La protección de datos personales en el contexto de la seguridad pública

Especial referencia a la Directiva 2016/680

PID_00268227

Ramón Miralles López

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Ramón Miralles López

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por la profesora: Mònica Vilasau Solana (2019)

Primera edición: septiembre 2019
© Ramón Miralles López
Todos los derechos reservados
© de esta edición, FUOC, 2019
Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea este eléctrico, químico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita de los titulares de los derechos.

Índice

Introducción

El uso de los datos personales está extendido en todos los ámbitos, tanto en el ámbito de las actividades que son propias de las empresas y organizaciones que actúan en el tráfico mercantil y de los negocios, como respecto a las administraciones públicas, en sus diferentes actividades de prestación de servicios a los ciudadanos y de protección de los intereses generales.

Muchos de los avances tecnológicos de las tres últimas décadas se han desarrollado en el contexto de las tecnologías de la información y la comunicación, en particular entorno a internet y sus servicios, cada vez más avanzados, y que tienen como centro de acción a las personas, por lo que los datos personales han adquirido una especial transcendencia.

La capacidad de tratar grandes volúmenes de información, en todo tipo de formatos, y la ubicación de servicios e información en la red, han propiciado el desarrollo de delincuencia organizada en la red, que ha conllevado la aparición de conceptos como los «ciberdelitos» o la «ciberdelincuencia».

Los Estados se han visto obligados a tomar coordinadamente medidas para luchar contra esas actividades delictivas; en el «Convenio sobre la Ciberdelincuencia» del Consejo de Europa, aprobado en Budapest el 23 de noviembre de 2001, los delitos informáticos se definían como: «actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, medios y datos».

Del mismo modo, resulta relevante la Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: «Hacia una política general de lucha contra la ciberdelincuencia [COM (2007) 267», en la que se define a la ciberdelincuencia como: «actividades delictivas realizadas con la ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas».

En ese escenario los datos personales son particularmente valiosos para la prevención, investigación o detección de esas conductas, de modo que los avances tecnológicos también pueden ponerse al servicio de esa lucha, si bien ese uso no está exento de riesgos para los derechos y libertades del conjunto de los ciudadanos, ya que pueden verse limitados, o incluso vulnerados.

Los datos personales gozan de una protección específica, puesto que un mal uso de los mismos puede llegar a causar importantes daños y perjuicios a las personas, de ahí el reconocimiento del derecho fundamental a la protección

de los datos personales, que como cualquier otro derecho no es ilimitado, de modo que puede ser preciso aplicar medidas que lo limiten en favor de otros bienes jurídicos o intereses generales prevalentes.

El presente módulo tiene por objeto analizