procedimientos reales? Si el conocimiento fuera escaso… ¿Sería a causa una falta de interés por su parte?

Y en caso de conocer las realidades que rodean a la recogida, manipulación, y uso de datos personales, ¿Cambiarían su conducta frente a las políticas de privacidad?

Son muchas las dudas que se nos plantean cuando tratamos de especificar algo tan diverso y personal como las diferentes actitudes de las personas hacia la ciencia de los datos, (una ciencia en crecimiento, pero con total presencia silenciosa en la sociedad.

Para conocer los niveles de conciencia, confianza e interés por parte de la población española, llevaré a cabo una encuesta en la que tomaré como muestra

poblacional el máximo número de personas posible, para así obtener unos resultados más fiables y de los cuales se puedan extraer fenómenos como diferencias en función de la localidad, sexo, profesión o edad. El aprendizaje que pretendo obtener de esta encuesta, es una medición algo más analítica y consistente que una mera intuición o percepción por comentarios oídos, a cerca de lo que la gente realmente piensa, dónde se posiciona, y qué actitud o sentimiento les evoca esta ciencia de datos, por lo que llevaré a cabo un análisis de naturaleza descriptiva.

Lo referente al párrafo anterior, lo veremos en el siguiente capítulo del trabajo. Pero antes, hagamos un análisis de la manera en la que puede influir el Big Data en general, la importancia que se le da a la intimidad personal cuando se trata de recogida de datos, en momentos tan críticos como el que actualmente estamos atravesando.

3.5. DATOS PERSONALES EN TIEMPOS DE PANDEMIA MUNDIAL (COVID-19)

Volviendo sobre un tema actual y en tendencia como lo es la pandemia mundial que estamos sufriendo en estos momentos, el Big Data no se limita a un uso informativo como el que comentábamos en el capítulo 2 sobre su importancia y presencia en nuestras vidas. Las posibles aplicaciones del Big Data frente problemas como este, veremos que pueden suponer soluciones radicales. Encontramos en La Vanguardia, un artículo en que se detallan las soluciones establecidas por el Partido Comunista Chino, (país de origen y principal foco de esta pandemia) como solución a las grandes tasas de contagio, infecciones y muertes, utilizando como herramienta principal, el Big Data.

"China ha pasado en cuestión de semanas de ser el principal foco de la pandemia a casi eliminar las infecciones locales de COVID-19. ¿Un ejemplo para el resto del mundo? Sólo si este está dispuesto a renunciar por completo a su privacidad, algo que en Occidente no parece nada fácil" **(Pandiello. O y Arcas.M, 2020).**

"*El control que ejerce el Partido Comunista Chino sobre la ciudadanía ha permitido al Gobierno de Pekín recabar enormes cantidades de datos (Big Data) relativos a la movilidad de las personas y a su estado de salud, sin consentimiento ni transparencia*", añaden los periodistas.

El caso más sonado es el de la aplicación para móviles bautizada oficialmente como "Código de salud", que fue distribuida en las populares plataformas Alipay y WeChat.

En base a datos introducidos por el propio individuo y a información gubernamental, asigna un código de color a cada persona. Este código (verde, amarillo o rojo) determina la movilidad del individuo, y puede ser requerido para comprobación por las autoridades en la calle, en los accesos a los establecimientos comerciales o en el transporte público.

Se desconoce el criterio de asignación empleado por el Gobierno, ni el uso exacto que hace de los datos. Trasladar este tipo de prácticas a sociedades occidentales con regímenes democráticos y donde la confianza en los Gobiernos está ya de por sí maltrecha, supone no sólo un enorme reto logístico sino también un peligro de cara al futuro, según explican a Efe los especialistas en ciencias de la salud y tecnología de la Escuela Politécnica Federal de Zúrich.

Exponen los periodistas, que mediante el uso de prácticas no transparentes se pondría en peligro la relación entre ciudadanos y Gobiernos, especialmente en países como Francia, Italia o EE.UU. Donde las encuestas indican que ya hay un alto grado de desconfianza.

Los investigadores no se oponen a que los Gobiernos recurran al Big Data (por ejemplo, con la localización de las personas mediante el GPS de sus móviles) para avanzar en las medidas de contención de la pandemia, pero si sostienen que es necesario que estos respeten en todo momento cuatro principios:

1- Transparencia sobre qué datos y cómo se están compilando.

2- Circunscripción de todas las medidas a un marco regulatorio claro.

3- Demostración ante el público de la ausencia de alternativas menos invasivas para la privacidad.

4- Garantía de que habrá un sistema de control independiente.

"*Este es un gran experimento social. Algo que no hemos hecho nunca antes de forma tan continuada y a esta escala y, por tanto, debemos disponer de alguna forma de supervisar este experimento*", concluyen los doctores de la Escuela Politécnica Federal de Zúrich Vayena y Ienca **(Pandiello. O y Arcas.M, 2020).**

Obtenemos de esta misma fuente, el artículo del periodístico de la Vanguardia, el problema derivado de la aplicación de este mismo sistema en una civilización como la europea.

Europa ha creado recientemente una alternativa, que a diferencia de la anterior (por la diferencia de carácter gubernamental) propone el Rastreo de Proximidad Paneuropeo con Preservación de Privacidad (PEPP-PT, por sus siglas en inglés), un

proyecto que pretende ofrecer una solución única y de código abierto, en el intento de erradicar con esta pandemia y siguiendo un ejemplo de éxito como es el caso de China, de una manera adaptada a la legislación aquí vigente para recabar datos móviles en los países de la Unión Europea.

La tecnología, impulsada por 130 expertos de universidades, empresas y fundaciones de ocho países, se apoya en el uso de Bluetooth, "Basada en la participación voluntaria, respeta el anonimato, y no usa ni información personal ni geolocalización", según recogen sus impulsores en su página web. *"PEPP-PT se ofrecerá de manera gratuita a los desarrolladores europeos, y algunos países como Alemania ya trabajan en la puesta en marcha de una aplicación basada en esta tecnología*" Según ha explicado el director del Instituto Robert Koch **(Pandiello. O y Arcas.M, 2020).**

Hasta ahora, la Comisión Europea estaba llevando a cabo una recopilación anónima, a través de los dispositivos móviles individuales, de los movimientos. Analizando estos patrones de movilidad, obteniendo la información que les permitía medir el impacto de las medidas del confinamiento, la intensidad en cuanto al contacto interpersonal por extensión, y de esta manera los riesgos de contaminación.

Este proceso de medición fue llevado a cabo gracias a la colaboración de varias empresas operadoras de telecomunicaciones, como son Deutsche Telekom, Orange, Telefónica, Telecom Italia, Telenor, Telia, A1 Telekom Austria y Vodafone. "El reto entre Big Data y privacidad en Europa es mayúsculo, puesto que durante años las instituciones comunitarias se han esforzado en crear una legislación garantista con los derechos y la privacidad de sus ciudadanos, que halló su máxima expresión en el restrictivo Reglamento General de Protección de Datos (GDPR), que entró en vigor en 2018" **(Vayena.E y Ienca.M, 2020).**

4. CASO PRÁCTICO (ENCUESTA DE PERCEPCIONES)

Realizaremos ahora una encuesta de la que pretendemos obtener información en cuanto a conocimientos, percepciones y opiniones de nuestra muestra seleccionada, y de esta manera, percibir de una manera aproximada el estado del concepto "Big Data" en la población no experta en el tema.

Las preguntas serán cerradas, no queremos agotar demasiado a los participantes voluntarios de este proyecto hablando con un vocabulario técnico, les pediremos que seleccionen la opción con la que más se identifiquen en cuanto a hechos u opiniones, de una manera llevadera e intercalada, no les llevará mucho tiempo responder, incluso puede que algunos quieran aprender más.

De esta manera se pretende identificar patrones de conducta (en cuanto a acciones y pensamientos) en función de las variables ya comentadas. Puede resultar interesante observar fenómenos que no se esperen, el pensamiento de una gran muestra de personas, es impredecible.

4.1. DISEÑO DE LA ENCUESTA.

El cuestionario que se realizó tenía el siguiente texto y preguntas:

Con el fin de estudiar el nivel de conocimiento y confianza de la población respecto a los nuevos medios de investigación, lanzamos este breve cuestionario que rogamos contesten con honestidad.

Forma parte del trabajo de fin de grado de Natalia Celada, los resultados obtenidos serán anónimos e impersonales.

Muchas gracias por tu aportación:)

1. **Edad**
   - (18 – 30)
   - (30 – 50)
   - (50 - 65)
   - Más de 65

2. **Género**
   - Masculino
   - Femenino

3. **Lugar de residencia habitual.** → Respuesta corta.

4. **Nivel de estudios.**
   - Estudios básicos
   - Estudios secundarios
   - Formación profesional
   - Grado universitario
   - Master(s)

5. **Campo de estudios/ profesión.**
   - Negocios/empresariales.
   - Área creativa/ educativa/ religiosa.
   - Ingeniería/tecnología.
   - Ciencias de la salud.
   - Ciencias (física, químicas, matemáticas)
   - Oficio artesanal/agricultura/ganadería.
   - Filologías/literatura/historia.
   - Otro.

6. **¿Conoces el concepto "Big Data"?**
   - Sí
   - No.

7. **¿Y las "cookies"? (ámbito informático)**
   - Sí
   - No

8. **¿Y la "huella digital"? (ámbito informático)**
   - Si
   - No

9. **¿Consideras que formas parte del Big Data?**
   - Yo no utilizo eso.
   - Claro, todos formamos parte.
   - No, siempre he preferido mantenerme al margen de ello.
10. **¿Cuántos de estos procesos crees que son objeto, o están relacionados con la recogida de datos para el Big Data?**

- Redes sociales.
- Lugares frecuentados.
- Cantidad y contenido de mensajes.
- Compras online.
- Compras en tiendas físicas.
- Fotos en el móvil u ordenador.
- Datos médicos y de salud.
- Detección de posibles acciones peligrosas.
- Hábitos en general.

11. ¿Crees que existen apartados en la ley, destinados al tratamiento de los datos personales?

- Sí, conozco esta ley
- Supongo que sí, aunque no conozco su alcance.
- No.

12. ¿Te parece lícita la utilización de estas tecnologías por parte del gobierno, para asegurar el cumplimiento de las normas establecidas?
(Ejemplo: seguimiento GPS, que detecta el incumplimiento del confinamiento)

- Sí
- No, me parece una medida desmesurada.
- No, es una violación de nuestra intimidad.
- No, puede dar lugar a errores.

13. ¿Estás de acuerdo con el análisis de los datos personales (facturación, movilidad, redes sociales, datos médicos…) a fin de crear conocimiento?

- No.
- Sí, considero que es necesario para el desarrollo.
- No me importa.

14. ¿Y de acuerdo con la utilización por parte de las empresas?

- No
- Sí, considero que es necesario para el desarrollo.
- No me importa.

15. Puntúa el nivel de interés que consideras las empresas, siendo 0 un interés mínimo, y 5 máximo interés en la consecución de los siguientes fines:

- Aumentar las ventas. (0 1 2 3 4 5)
- Personalizar y facilitar el proceso de compra. (0 1 2 3 4 5)

- Espionaje invasivo. (0 1 2 3 4 5)
- Adaptar sus acciones de marketing. (0 1 2 3 4 5)
- Fines maliciosos. (0 1 2 3 4 5)
- Vender dichos datos a otras compañías. (0 1 2 3 4 5)

16. **¿Qué frase se acomoda más a tus actuaciones, en cuanto a la protección de tus datos personales?**
    - Siempre me aseguro de que los datos que ofrezco no me resulten invasivos.
    - A veces preferiría no tener que aceptar las políticas de cookies para seguir con mi navegación, pero no hay otra opción.
    - Entiendo que se recojan datos, para mejorar el servicio.
    - No me preocupa.
    - Nunca doy mis datos personales.
    - Nunca me ha preocupado, pero ahora sí.

4.2. ANÁLISIS DE RESULTADOS OBTENIDOS.

Para analizar de una manera ordenada la encuesta, dividimos la encuesta en 4 bloques:

BLOQUE 1: este primer bloque recoge las preguntas de 1 a 5, en las cuales se pretende clasificar el perfil del encuestado (según género, edad y tipo de estudios) De esta manera podemos segmentar nuestra muestra, permitiéndonos observar posibles patrones que se repitan en función del perfil.

BLOQUE 2: las preguntas de 6 a 11, en estas se refleja el grado de conocimiento de nuestra muestra a cerca del Big Data y temas relacionados, pudiendo obtener de sus respuestas, cuál es el concepto más extendido o qué percepciones previas tiene la población a cerca de los conceptos y temas planteados en las preguntas.

BLOQUE 3: recoge las preguntas de 12 a 15, cuyo objetivo es determinar la confianza que los encuestados expresan cuando se trata de sus datos personales, dependiendo qué figura esté utilizando dichos datos, y averiguar cuáles consideran que son sus objetivos para hacerlo.

BLOQUE 4: ponemos fin a la encuesta con las preguntas 16 y 17, en las que se trata de que el encuestado se posicione frente a unas afirmaciones que reflejan pensamiento, pidiéndole que se identifique con la que más se adecue a sus ideas o percepciones generales.

4.2.1. BLOQUE 1: ANÁLISIS SOCIODEMOGRÁFICO.

Empezamos analizando el primer bloque, del cual no pretendemos obtener ningún conocimiento aisladamente, pues su función dentro de la encuesta es segmentar el tipo de muestra que hemos obtenido, y eso haremos.

Es justo puntualizar que nos encontramos ante una encuesta respondida por 380 participantes, un número elevado. Si bien se puede considerar que es una muestra sesgada ya que está condicionada a que la mayor parte de los encuestados tienen estudios referentes a áreas del ámbito económico/empresarial, y entre 18 y 30 años (aunque ha sido lanzada a un público general, en mayor proporción ha sido realizada por miembros de la Facultad de Comercio) el estudio es perfectamente válido y extrapolable a la población en general.

Tomando esta predominancia [población joven, con estudios universitarios del campo económico, con residencia habitual en Valladolid] como un fenómeno propio del sesgo de la muestra, y no como un dato objeto de estudio. Analicemos el resto:

En cuanto a género nuestra muestra es bastante equitativa, 184 hombres, y 195 mujeres contestaron a la encuesta.

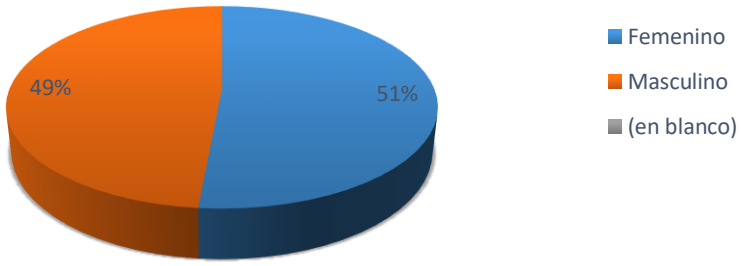

Ilustración 8: Distribución de la muestra por género. Fuente: elaboración propia.

Como ya señalamos anteriormente, existe un rango de edad predominante entre nuestra muestra, 281 encuestado de los 380, tiene entre 18 y 30 años, y el segundo rango de edad que le sigue se encuentra entre los 50 y los 65 años de edad con 62 participantes pertenecientes a este rango.

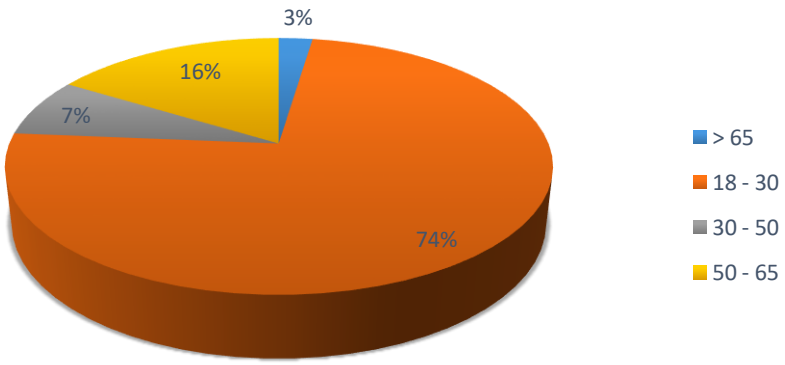

Ilustración 9: Distribución de la muestra por edad. Fuente: elaboración propia.

Atendiendo a la localidad en la que nuestros encuestados residen, existe una predominancia de residentes en Valladolid, 204 encuestados de esta localidad, también tenemos una notable presencia de habitantes en Palencia, 97 de encuestados. Las otras dos localidades que han tenido algo de presencia son Vigo y Madrid, excluyendo estas obtenemos respuestas de otras localidades españolas, incluso personas residentes en el extranjero.

Respecto al nivel de estudios de la muestra, nos encontramos con una población mayormente formada, sólo un 3,1% se sitúan en los estudios básicos, un 11% en estudios secundarios, 11% de formación profesional, frente a un 60% con un Grado universitario, y un 17% en máster.

4.2.2. BLOQUE 2: CONOCIMIENTOS PREVIOS.

En las preguntas 6, 7 y 8 se les plantea a los encuestados 3 conceptos informáticos, [Big Data, Cookies y Huella digital] para saber si los conocen o no. Veamos sus respuestas.

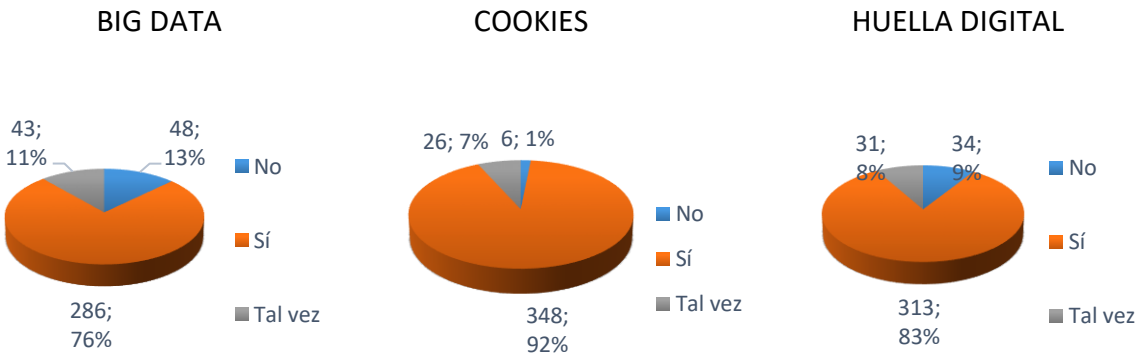

Ilustración 10: ¿Conoces los conceptos "Big Data" "Cookies" y "Huella digital"? Fuente: elaboración propia.

Como se muestra en los gráficos, el término más extendido y popular son las "cookies" pues sólo un 1% de los encuestados responde a la pregunta 7 con "No", un 7% dudoso, y un 92% que asegura conocer el concepto.

El conocimiento del concepto "cookies" por encima del resto, puede deberse a la presencia de la palabra. Cualquier usuario de internet ve aparecer este concepto en mensajes de alerta cada vez que accede a una página web.

El segundo concepto más extendido entre nuestra muestra es la "Huella digital", un 83% reconoce el concepto. Sin embargo "Big Data" aun siendo el más amplio y

general de los conceptos lanzados, es el menos reconocido de los tres, y no por esto desconocido, el 76% de los encuestados afirma conocer el concepto.

Por lo que a estos datos respecta, podemos decir que la muestra con la que trabajamos es conocedora de este tipo de tecnologías en su gran mayoría.

Con Excel como herramienta, realizamos una tabla de respuestas por encuestado, en la que contamos el número de personas que han contestado afirmativamente a las tres preguntas consecutivas, siendo este el grupo de encuestados que conoce los tres conceptos, y el resto de combinaciones de respuestas para agrupar a los encuestados, identificando también a aquel grupo que no conoce ninguno de ellos:

BIG DATA	COOKIES	HUELLA DIGITAL	
Si	Si	si	**240**
Si	Si	no	**18**
Si	No	si	**0**
Si	No	no	**0**
No	Si	si	**29**
No	Si	no	**5**
No	No	si	**1**
No	No	no	**2**

Tabla 1: Frecuencia de conocimiento por encuestado. Fuente: elaboración propia.

Con esta tabla podemos observar los siguientes resultados:

- Sólo 2 encuestados no conocen ninguno de los tres conceptos.
- 240 conocen los tres.
- 29 de ellos conocen cookies y huella digital, pero no conocen Big Data.
- Y ninguno de los que afirma conocer “Big Data”, desconoce alguno de los otros dos conceptos señalados.

Esto nos confirma lo ya señalado en los porcentajes de respuesta de cada concepto por separado: El concepto más desconocido, de entre los ofrecidos, es el de “Big Data” en contraposición con el concepto más extendido, las “Cookies” y el más conocido son las “Cookies”.

Estos resultados nos llevan a pensar los motivos de los resultados que se muestran:

Cuando se habla de un término tan general como es "Big Data", existe gran desconocimiento por parte de la población. Esto podría deberse a que son pocos los que conocen los procesos que hay detrás de sus acciones cotidianas, pues el término "Big Data" no forma parte del vocabulario cotidiano a no ser que estemos enfocados en el conocimiento de dicha metodología de trabajo, en un ámbito más profesional.

Ahora ahondaremos un poco más en la raíz y detalles de este desconocimiento a cerca del concepto, con la pregunta **9 - ¿Consideras que formas parte del Big Data?** Obtenemos los siguientes resultados:

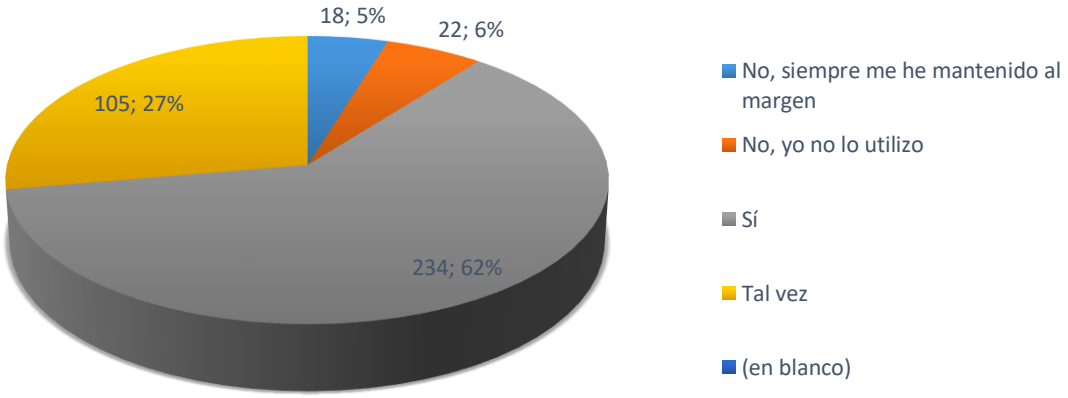

Ilustración 11: ¿Consideras que formas parte del Big Data? Fuente: elaboración propia.

Observamos que el 62% de los encuestados se considera objeto de estudio de esta área de conocimiento, un 27% lo pone en duda, y un 11% (5+6), unificando 2 de las opciones en las que se niega la pertenecer al Big Data.

En capítulos anteriores establecimos que el Big Data está muy presente en nuestras vidas, siendo cada vez más el número de procesos cotidianos, objeto de su estudio, luego establecemos que todos formamos parte del Big Data.

Ahora combinaremos estas respuestas con las de la pregunta **6 - ¿Conoces el concepto Big Data?** A fin de conocer el porcentaje de encuestados que afirmaron conocer el concepto, y sin embargo no se consideran parte del mismo.

Así como aquellos que no conocía el concepto, y sin embargo tienen una clara opinión de negación respecto a la pertenencia a este.

6- Conocen concepto.	9- Forman parte de los procesos		
si	si	**212**	**56%**
si	no	**9**	**2%**
si	tal vez	**53**	**14%**
no	si	**4**	**1%**
no	no	**14**	**4%**
no	tal vez	**29**	**8%**
tal vez	si	**16**	**4%**
tal vez	no	**11**	**3%**
tal vez	tal vez	**22**	**6%**

Tabla 2: Pertenencia en función del conocimiento previo. Fuente: elaboración propia.

En esta tabla, hemos hecho todas las combinaciones de posibles respuestas ante estas dos preguntas, unificando en el caso de la pregunta 9, las dos respuestas que niegan la pertenencia al Big Data.

El hecho de ofrecer las opciones **"No, yo no lo utilizo"** y **"No, siempre me he mantenido al margen"** fue con el fin de ampliar las posibilidades de que el encuestado se sitiera más identificado con alguna de las opciones, y lo tuviera más claro a la hora de responder, esta diferenciación también nos permite conocer con más detalle el motivo de que opine que no pertenece al Big Data, se muestra en la Ilustración 11, aunque los porcentajes de ambas respuestas están bastante igualados 5 y 6%. Pero en esta parte del análisis, ambas respuestas pertenecen la respuesta **"no".** Observamos los siguientes fenómenos:

- "Conozco el concepto"

  Un 2% de los encuestados, afirmaba conocer el concepto de Big Data, y sin embargo no se considera parte del mismo. Este porcentaje de la muestra podríamos tomarlos como "confundidos" o "errados".

  Un 14% duda de su pertenencia al Big Data, habiendo afirmado conocer el concepto.

  Y un amplio 56% de los encuestados, conocen el concepto de Big Data y se consideran parte del mismo. Siendo estos los que con mayor seguridad conocen verdaderamente el concepto de Big Data.

- "No conozco el concepto Big Data"

  Este segmento de la población, se muestra como ignorante del concepto, y representa un 13% de los encuestados. Lo más lógico sería que en caso de no conocer el concepto, la respuesta más común a la pregunta 9 fuera **"Tal vez formo parte del Big Data"** y así es, este 13% lo componen:

  Un 8% de los encuestados pone en duda de su pertenencia al Big Data, habiendo reconocido no saber de qué se trata.

  Un 4%, niegan su pertenencia al campo de estudio, sin saber de qué se trata.

  Un curioso 1% admite no saber qué es el Big Data, y aun así considera que forma parte de él. Este último grupo puede tratarse de un segmento que haya oído el concepto, y acerca de su presencia en los procesos, y reconoce abiertamente no saber exactamente de qué se trata.

A través de la pregunta **10 - ¿Cuántos de estos procesos crees que son objeto, o están relacionados con la recogida de datos para el Big Data?** Pretendemos extraer:

- Cuál de los procesos ofrecidos como posibles respuestas, es más y cuál menos asociado a la recogida de datos por parte de nuestra muestra.

- Cuántos encuestados han marcado 1, 2, 3 o todos los procesos, como susceptibles de la recogida de datos.

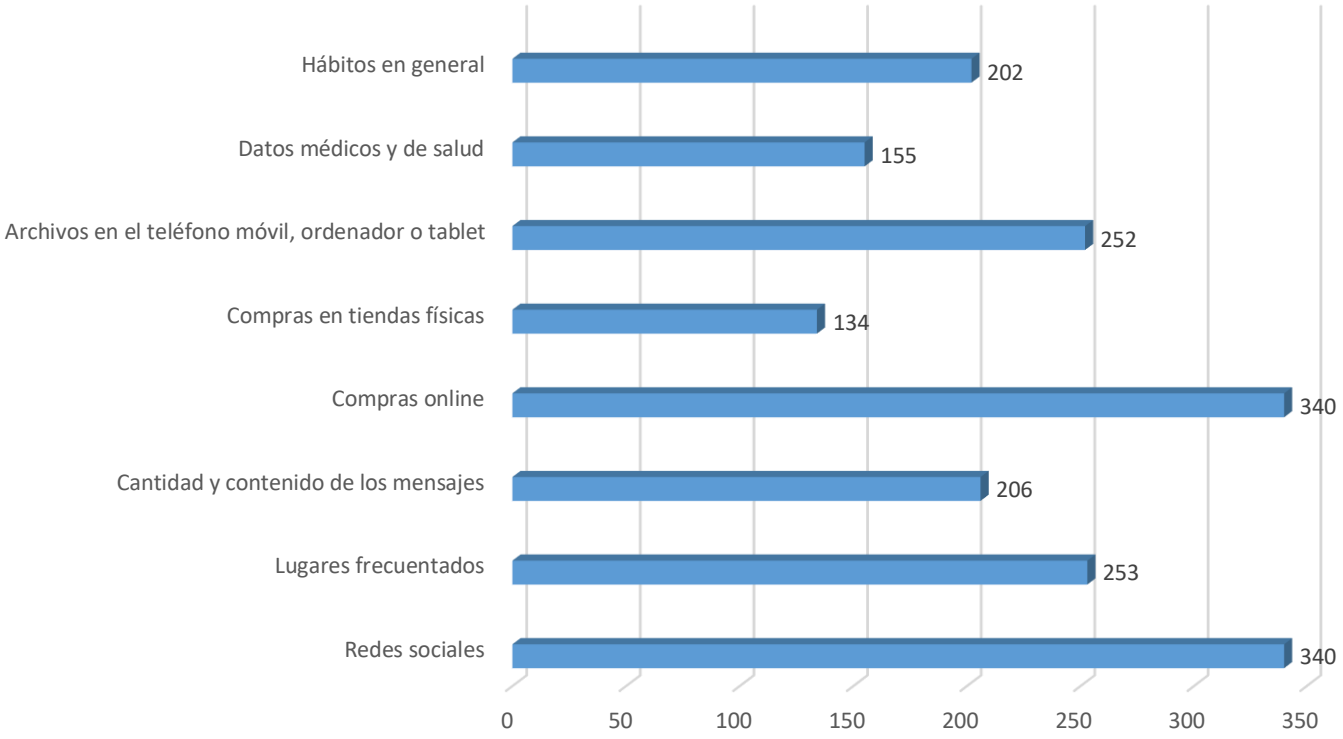

Tabla 3: Asociación de actividades a la recogida de datos. Fuente: elaboración propia.

A través de esta tabla, podemos apreciar las tasas de respuesta, y frecuencia en la que estas han sido seleccionadas como actividades susceptibles de la recogida de datos.

A priori, observamos las dos actividades más relacionadas con el mundo del Big Data y la extracción de datos por nuestros encuestados, estas son "Redes sociales" y "Compras online" con una tasa de asociación del 90,4% por los encuestados.

El hecho de que un gran porcentaje de la muestra, los considere susceptibles, no es un dato que nos sorprenda, pues ambas acciones se realizan mediante dispositivos conectados a internet e implican la introducción activa de datos, por parte del usuario como condición indispensable para su realización. Más llamativo nos resulta ese 9,6% que opina que estas dos acciones, no implican una recogida de datos, tal vez en estudios posteriores podamos averiguar qué argumentos o creencias apoyan esta respuesta por su parte, pero en este, nos limitaremos a conocer sus percepciones finales.

A estos dos conceptos asociados a la recogida de datos en un 90,4%, les siguen "Lugares frecuentados" y "Archivos en el teléfono móvil, ordenador o Tablet" con un 67, y 67,3% de asociación. De esta cifra podemos deducir un porcentaje poblacional que podría creer que sus datos personales no lo son tanto, incluso pudiera estar siendo

víctima del espionaje activo llevado a cabo por parte de algún organismo poderoso, que sienta estos datos como fuera de control.

Dentro de este mismo porcentaje también se incluye la población que efectivamente conoce los procesos de recolección y datos, tiene información acerca de lo que supone tener activada la funcionalidad de localización en el móvil, y conozca con mayor detalle los dispositivos de almacenamiento de archivos contenidos en nuestros dispositivos, como pueden ser La nube, dispositivos externos no conectados a internet… y sus diferencia respecto a una galería de fotos, o lista de música archivadas en el móvil.

No se ha hallado ningún dato veraz, que demuestre o desmienta todos los mitos, rumores y conspiraciones que existen alrededor de los temas que se están tratando. Sabemos que nuestros datos, en el momento en que están registrados en la web, ya corren el riesgo de ser objeto de ataques por parte de ciberdelincuentes, también sabemos que muchas de las acciones que realizamos diariamente de una manera u otra, son susceptibles de registro.

Es por esto, la humanidad de nuestra mente, o simplemente las desconfianza en lo desconocido, es lo que nos puede llevar a pensar, que pese a la existencia de un marco jurídico que nos protege, tal y como se expuso en el apartado 2 de este mismo capítulo, si alguna figura con el suficiente poder e interés por ciertos datos registrados, los quisiera, probablemente podría extraerlos sin que sus dueños se percataran de ello.

También es cierto, que esto solo es una posibilidad, o riesgo existente por el hecho de estar ahí, por lo tanto no significa que esté ocurriendo, y que nosotros personalmente estemos siendo objeto de espionaje activo, pero a mi parecer, forma parte de la mentalidad humana llegar a pensar esto, sobre todo si este tipo de pensamientos, nos es inducido.

De modo que concluimos con que un 67% de la población que considera los lugares frecuentados, y los archivos personales objeto de recogida de datos, por ser conocedores de los métodos empleados, o simples sospechas en base a rumores.

Las siguientes dos acciones más relacionadas con la recogida de datos, son "Cantidad y contenido de mensajes" y "Hábitos en general". Estas dos, son seleccionadas por un 54,8 y 53,7% de los encuestados respectivamente, ambas hacen alusión a información de carácter bastante personal, ya que con este tipo de información podemos conocer estratégicamente cuáles podrían ser sus necesidades, cómo es su vida social, si padecen algún tipo de enfermedad… Son datos que por lo general la mayoría de la población renegaría de su cesión, afirmación que se ve reforzada en los resultados obtenidos en preguntas posteriores de esta misma encuesta.

Existe un sentimiento de resignación por parte de la población a que los datos como de carácter personal y sensible, sean manipulados por terceras personas.

En un 54% son conocedores de esta realidad, y aun así es algo a lo que está dispuestos. Esta postura de conformidad respecto al tema tratado, puede consolidarse con varios pensamientos. Utilizaremos sucesivas preguntas para extraer conclusiones más certeras y concretar con perfiles más detallados de pensamiento.

Por último, podemos hacer alusión a las bajas tasas de asociación de "Compras en tiendas físicas" y "Datos médicos y de salud". Estas tasas pueden deberse a una falta de concreción en cuanto a tipo de compras en tiendas, incluso falta de concreción en cuanto a los datos médicos por los que se pregunta. Cuando pensamos en una compra en tienda física, dependiendo del perfil y el tipo de compra más habitual que realicemos, se nos viene a la mente una situación u otra. Tal vez quien no marcó esta acción como susceptible de recogida de datos, no estaba pensando en una tienda o supermercado en la que tienes club de socio, pagas con tarjeta, o dejas algún tipo de reseña personal de la compra realizada, pues también podemos pensar en compras en efectivo, en pequeños comercios, panaderías o cualquier otro tipo de compra que realmente no implique un tránsito de datos.

Concluyendo con el Bloque 2, la pregunta **11 - ¿Crees que existen apartados en la ley, destinados al tratamiento de los datos personales?** El objeto de esta cuestión era principalmente, recordar a los usuarios (para que lo tengan en cuenta desde aquí en adelante) que frente las acciones que llevan a cabo distintas organizaciones, existe una ley, con sus pertinentes deberes y conductas prohibidas, principalmente con el deber de la información y la prohibición de los usos de mala fe.

Obtenemos estas respuestas:

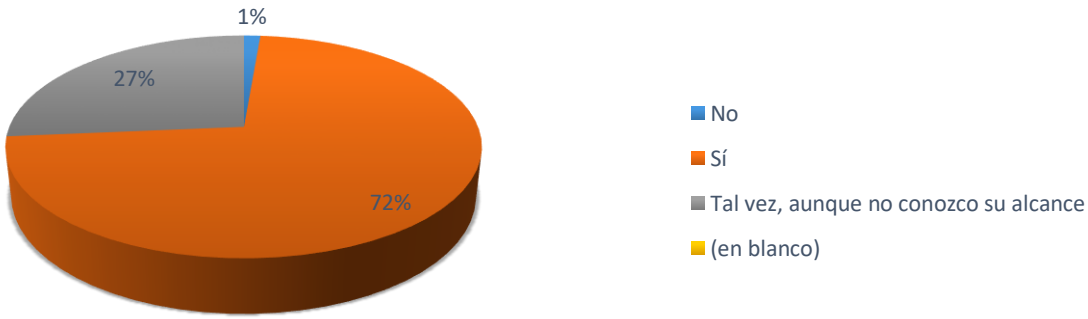

Ilustración 12: ¿Crees que existen apartados en la ley destinados al tratamiento de los datos? Fuente: elaboración propia.

Un 72% de los encuestados afirma conocer de su existencia, un 27% lo supone, y un 1% ha declarado que no existe la ley en cuestión. Estas cifras no nos sorprenden demasiado ya que la ley de protección de datos, es un concepto muy frecuente que la mayoría de nosotros habremos oído, y sólo por el hecho de haberlo preguntarlo, evocamos a la respuesta positiva. Por lo tanto la información que nos ofrece esta pregunta es limitada. Sin embargo, desde este punto de la encuesta podemos suponer que el 99% de los encuestados cuentan con la existencia de esta ley, y de alguna manera cuentan con esta protección.

4.2.3. BLOQUE 3: CONFIANZA EN LA CESIÓN DE DATOS PERSONALES.

El objetivo principal de este bloque no es otro que el de medir la confianza de los usuarios en las distintas entidades que poseen, y tratan sus datos personales, qué idea tienen acerca de ese trato, y conocer sus percepciones respecto a este trabajo de campo, en función de las distintas utilidades.

12 - ¿Te parece lícita la utilización de estas tecnologías por parte del gobierno, para asegurar el cumplimiento de las normas establecidas?.....

Haciendo referencia al apartado justo anteriormente tratado de este mismo capítulo (Datos personales), se nos ofrece la posibilidad de saber qué opina la gente respecto a la situación expuesta en este.

Exponiendo la situación como un simple ejemplo aleatorio (del cual, parte de los encuestados habrá oído hablar, por lo que conocerá con más detalles el caso, y otro porcentaje considerará este, como un simple ejemplo hipotético). Aunque no por hipotético, necesariamente alejado de la realidad, pues es un ejemplo actual de la crítica situación que estamos atravesando, incluso se trata de un tema sensible, lo que podría suponer un aumento del interés en la realización de la encuesta por parte de los participantes.

Los resultados en la ilustración que a continuación se muestra:

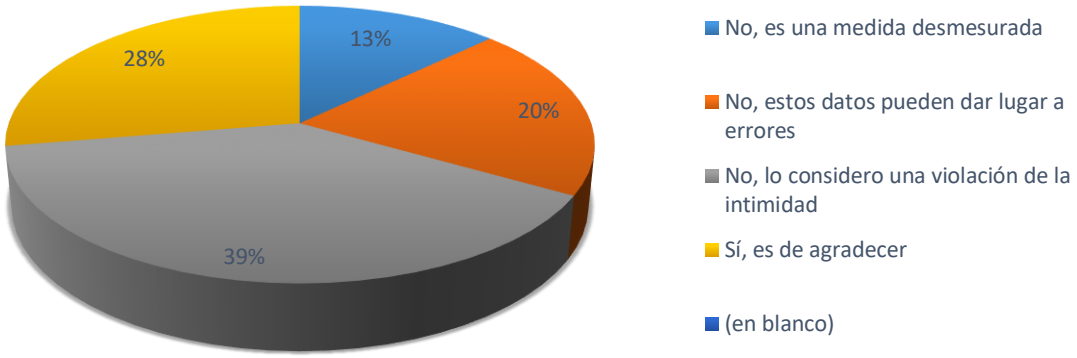

Ilustración 13: Confianza en el Gobierno (en el tratamiento de datos). Fuente: elaboración propia.

Un 28% de los encuestados se posicionan a favor de este tipo de medidas, les parece algo aceptable, y agradecen la labor de control por parte del gobierno a fin de mantener la seguridad. Es decir, el 28% confían sus datos personales al gobierno.

Sin embargo, el 72% está en contra de estas medidas por diversos motivos (indicados en la ilustración 6) destacamos el predominante entre ellos, que es el derecho a la intimidad que reclaman los usuarios. Un ·39% opina que se trata de una violación a su intimidad, cómo podemos ver este pensamiento, es el más común entre los encuestados.

Planteado como lo ha sido (rastreo GPS), una vez más tratando de imaginar los procesos mentales en los que nuestra muestra ha podido desembocar, podemos considerar que el pensamiento más directo y común (sobre todo en el caso de esta mayoría que considera esta práctica, una violación de su intimidad) es la de una figura rastreando la ubicación y tránsitos personales casi individualmente, suponiendo esto un control excesivo en intimidatorio.

La realidad es que esta suposición acerca de los pensamientos de tantas personas, sería demasiado generalizar, aun así, creo que es común haber imaginado alguna vez esa situación exagerada ante información o alerta de este tipo, y su consecutiva sensación de pérdida de la intimidad, inseguridad o malestar.

Aunque racionalmente sabemos que esto no es exactamente así, es cierto que existe el dato de nuestra localización en todo momento (si así tenemos configurado

nuestro dispositivo móvil) pero también es cierto que no tendría demasiado sentido el análisis exhaustivo de todos los datos generados, por la cantidad de personas que lo utilizan. Una pérdida de tiempo a todos los niveles.

Tal y como se expuso en el apartado 3.5 de este trabajo, esta alternativa sólo tendría en cuenta parámetros de distancia, tránsito y número de contactos personales, es decir los necesarios para detectar posibles conductas peligrosas, ante esta situación de alarma en la que se hace tan difícil, y tan necesario al mismo tiempo el cumplimiento de las mismas, planteado en todo momento como medida temporal.

Y tal vez sea este el planteamiento realizado por este 28%, cuya respuesta ha mostrado acuerdo con la medida planteada. Por el momento sólo podemos afirmar, que el porcentaje de desconfianza por parte de la población, respecto al trato de sus datos por parte del gobierno, es bastante superior al porcentaje que sí confiaría sus datos a la gestión del gobierno.

13 - ¿Estás de acuerdo con el análisis de los datos personales (facturación, movilidad, redes sociales, datos médicos…) a fin de crear conocimiento?

En este caso la pregunta formulada, tiene la misma estructura que la anterior, preguntamos opinión o posicionamiento ante la utilización de sus datos personales, pero esta vez no es el gobierno quien los recoge y gestiona, sino una figura que identificaremos como "Investigadores" y el objetivo no es mantener un control por la seguridad, sino el de crear conocimiento, descubrir fenómenos sociológicos, identificar patrones… por y para la ciencia y el conocimiento en general. Los resultados obtenidos:

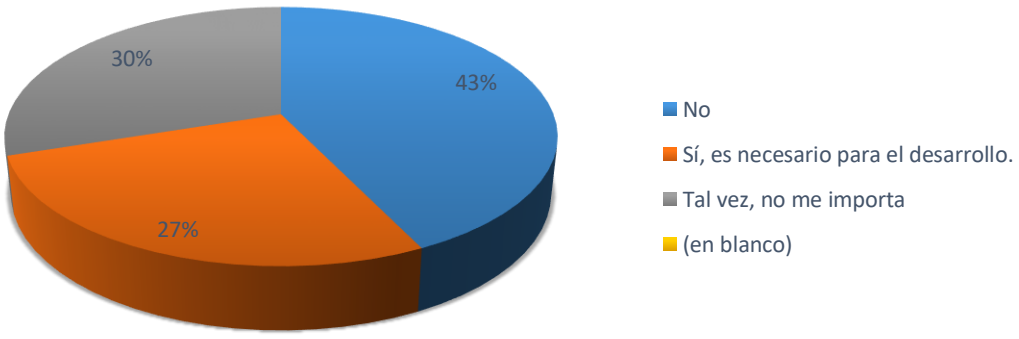

Ilustración 14: Confianza en Investigadores. Fuente: elaboración propia.

Un 43% se opone a la recogida de datos con dicho fin por parte de los investigadores.

El 27% apoya dicha práctica o estudio, y lo considera necesario, y a un 30% de la muestra le trae sin cuidado, estas cifras traducidas en el sentido de la confianza (objeto de estudio) se vería reflejadas como que un 43% no confía en la manipulación de sus datos por los investigadores, frente a un 57% que estaría dispuesto a ceder sus datos a favor de la causa, es decir, confía en los investigadores y analistas de datos.

Antes que esta pregunta fuera planteada, contábamos con una clara división en la población que siempre ha existido, y esta es la población más favorable, y la más reticente al progreso de la ciencia en general, sin necesidad de especificar el campo de avance. Y es cierto que la pregunta planteada podría ser paralela a esta división, pues las personas más interesadas en la investigación y el conocimiento a favor del progreso (tecnológico, conceptual, histórico…) podrían ser las mismas que contestaron afirmativamente, es decir dando consentimiento para la recogida y manipulación de sus datos personales a favor de este progreso.

Por otro lado, aquellos que se niegan a la cesión de sus datos, en este caso la mayoría (43%) podría deberse a la incomodidad que les supone que sus datos sean tratados como objeto de estudio y este sentido, prefieran no cederlos. O por el contrario su oposición ante este tipo de investigaciones, sea consecuencia de una magnificación de los procesos, y simple oposición a la ciencia y el avance.

No obstante interpretaremos esta respuesta de la mayoría, como una reticencia a mostrar sus datos personales, que en este caso es más fuerte que el deseo de progreso y su confianza en estos investigadores.

14 - ¿Y de acuerdo con la utilización por parte de las empresas?

Una vez más, utilizamos esta pregunta indirecta a fin de extraer la confianza que expresan los usuarios, sobre las empresas en esta ocasión.

El siguiente gráfico muestra los resultados:

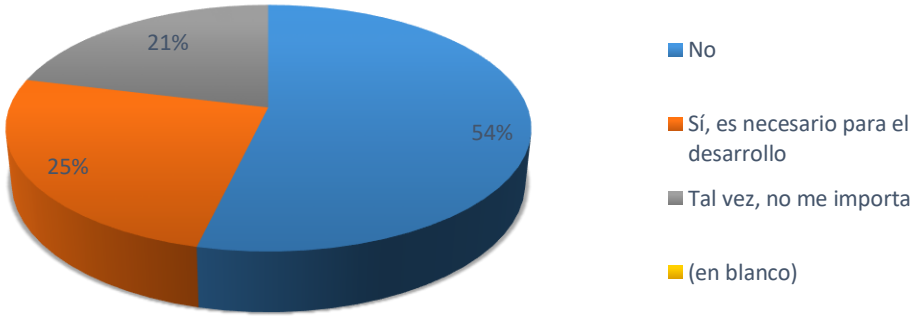

Ilustración 15: Confianza en las empresas. Fuente: elaboración propia.

Cuando se trata de empresas utilizando nuestros datos personales, tan sólo un 25% apoya dicha conducta empresarial, con un 21% que acepta su uso por despreocupación al respecto, frente a una mayoría de 54% que se opone a la utilización de nuestros datos por parte de las empresas.

Estos porcentajes no llamarían tanto la atención en caso de haber sido tomados de una parte aleatoria de la población, pero personalmente me sorprende esta mayoría de respuesta en contra de este tipo de medidas empresariales, en una muestra en la que el 64% estudia o trabaja en el campo económico/ empresarial.

Tal y como se planteó en los apartados 2 y 3 del capítulo sobre Big Data, se exponían las ventajas de este tipo de procesos, y la mayor parte de ellas estaban relacionadas con las ventajas competitivas que podría obtener una empresa de utilizarlas de manera adecuada, este hecho, suponemos que es conocido por cualquier estudiante del campo empresarial, por ello consideramos que estos resultados, más que al desconocimiento, pueden deberse a un cruce de intereses. La población siente a las empresas como organismos sustentados a través de los intereses de la población, como si una de las partes tuviera que perder para que la otra gane, y no como medios para satisfacer sus necesidades de la mejor manera posible.

Haciendo un balance general de las 3 figuras expuestas a la aprobación comparemos sus niveles de oposición o desconfianza hacia a los procesos empleados.

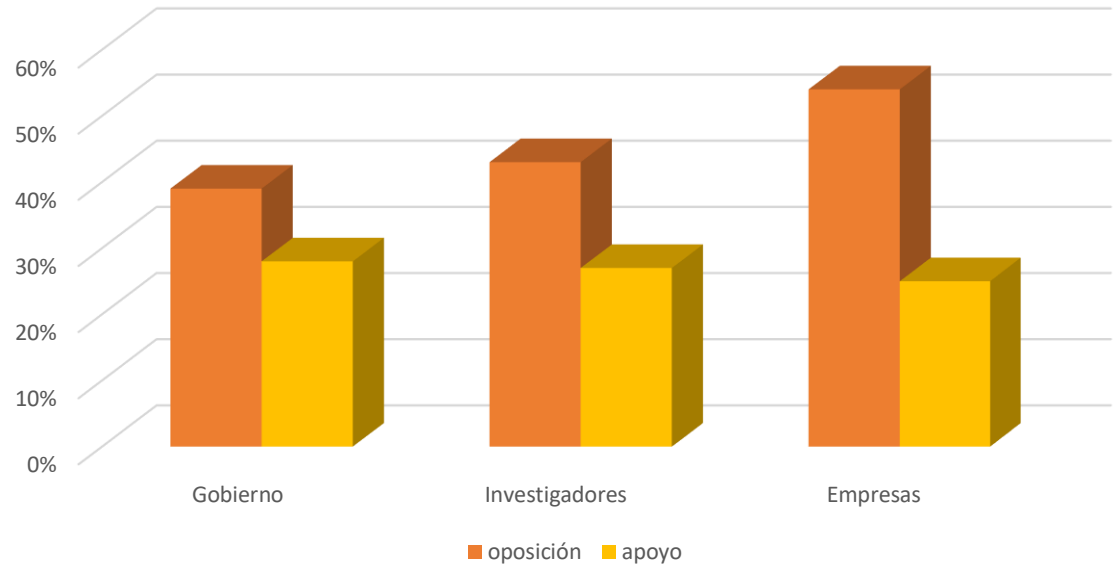

Ilustración 16: Figuras manipuladoras de datos personales. Fuente: elaboración propia.

Se observa que la figura que más desconfianza genera en los usuarios en lo que a recogida de datos se refiere, son las empresas. Este dato puede ser precisamente por este concepto que comentábamos en el párrafo anterior con el que deducimos que la población percibe a las empresas, (como enemigos en una lucha de intereses).

También existe la posibilidad que la desconfianza o desacuerdo en el uso de sus datos, no provenga tanto de la figura que los utiliza, sino el fin con el que los utiliza, y si realmente confía en que los fines señalados y expuestos por los mismos, sean los únicos.

En cada una de las figuras planteadas, siempre predomina la desconfianza sobre la confianza en cuanto a recogida y manipulación de datos se refiere, y en una mayor medida en el caso de las empresas.

A raíz de estos mismos datos, también podríamos averiguar si esos porcentajes de aceptación y apoyo en el uso de los datos (tan parecidos en cuanto a número) se tratan de un mismo grupo poblacional. Un grupo de encuestados que está de acuerdo en la utilización general de los datos personales por parte de diversas figuras para diversos fines, entendiendo a este grupo de encuestados como **"Facilitadores o en acuerdo con el uso de los datos personales a fin de optimizar procesos".**

Aquellos que entienden este recurso como una mera herramienta de trabajo que debe ser empleada, tal y cómo fue expuesta en el capítulo 2, para ello, volvemos a

recurrir a la herramienta de realizar una tabla con las secuencias de respuesta de cada encuestado.

Gobierno	Investigadores	Empresas	
Si	Si	Si	26
Si	Si	No	11
Si	No	Si	4
Si	No	No	14
No	Si	Si	0
No	Si	No	15
No	No	Si	7
No	No	No	68

Tabla 4: Secuencias de confianza; Fuente: elaboración propia.

Para no complicar en exceso los resultados, hemos excluido a la población que ha contestado de una manera más indiferente, teniendo únicamente en cuenta a aquellos que responden con firme acuerdo o desacuerdo.

Tal y como podemos observar en la tabla, las secuencias de respuesta más comunes de entre las tenidas en cuenta, son las que muestran acuerdo o desacuerdo en cada una de las figuras, es decir confianza o desconfianza total en los procesos de recogida de datos para su posterior utilización. Siendo bastante superior la desconfianza, que la confianza, pero con este fenómeno ya contábamos con anterioridad a la tabla.

Confirmamos la existencia de un pequeño grupo poblacional de encuestados, que se posiciona a favor de la utilización de la recogida de datos como herramienta utilizable y disponible para su uso en los distintos fines buscados, independientemente de la figura que los manipule.

Por pequeño que parezca este grupo en comparación con el tamaño de la muestra, nos sirve para establecer la existencia de este fenómeno, la confianza en la

recogida de datos como herramienta útil, en contraposición de aquellos que perciben esta ciencia como una amenaza para su seguridad. Claro está, que este fenómeno coexiste con las preferencias, y diferencias en cuanto a la confianza depositada por los ciudadanos y usuarios en cada una de las figuras expuestas.

15 - Puntúa el nivel de interés que consideras que tienen las empresas en la consecución de los siguientes fines (siendo 0 un interés mínimo, y 5 máximo interés)

La siguiente, y última pregunta de este bloque, pide a los encuestados que evalúen de 0 a 5 el grado de interés que consideran que tienen las empresas en la consecución de unos fines sugeridos, (dichos fines, logrados a raíz de la extracción de datos personales)

Estas son las puntuaciones en cuanto a nivel de interés percibido:

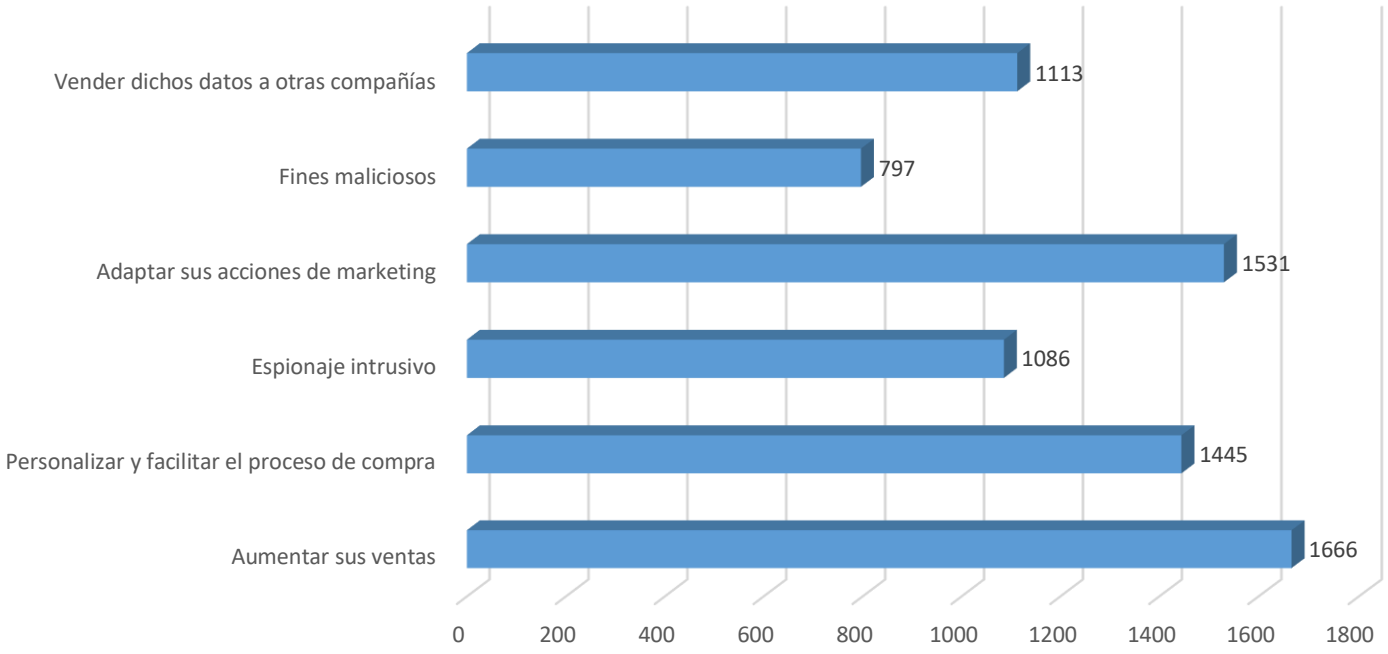

Ilustración 17: Percepción del interés empresarial. Fuente: elaboración propia.

Observamos unas puntuaciones bastante acordes la idea previa que teníamos sobre cómo se perciben las empresas por los propios consumidores.

A percepción de nuestros encuestados, el principal motivo de las empresas para llevar a cabo estrategias con recogida de datos de los consumidores es “aumentar sus ventas”, tal vez haya sido este fin el más destacado por lo genérico que se expone, y porque por todos es sabido, que aumentar los ingresos es el fin primordial de las

empresas, cierto es que para ello deberán llevar a cabo medidas más concretas y centralizadas.

"Fines maliciosos" se percibe como el de menor de los intereses empresariales, detrás del "espionaje intrusivo", la comparativa podría dar la impresión de que existe confianza por parte de los consumidores en cuanto a la benevolencia de los fines empresariales, no obstante, esto no es más que una visión relativa al resto de fines.

"Fines maliciosos" y "espionaje intrusivo" obtienen unas puntuaciones medias de interés percibido de 2,85 y 2,09, sobre 5 puntos. Estos datos en combinación con los anteriores, nos reafirman en lo ya establecido, la mala imagen de las empresas por parte de una amplia parte de la población, que tal vez las conciba como un enemigo en una constante lucha de intereses.

Y es que las puntuaciones de estos dos últimos fines, son las menores de entre los 6 intereses expuestos, pero desde un punto de vista personal considero que los otros 4 fines son de pensamiento inmediato, y algo obvio, sin embargo, pese a la existencia de empresas con fines poco éticos, alguna mala decisión, o prevalencia de los intereses propios frente a los de los consumidores, no están todas las empresas cortadas con un mismo patrón. Y que a pesar de ser este un miedo humano, ante el desconocimiento de los procesos con los que tratan nuestra información personal, se trata de un pensamiento más pasional que lógico, ya que en muchos casos llevar a cabo este tipo de acciones por parte de las empresas no tendría mucho sentido, o posibilidad de ello.

No debemos cometer el error de concebir a cualquier tercero que utilice nuestros datos, como terceros en general y asociar a estos, las acciones también existentes de los ciberdelicuentes. Estos ataques son algo ante lo que debemos estar preparados, de hecho, son frecuentes las alertas en este sentido, los rumores, historias… y muchas veces no entendemos exactamente qué ni cómo lo hicieron, y de ese desconocimiento y miedo fundado alrededor de la metodología, podría nacer ese rechazo por parte de aquellos que no apoyan, incluso se oponen a la recogida de datos independientemente del fin, o figura al mando de estos.

4.2.4. BLOQUE 4: PERCEPCIONES GENERALES

Con este bloque se pone fin a la encuesta realizada, cuenta únicamente con una pregunta y su objetivo es clarificar y posicionar a los participantes en un pensamiento o idea generalizada que se les es expuesta, pidiéndoles que se ubiquen en la opción que más se ajuste a su pensamiento.

1. ¿Qué frase se acomoda más a tus actuaciones, en cuanto a la protección de tus datos personales?

- Siempre me aseguro de que los datos que ofrezco no me resulten invasivos.
- A veces preferiría no tener que aceptar las políticas de cookies para seguir con mi navegación, pero no hay otra opción.
- Entiendo que se recojan datos, para mejorar el servicio.
- No me preocupa.
- Nunca doy mis datos personales.
- Nunca me ha preocupado, pero ahora sí.

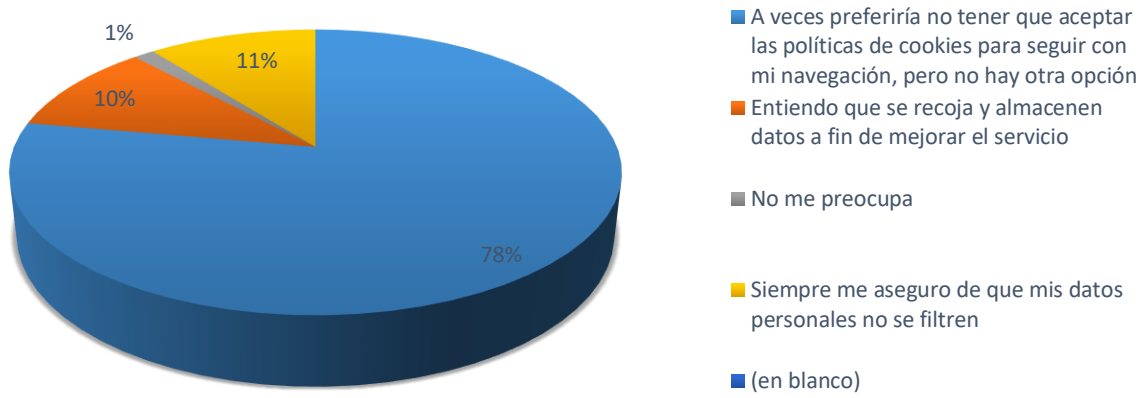

Ilustración 18: Opinión respecto a la protección de datos personales. Fuente: elaboración propia.

Este gráfico nos muestra un mínimo 1% de la muestra a la que no le preocupa la recogida y trato de sus datos por agentes externos o terceros.

Un reducido 10% se muestra favorable y comprensivo hacia el uso de estas herramientas por parte de las empresas y otras figuras manipuladoras de datos, ya que entienden que sus motivos son de buena fe y promueven la mejora en cuanto a calidad de servicio, y optimización de procesos.

Identificamos a este 10% con el grupo anteriormente destacado, los que se muestran en acuerdo con esta tecnología, y conocedores de la actual presencia e importancia en la sociedad, del uso de Big Data.

Observamos también que este grupo, es un 96% población juvenil (de 18 a 30 años) y aunque es cierto que este grupo es el mayoritario en el caso de particular de nuestra muestra, podemos extraer de los resultados, la siguiente conclusión:

La población más favorecedora, o en acuerdo con el uso del Big Data como "herramienta útil" en distintos ámbitos de aplicación, es la población joven.

Personalmente pienso que si la población estuviera más informada de la cantidad de procesos en los que el Big Data está implicado, y se hiciera consciente de lo que su omisión, podría suponer para la comodidad de sus vidas jamás rechazarían su uso. Lo que también es cierto es que esta potente arma, como ya comentamos anteriormente, puede ser origen de muchos daños si es utilizada con el fin de hacer daño, y es eso de lo que muchas veces nos han advertido, y pienso que es por esto, por lo que muchas veces es rechazada la tecnología como concepto, ante un miedo de ese posible y real riesgo, en combinación con el desconocimiento.

5. CONCLUSIONES.

Para establecer de una manera ordenada las conclusiones a las que la realización de este trabajo me ha llevado, debería empezar por el marco teórico de este, del cual obtengo múltiples conocimientos a nivel técnico acerca del funcionamiento de la ciencia (expuestos en el capítulo 2) los procesos necesarios, las posibles situaciones a las que el buen o mal uso de la misma nos puede llevar… Incluso he obtenido cierto aprendizaje de la actualidad (datos reales COVID), pero toda esta información, obra de los expertos en la materia y profesores ya ha sido expuesta anteriormente.

Hablando de conclusiones propias o pensamientos inducidos por la investigación en la materia, en primer lugar me gustaría destacar el potencial del Big Data. Como estudiante de Grado en Comercio, habiendo cursado varias asignaturas en las que nos enseñan la importancia de saber ver las oportunidades de negocio como tal y aprovechar al máximo las ventajas competitivas disponibles, honestamente creo que el Big Data, es una gran oportunidad.

Bien es cierto, que esta conclusión ha sido algo reiterativo en la mayor parte de los artículos expuestos, por lo que no debería considerarla como propia, pero creo que no es suficiente con escuchar lo importante que es algo para realmente saberlo. Y es en este momento, de una manera consciente, basándome en ejemplos como los expuestos en el capítulo 2.3 “Casos reales de éxito” cuando puedo decir que creo conocer el alcance de esta ciencia y veo en ella un inmenso valor económico, estratégico, educacional, lo que me hace considerarlo un campo interesante de estudio en el que avanzar profesionalmente.

Otra conclusión extraída de la realización del trabajo, aunque también mencionada anteriormente, es la toma de conciencia acerca de la cantidad de procesos implicados, relacionados y guiados mediante la aplicación del Big Data, procesos cotidianos y habituales sobre los que no nos detenemos a analizar en condiciones normales.

En definitiva, los conocimientos adquiridos a partir del marco teórico con sus respectivas conclusiones de firma ajena, han repercutido en mi manera de pensar, adquiriendo asombro y consciencia acerca de la realidad de esta ciencia, y del mundo en general.

Ahora haciendo referencia a los resultados obtenidos en la encuesta, extraemos las siguientes conclusiones a cerca de la actitud generalizada respecto al Big Data

- Cuando se trata de una población general no especializada en el tema, existe confusión cuando se emplean términos del ámbito informático más allá de los comunes. Big Data se trata de un término poco extendido.

- Teniendo en cuenta este desconocimiento, y también refiriéndonos la población general, existe una tendencia muy extendida de desconfianza hacia la tecnología y los procesos empleados por parte de las empresas y terceros.

Pienso que parte de este desconocimiento, general y personal, puede encontrar su justificación en la dificultad para la comprensión exacta de los procesos completos, añadiendo a esto, el estado embrionario de la ciencia de la que hablamos, no por poca antigüedad, sino por el crecimiento que tiene por delante.

Me atrevería a afirmar, que no es demasiado preocupante la extracción de datos por parte de terceros, ni que debamos tener una actitud esquiva hacia esto por temor a nuestra seguridad personal o la de nuestra intimidad, ya que por sí solos, nuestros datos carecen de valor. Pero sí creo que es conveniente y sobre todo muy interesante conocer los procesos empleados relacionados con esta ciencia.

Como próximos pasos en este campo, me gustaría conocer más acerca de los temas relacionados, y en los cuales no he entrado de una manera exhaustiva, como la inteligencia artificial o el machine learning que en combinación con el Big Data, ya están siendo capaces de realizar grandes avances en la ciencia, el comercio y en definitiva la sociedad.

Estamos ante un mundo nuevo, en que los datos junto con el tiempo son dos grandes capitales.

6. REFERENCIAS BIBLIOGRÁFICAS

- **Alcalá (2019)**;"Las cinco V que sirven para explicar el Big Data", Universidad de Alcalá, Madrid (España). Recuperado de https://www.master-bigdata.com/big-data-5-v/ en 27/03/2020.

- **Álvaro.B, (2017)**; "Big Data, la administración de los datos masivos en la gestión estratégica de la empresa". Recuperado de https://cutt.ly/DyOwl2X en 01/04/2020.

- **Calero.J (2020)**; "Covid-19", INNOVASPAIN (2020). Recuperado de https://www.innovaspain.com/covid-19-datos/ en 28/03/2020.

- **Camino a las TIC (2017)**; Autor desconocido. Recuperado de https://cutt.ly/QyOwmJu en 28/03/2020.

- **Del Pozo. P (2017)**; "3 ejemplo que ilustran el poder del Big Data". (BILIB) ; Recuperado de https://cutt.ly/1yOwIhr en 19/05/2020.

- **Derecho digital (2018)**; "Todo lo que necesitas saber sobre datos personales". Recuperado de https://cutt.ly/3yOwPoK en 17/04/2020.

- **Gartner (2001)**; "Big Data definition", Gartner Blog Network. Recuperado de https://cutt.ly/eyOwDeI en 17/05/2020.

- **GDMA (2018)**; "Privacidad de los datos del mundo". Recuperado de https://www.icemd.com/digital-knowledge/estudios/privacidad-de-datos-en-el-mundo/ en 06/04/2020.

- **IBM (2019)**;"La importancia del Big Data", VIEWNEXT S.A. IBM ESPAÑA GLOBAL SERVICES S.A. Recuperado de https://www.viewnext.com/importancia-del-big-data/ en 27/03/2020.

- **IEP (2017)**; "Ventajas y desventajas del Big Data", Instituto Europeo de Postgrado, Madrid (España). Recuperado de https://www.iep.edu.es/big-data-ventajas-desventajas/ en 27/03/2020.

- **Juan. C (2016);** "Éxito en Big Data Marketing". Recuperado de https://cutt.ly/lyOwBk1 en 12/04/2020.

- **Kallinikos, J. (2017)**; "La realidad recuperada: una investigación sobre la era de los datos". Madrid BBVA. Recuperado de https://cutt.ly/NyOwZZS en 17/05/2020.

- **Landa. J (2018)**; "Proceso KDD". Recuperado de http://fcojlanda.me/es/ciencia-de-los-datos/kdd-y-mineria-de-datos-espanol/ en 30/03/2020.

- **Marca (2020)**; Periódico Marca "Mapa coronavirus en vivo". Recuperado de https://cutt.ly/yyUMaQI en 12/05/2020.

- **Marketing directo (2018)**; "El 57% de los usuarios está dispuesto a compartir sus datos". Recuperado de https://cutt.ly/cyOw1GC en 06/04/2020.

- **Marketing directo (2018)**; "Transparencia". Recuperado de https://cutt.ly/tyOw90u en 07/04/2020.

- **Marta. B (2018)**;"El Data mining", MEDIACLOUD. Recuperado de https://blog.mdcloud.es/que-es-data-mining-algoritmos-y-ejemplos/ en 30/03/2020.

- **Nick (2019)**; "The Data veracity" (Tech entice). Recuperado de https://www.techentice.com/the-data-veracity-big-data/ en 13/05/2020.

- **Network World (2017)**; "Forbes y Teradata revelan los beneficios del Big Data". Recuperado de https://cutt.ly/tySCizJ en 27/04/2020.

- **Pandiello. O y Arcas.M (2020)**; "Luchar contra la pandemia a costa de nuestra privacidad". Recuperado de https://cutt.ly/CyOw7jd en 05/05/2020.

- **Rayo. A (2016)**;"Tipos de datos en Big Data"; (Netmind Computer Training). Recuperado de https://www.bit.es/knowledge-center/tipos-de-datos-en-big-data/ en 01/04/2020.

- **Redacción de Digital guide (2018**);"Esquema de los datos personales". Recuperado de https://www.ionos.es/digitalguide/paginas-web/derecho-digital/datos-personales/ en 13/05/20.

- **Twogood.C (2015)**; "Los beneficios de Big Data para las multinacionales". (TechWeek). Recuperado de https://cutt.ly/RyOetzd en 31/03/2020.

- **WebMining (2017)**; "el proceso de extracción del conocimiento". Recuperado de https://cutt.ly/6yOepnS en 30/03/2020.

7. ANEXO: Ley Orgánica 3/2018

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

TEXTO ORIGINAL

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

ÍNDICE

Disposición adicional séptima. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

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

Disposición adicional novena. Tratamiento de datos personales en relación con la notificación de incidentes de seguridad.

Disposición adicional décima. Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.

Disposición adicional undécima. Privacidad en las comunicaciones electrónicas.

Disposición adicional duodécima. Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.

Disposición adicional decimotercera. Transferencias internacionales de datos tributarios.

Disposición adicional decimocuarta. Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.

Disposición adicional decimoquinta. Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.

Disposición adicional decimosexta. Prácticas agresivas en materia de protección de datos.

Disposición adicional decimoséptima. Tratamientos de datos de salud.

Disposición adicional decimoctava. Criterios de seguridad.

Disposición adicional decimonovena. Derechos de los menores ante Internet.

Disposición adicional vigésima. Especialidades del régimen jurídico de la Agencia Española de Protección de Datos.

Disposición adicional vigésima primera. Educación digital.

Disposición adicional vigésima segunda. Acceso a los archivos públicos y eclesiásticos.

Disposición transitoria primera. Estatuto de la Agencia Española de Protección de Datos.

Disposición transitoria segunda. Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre.

Disposición transitoria tercera. Régimen transitorio de los procedimientos.

Disposición transitoria cuarta. Tratamientos sometidos a la Directiva (UE) 2016/680.

Disposición transitoria quinta. Contratos de encargado del tratamiento.

Disposición transitoria sexta. Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley.

Disposición derogatoria única. Derogación normativa.

Disposición final primera. Naturaleza de la presente ley.

Disposición final segunda. Título competencial.

Disposición final tercera. Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

Disposición final cuarta. Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Disposición final quinta. Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.

Disposición final sexta. Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Disposición final séptima. Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Disposición final octava. Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

Disposición final novena. Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Disposición final décima. Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

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

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

Disposición final decimotercera. Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.

Disposición final decimocuarta. Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.

Disposición final decimoquinta. Desarrollo normativo.

Disposición final decimosexta. Entrada en vigor.

PREÁMBULO

I

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «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». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que 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.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del

tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

II

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Así, se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente. Y en este marco la Comisión lanzó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que constituye el germen de la posterior reforma del marco de la Unión Europea. Al propio tiempo, el Tribunal de Justicia de la Unión ha venido adoptando a lo largo de los últimos años una jurisprudencia que resulta fundamental en su interpretación.

El último hito en esta evolución tuvo lugar con la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus 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), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

III

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Asimismo, se atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios. Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea.

La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

IV

Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales.

Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

V

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble. Así, en primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. En segundo lugar, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas, en referencia, entre otras, a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria cuarta la aplicación a estos tratamientos de la Ley Orgánica 15/1999, de 13 de diciembre, hasta que se apruebe la citada normativa.

En el Título II, «Principios de protección de datos», se establece que a efectos del Reglamento (UE) 2016/679 no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público. También se recoge expresamente el deber de confidencialidad, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una 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, Este es el caso, por ejemplo, de las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos

del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y 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 reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea.

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

El Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos», incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera

a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos». El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en

consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras.

De conformidad con la disposición adicional decimocuarta, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. La pervivencia de esta normativa supone la continuidad de las excepciones y limitaciones que en ella se contienen hasta que se produzca su reforma o abrogación, si bien referida a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y en esta ley orgánica. Así, por ejemplo, en virtud de la referida disposición adicional, las Administraciones tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Las disposiciones transitorias están dedicadas, entre otras cuestiones, al estatuto de la Agencia Española de Protección de Datos, el régimen transitorio de los procedimientos o los tratamientos sometidos a la Directiva (UE) 2016/680. Se recoge una disposición derogatoria y, a continuación, figuran las disposiciones finales sobre los preceptos con carácter de ley ordinaria, el título competencial y la entrada en vigor.

Asimismo, se introducen las modificaciones necesarias de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Finalmente, y en relación con la garantía de los derechos digitales, también se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, así como en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

TÍTULO I

Disposiciones generales

Artículo 1. Objeto de la ley.

La presente ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

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 3. Datos de las personas fallecidas.

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

TÍTULO II

Principios de protección de datos

Artículo 4. Exactitud de los datos.

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

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 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 este 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 7. Consentimiento de los menores de edad.

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

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 9. Categorías especiales de datos.

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Artículo 10. Tratamiento de datos de naturaleza penal.

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO III

Derechos de las personas

CAPÍTULO I

Transparencia e información

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.

CAPÍTULO II

Ejercicio de los derechos

Artículo 12. Disposiciones generales sobre ejercicio de los derechos.

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 13. Derecho de acceso.

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14. Derecho de rectificación.

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 15. Derecho de supresión.

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16. Derecho a la limitación del tratamiento.

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17. Derecho a la portabilidad.

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 18. Derecho de oposición.

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

TÍTULO IV

Disposiciones aplicables a tratamientos concretos

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.

Artículo 20. Sistemas de información crediticia.

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

Artículo 21. Tratamientos relacionados con la realización de determinadas operaciones mercantiles.

1. Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

2. En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica.

Artículo 22. Tratamientos con fines de videovigilancia.

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 23. Sistemas de exclusión publicitaria.

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas.

2. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias.

La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior. A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

3. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este deberá informarle de los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la autoridad de control competente.

4. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente.

No será necesario realizar la consulta a la que se refiere el párrafo anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en esta ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla.

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.

Artículo 25. Tratamiento de datos en el ámbito de la función estadística pública.

1. El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los

artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

Artículo 26. Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.

Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica con las especialidades que se derivan de lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, así como la legislación autonómica que resulte de aplicación.

Artículo 27. Tratamiento de datos relativos a infracciones y sanciones administrativas.

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO V

Responsable y encargado del tratamiento

CAPÍTULO I

Disposiciones generales. Medidas de responsabilidad activa

Artículo 28. Obligaciones generales del responsable y encargado del tratamiento.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la

evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Artículo 29. Supuestos de corresponsabilidad en el tratamiento.

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea.

1. En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679.

Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

2. Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

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.

Artículo 32. Bloqueo de los datos.

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO II

Encargado del tratamiento

Artículo 33. Encargado del tratamiento.

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

CAPÍTULO III

Delegado de protección de datos

Artículo 34. Designación de un delegado de protección de datos.

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35. Cualificación del delegado de protección de datos.

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36. Posición del delegado de protección de datos.

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni

sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37. Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

CAPÍTULO IV

Códigos de conducta y certificación

Artículo 38. Códigos de conducta.

1. Los códigos de conducta regulados por la sección 5.ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

Dichos códigos podrán dotarse de mecanismos de resolución extrajudicial de conflictos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679.

Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 37 de esta ley orgánica. Además, sin menoscabo de las competencias atribuidas por el Reglamento (UE) 2016/679 a las autoridades de protección de datos, podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta.

En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

La autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

3. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento.

El registro será accesible a través de medios electrónicos.

6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Artículo 39. Acreditación de instituciones de certificación.

Sin perjuicio de las funciones y poderes de acreditación de la autoridad de control competente en virtud de los artículos 57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del citado reglamento podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

TÍTULO VI

Transferencias internacionales de datos

Artículo 40. Régimen de las transferencias internacionales de datos.

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el

Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41. Supuestos de adopción por la Agencia Española de Protección de Datos.

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42. Supuestos sometidos a autorización previa de las autoridades de protección de datos.

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Artículo 43. Supuestos sometidos a información previa a la autoridad de protección de datos competente.

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier

transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679.

TÍTULO VII

Autoridades de protección de datos

CAPÍTULO I

La Agencia Española de Protección de Datos

Sección 1.ª Disposiciones generales

Artículo 44. Disposiciones generales.

1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

3. La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Artículo 45. Régimen jurídico.

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679, la presente ley orgánica y sus disposiciones de desarrollo.

Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto.

Artículo 46. Régimen económico presupuestario y de personal.

1. La Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en el Estatuto de la Agencia Española de Protección de Datos.

Corresponde a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos, siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno.

3. La Agencia Española de Protección de Datos contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del Reglamento (UE) 2016/679.

4. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

5. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral.

6. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

7. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Artículo 47. Funciones y potestades de la Agencia Española de Protección de Datos.

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 48. La Presidencia de la Agencia Española de Protección de Datos.

1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos regulados por el Título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto.

5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

a) Incumplimiento grave de sus obligaciones,

b) incapacidad sobrevenida para el ejercicio de su función,

c) incompatibilidad, o

d) condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.

6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Artículo 49. Consejo Consultivo de la Agencia Española de Protección de Datos.

1. La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un Diputado, propuesto por el Congreso de los Diputados.

b) Un Senador, propuesto por el Senado.

c) Un representante designado por el Consejo General del Poder Judicial.

d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia.

e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.

f) Un experto propuesto por la Federación Española de Municipios y Provincias.

g) Un experto propuesto por el Consejo de Consumidores y Usuarios.

h) Dos expertos propuestos por las Organizaciones Empresariales.

i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.

j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia.

k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas.

l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia.

m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados.

n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.

ñ) Dos expertos propuestos por las organizaciones sindicales más representativas.

2. A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico.

3. Los miembros del Consejo Consultivo serán nombrados por orden del Ministro de Justicia, publicada en el Boletín Oficial del Estado.

4. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

5. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

6. En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Artículo 50. Publicidad.

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.

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 54. Planes de auditoría.

1. La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

2. A resultas de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.

En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.

3. Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría.

Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos

Artículo 55. Potestades de regulación. Circulares de la Agencia Española de Protección de Datos.

1. La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán «Circulares de la Agencia Española de Protección de Datos».

2. Su elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

3. Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Artículo 56. Acción exterior.

1. Corresponde a la Agencia Española de Protección de Datos la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos.

Asimismo a las comunidades autónomas, a través de las autoridades autonómicas de protección de datos, les compete ejercitar las funciones como sujetos de la acción exterior en el marco de sus competencias de conformidad con lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, así como celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, sobre materias de su competencia en el marco de la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

2. La Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

La Agencia Española de Protección de Datos informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.

3. Sin perjuicio de lo dispuesto en el apartado 1, la Agencia Española de Protección de Datos:

a) Participará en reuniones y foros internacionales de ámbito distinto al de la Unión Europea establecidos de común acuerdo por las autoridades de control independientes en materia de protección de datos.

b) Participará, como autoridad española, en las organizaciones internacionales competentes en materia de protección de datos, en los comités o grupos de trabajo, de estudio y de colaboración de organizaciones internacionales que traten materias que afecten al derecho fundamental a la protección de datos personales y en otros foros o grupos de trabajo internacionales, en el marco de la acción exterior del Estado.

c) Colaborará con autoridades, instituciones, organismos y Administraciones de otros Estados a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de

datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.

CAPÍTULO II

Autoridades autonómicas de protección de datos

Sección 1.ª Disposiciones generales

Artículo 57. Autoridades autonómicas de protección de datos.

1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica.

Artículo 58. Cooperación institucional.

La Presidencia de la Agencia Española de Protección de Datos convocará, por iniciativa propia o cuando lo solicite otra autoridad, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 y de la presente ley orgánica. En todo caso, se celebrarán reuniones semestrales de cooperación.

La Presidencia de la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán solicitar y deberán intercambiarse mutuamente la información necesaria para el cumplimiento de sus funciones y, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos. Asimismo, podrán constituir grupos de trabajo para tratar asuntos específicos de interés común.

Artículo 59. Tratamientos contrarios al Reglamento (UE) 2016/679.

Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento (UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679

Artículo 60. Coordinación en caso de emisión de dictamen por el Comité Europeo de Protección de Datos.

Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando éstas, como autoridades competentes, deban someter su proyecto de decisión al citado comité o le soliciten el examen de un asunto en virtud de lo establecido en los apartados 1 y 2 del artículo 64 del Reglamento (UE) 2016/679.

En estos casos, la Agencia Española de Protección de Datos será asistida por un representante de la Autoridad autonómica en su intervención ante el Comité.

Artículo 61. Intervención en caso de tratamientos transfronterizos.

1. Las autoridades autonómicas de protección de datos ostentarán la condición de autoridad de control principal o interesada en el procedimiento establecido por el artículo 60 del Reglamento (UE) 2016/679 cuando se refiera a un tratamiento previsto en el artículo 57 de esta ley orgánica que se llevara a cabo por un responsable o encargado del tratamiento de los previstos en el artículo 56 del Reglamento (UE) 2016/679, salvo que desarrollase significativamente tratamientos de la misma naturaleza en el resto del territorio español.

2. Corresponderá en estos casos a las autoridades autonómicas intervenir en los procedimientos establecidos en el artículo 60 del Reglamento (UE) 2016/679, informando a la Agencia Española de Protección de Datos sobre su desarrollo en los supuestos en que deba aplicarse el mecanismo de coherencia.

Artículo 62. Coordinación en caso de resolución de conflictos por el Comité Europeo de Protección de Datos.

1. Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando estas, como autoridades principales, deban solicitar del citado Comité la emisión de una decisión vinculante según lo previsto en el artículo 65 del Reglamento (UE) 2016/679.

2. Las autoridades autonómicas de protección de datos que tengan la condición de autoridad interesada no principal en un procedimiento de los previstos en el artículo 65 del Reglamento (UE) 2016/679 informarán a la Agencia Española de Protección de Datos cuando el asunto sea remitido al Comité Europeo de Protección de Datos, facilitándole la documentación e información necesarias para su tramitación.

La Agencia Española de Protección de Datos será asistida por un representante de la autoridad autonómica interesada en su intervención ante el mencionado comité.

TÍTULO VIII

Procedimientos en caso de posible vulneración de la normativa de protección de datos

Artículo 63. Régimen jurídico.

1. Las disposiciones de este Título serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica.

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las

disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

3. El Gobierno regulará por real decreto los procedimientos que tramite la Agencia Española de Protección de Datos al amparo de este Título, asegurando en todo caso los derechos de defensa y audiencia de los interesados.

Artículo 64. Forma de iniciación del procedimiento y duración.

1. Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.

En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de reclamación.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.

Cuando fuesen de aplicación las normas establecidas en el artículo 60 del Reglamento (UE) 2016/679, el procedimiento se iniciará mediante la adopción del proyecto de acuerdo de inicio de procedimiento sancionador, del que se dará conocimiento formal al interesado a los efectos previstos en el artículo 75 de esta ley orgánica.

Admitida a trámite la reclamación así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio, podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

3. El procedimiento podrá también tramitarse como consecuencia de la comunicación a la Agencia Española de Protección de Datos por parte de la autoridad de control de otro Estado miembro de la Unión Europea de la reclamación formulada ante la misma, cuando la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679. Será en este caso de aplicación lo dispuesto en el apartado 1 y en los párrafos primero, tercero, cuarto y quinto del apartado 2.

4. Los plazos de tramitación establecidos en este artículo así como los de admisión a trámite regulados por el artículo 65.5 y de duración de las actuaciones previas de investigación previstos en el artículo 67.2, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de los Estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

Artículo 65. Admisión a trámite de las reclamaciones.

1. Cuando se presentase ante la Agencia Española de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia Española de Protección de Datos, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74 de esta ley orgánica.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento o al organismo de supervisión establecido para la aplicación de los códigos de conducta a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica.

La Agencia Española de Protección de Datos podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un delegado de protección de datos ni estuviera adherido a mecanismos de resolución extrajudicial de conflictos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en este Título a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos.

Artículo 66. Determinación del alcance territorial.

1. Salvo en los supuestos a los que se refiere el artículo 64.3 de esta ley orgánica, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia Española de Protección de Datos considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia Española de Protección de Datos notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia Española de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679.

Artículo 67. Actuaciones previas de investigación.

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la Sección 2.ª del Capítulo I del Título VII de esta ley orgánica y no podrán tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa o como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.3 de esta ley orgánica.

Artículo 68. Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.

1. Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá a la Presidencia de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

2. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo.

Artículo 69. Medidas provisionales y de garantía de los derechos.

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

TÍTULO IX

Régimen sancionador

Artículo 70. Sujetos responsables.

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos.

b) Los encargados de los tratamientos.

c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.

d) Las entidades de certificación.

e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título.

Artículo 71. Infracciones.

Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.

Artículo 72. Infracciones consideradas muy graves.

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.

b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.

c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.

d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de esta ley orgánica.

g) El tratamiento de datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.

j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

2. Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

Artículo 73. Infracciones consideradas graves.

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

h) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

i) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

j) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

l) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

n) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

ñ) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

o) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

p) El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 28 de esta ley orgánica.

q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

u) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

x) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.

y) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.

z) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 39 de esta ley orgánica.

aa) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.

ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 74. Infracciones consideradas leves.

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73 c) de esta ley orgánica.

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3 de esta ley orgánica.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al

tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de este de las disposiciones del Reglamento (UE) 2016/679 o de esta ley orgánica, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y a la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.

o) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 75. Interrupción de la prescripción de la infracción.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas.

Artículo 76. Sanciones y medidas correctivas.

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.

4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.

Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación.

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.

Artículo 78. Prescripción de las sanciones.

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

TÍTULO X

Garantía de los derechos digitales

Artículo 79. Los derechos en la Era digital.

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80. Derecho a la neutralidad de Internet.

Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Artículo 81. Derecho de acceso universal a Internet.

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.

2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.

3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.

4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.

5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.

6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82. Derecho a la seguridad digital.

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Artículo 83. Derecho a la educación digital.

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Artículo 84. Protección de los menores en Internet.

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

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 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88. Derecho a la desconexión digital en el ámbito laboral.

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 89. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

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.

Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización 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.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91. Derechos digitales en la negociación colectiva.

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Artículo 92. Protección de datos de los menores en Internet.

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

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.

Artículo 96. Derecho al testamento digital.

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales

o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Artículo 97. Políticas de impulso de los derechos digitales.

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.

Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Disposición adicional segunda. Protección de datos y transparencia y acceso a la información pública.

La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición adicional tercera. Cómputo de plazos.

Los plazos establecidos en el Reglamento (UE) 2016/679 o en esta ley orgánica, con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se regirán por las siguientes reglas:

a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.

c) Si el plazo se fija en meses o años, concluirá el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes.

d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

Disposición adicional cuarta. Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.

Lo dispuesto en el Título VIII y en sus normas de desarrollo será de aplicación a los procedimientos que la Agencia Española de Protección de Datos hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

Disposición adicional quinta. Autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencia internacional de datos.

1. Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente.

Las decisiones de la Comisión Europea a las que puede resultar de aplicación este cauce son:

a) aquellas que declaren el nivel adecuado de protección de un tercer país u organización internacional, en virtud del artículo 45 del Reglamento (UE) 2016/679;

b) aquellas por las que se aprueben cláusulas tipo de protección de datos para la realización de transferencias internacionales de datos, o

c) aquellas que declaren la validez de los códigos de conducta a tal efecto.

2. La autorización a la que se refiere esta disposición solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del

Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

Disposición adicional sexta. Incorporación de deudas a sistemas de información crediticia.

No se incorporarán a los sistemas de información crediticia a los que se refiere el artículo 20.1 de esta ley orgánica deudas en que la cuantía del principal sea inferior a cincuenta euros.

El Gobierno, mediante real decreto, podrá actualizar esta cuantía.

Disposición adicional séptima. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

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.

Disposición adicional novena. Tratamiento de datos personales en relación con la notificación de incidentes de seguridad.

Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

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.

Disposición adicional undécima. Privacidad en las comunicaciones electrónicas.

Lo dispuesto en la presente ley orgánica se entenderá sin perjuicio de la aplicación de las normas de Derecho interno y de la Unión Europea reguladoras de la privacidad en el sector de las comunicaciones electrónicas, sin imponer obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación en ámbitos en los que estén sujetas a obligaciones específicas establecidas en dichas normas.

Disposición adicional duodécima. Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.

2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.

3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

Disposición adicional decimotercera. Transferencias internacionales de datos tributarios.

Las transferencias de datos tributarios entre el Reino de España y otros Estados o entidades internacionales o supranacionales, se regularán por los términos y con los límites establecidos en la normativa sobre asistencia mutua entre los Estados de la Unión Europea, o en el marco de los convenios para evitar la doble imposición o de otros convenios internacionales, así como por las normas sobre la asistencia mutua establecidas en el Capítulo VI del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional decimocuarta. Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.

Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.

Disposición adicional decimoquinta. Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión o inspección, la Comisión Nacional del Mercado de Valores 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 relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.

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.

Disposición adicional decimosexta. Prácticas agresivas en materia de protección de datos.

A los efectos previstos en el artículo 8 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, se consideran prácticas agresivas las siguientes:

a) Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

b) Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

c) Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

d) Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

e) Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

Disposición adicional decimoséptima. Tratamientos de datos de salud.

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Disposición adicional decimoctava. Criterios de seguridad.

La Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del Reglamento (UE) 2016/679 y en el Título V de esta ley orgánica.

Disposición adicional decimonovena. Derechos de los menores ante Internet.

En el plazo de un año desde la entrada en vigor de esta ley orgánica, el Gobierno remitirá al Congreso de los Diputados un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

Disposición adicional vigésima. Especialidades del régimen jurídico de la Agencia Española de Protección de Datos.

1. No será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 85 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Disposición adicional vigésima primera. Educación digital.

Las Administraciones educativas darán cumplimiento al mandato contenido en el párrafo segundo del apartado 1 del artículo 83 de esta ley orgánica en el plazo de un año a contar desde la entrada en vigor de la misma.

Disposición adicional vigésima segunda. Acceso a los archivos públicos y eclesiásticos.

Las autoridades públicas competentes facilitarán el acceso a los archivos públicos y eclesiásticos en relación con los datos que se soliciten con ocasión de investigaciones policiales o judiciales de personas desaparecidas, debiendo atender las solicitudes con prontitud y diligencia las instituciones o congregaciones religiosas a las que se realicen las peticiones de acceso.

Disposición transitoria primera. Estatuto de la Agencia Española de Protección de Datos.

1. El Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, continuará vigente en lo que no se oponga a lo establecido en el Título VIII de esta ley orgánica.

2. Lo dispuesto en los apartados 2, 3 y 5 del artículo 48 y en el artículo 49 de esta ley orgánica se aplicará una vez expire el mandato de quien ostente la condición de Director de la Agencia Española de Protección de Datos a la entrada en vigor de la misma.

Disposición transitoria segunda. Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica.

Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.

Disposición transitoria tercera. Régimen transitorio de los procedimientos.

1. Los procedimientos ya iniciados a la entrada en vigor de esta ley orgánica se regirán por la normativa anterior, salvo que esta ley orgánica contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Disposición transitoria cuarta. Tratamientos sometidos a la Directiva (UE) 2016/680.

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

Disposición transitoria quinta. Contratos de encargado del tratamiento.

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Disposición transitoria sexta. Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica.

Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:

a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.

b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

Disposición derogatoria única. Derogación normativa.

1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición final primera. Naturaleza de la presente ley.

La presente ley tiene el carácter de ley orgánica.

No obstante, tienen carácter de ley ordinaria:

– El Título IV,

– el Título VII, salvo los artículos 52 y 53, que tienen carácter orgánico,

– el Título VIII,

– el Título IX,

– los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X,

– las disposiciones adicionales, salvo la disposición adicional segunda y la disposición adicional decimoséptima, que tienen carácter orgánico,

– las disposiciones transitorias,

– y las disposiciones finales, salvo las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta, que tienen carácter orgánico.

Disposición final segunda. Título competencial.

1. Esta ley orgánica se dicta al amparo del artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

2. El Capítulo I del Título VII, el Título VIII, la disposición adicional cuarta y la disposición transitoria primera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.

3. Los artículos 87 a 90 se dictan al amparo de la competencia exclusiva que el artículo 149.1.7.ª y 18.ª de la Constitución reserva al Estado en materia de legislación laboral y bases del régimen estatutario de los funcionarios públicos respectivamente.

4. La disposición adicional quinta y las disposiciones finales séptima y sexta se dictan al amparo de la competencia que el artículo 149.1.6.ª de la Constitución atribuye al Estado en materia de legislación procesal.

5. La disposición adicional tercera se dicta al amparo del artículo 149.1.18.ª de la Constitución.

6. El artículo 96 se dicta al amparo del artículo 149.1.8.ª de la Constitución.

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.»

Disposición final cuarta. Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Se modifica la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, en los siguientes términos:

Uno. Se añade un apartado tercero al artículo 58, con la siguiente redacción:

«Artículo 58.

Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.»

Dos. Se añade una letra f) al artículo 66, con la siguiente redacción:

«Artículo 66.

f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añaden una letra k) al apartado 1 y un nuevo apartado 7 al artículo 74, con la siguiente redacción:

«Artículo 74.

1. […]

k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.

[…]

7. Corresponde a las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Cuatro. Se añade un nuevo apartado 7 al artículo 90:

«7. Corresponde a los Juzgados Centrales de lo Contencioso-administrativo autorizar, mediante auto, el requerimiento de información por parte de la Agencia Española de Protección de Datos y otras autoridades administrativas independientes de ámbito estatal a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Disposición final quinta. Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.

Se añade un nuevo Capítulo II al Título VI de la Ley 14/1986, de 25 de abril, General de Sanidad con el siguiente contenido:

«CAPÍTULO II

Tratamiento de datos de la investigación en salud

Artículo 105 bis.

El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.»

Disposición final sexta. Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

La Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, se modifica en los siguientes términos:

Uno. Se añade un nuevo apartado 7 al artículo 10:

«7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.»

Dos. Se añade un nuevo apartado 5 al artículo 11:

«5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añade un nuevo apartado 4 al artículo 12:

«4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.»

Cuatro. Se introduce un nuevo artículo 122 ter, con el siguiente tenor:

«Artículo 122 ter. Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.

1. El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.

2. Serán partes en el procedimiento, además de la autoridad de protección de datos, quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.

4. Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que dé traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.

5. Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.

6. Transcurrido el período de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal podrá decidir el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.

7. Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:

a) Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.

b) En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

8. El régimen de recursos será el previsto en esta ley.»

Disposición final séptima. Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Se modifica el artículo 15 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado como sigue:

«Artículo 15 bis. Intervención en procesos de defensa de la competencia y de protección de datos.

1. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas en el ámbito de sus competencias podrán intervenir en los procesos de defensa de la competencia y de protección de datos, sin tener la condición de parte, por propia iniciativa o a instancia del órgano judicial, mediante la aportación de información o presentación de observaciones escritas sobre cuestiones relativas a la aplicación de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea o los artículos 1 y 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Con la venia del correspondiente órgano judicial, podrán presentar también observaciones verbales. A estos efectos, podrán solicitar al órgano jurisdiccional competente que les remita o haga remitir todos los documentos necesarios para realizar una valoración del asunto de que se trate.

La aportación de información no alcanzará a los datos o documentos obtenidos en el ámbito de las circunstancias de aplicación de la exención o reducción del importe de las multas previstas en los artículos 65 y 66 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

2. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas aportarán la información o presentarán las observaciones previstas en el número anterior diez días antes de la celebración del acto del juicio a que se refiere el artículo 433 o dentro del plazo de oposición o impugnación del recurso interpuesto.

3. Lo dispuesto en los anteriores apartados en materia de procedimiento será asimismo de aplicación cuando la Comisión Europea, la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, en el ámbito de sus competencias, consideren precisa su intervención en un proceso que afecte a cuestiones relativas a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.»

Disposición final octava. Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

Se incluye una nueva letra l) en el apartado 2 del artículo 46 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, con el contenido siguiente:

«l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.»

Disposición final novena. Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Se modifica el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que pasa a tener el siguiente tenor:

«Artículo 16. [...]

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.»

Disposición final décima. Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

Se incluye una nueva letra l) en el apartado 1 del artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, que queda redactado como sigue:

«l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva.»

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.»

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

Se modifican los apartados 2 y 3 del artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que pasan a tener la siguiente redacción:

> **«Artículo 28. [...]**
>
> 2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.
>
> Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.
>
> Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.
>
> 3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.
>
> Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.»

Disposición final decimotercera. Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.

Se añade un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, con el siguiente contenido:

> **«Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.**
>
> Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimocuarta. Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

> «j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia 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.»

Disposición final decimoquinta. Desarrollo normativo.

Se habilita al Gobierno para desarrollar lo dispuesto en los artículos 3.2, 38.6, 45.2, 63.3, 96.3 y disposición adicional sexta, en los términos establecidos en ellos.

Disposición final decimosexta. Entrada en vigor.

La presente ley orgánica entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

Por tanto,

Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley orgánica.

Madrid, 5 de diciembre de 2018.

FELIPE R.

El Presidente del Gobierno,

PEDRO SÁNCHEZ PÉREZ-CASTEJÓN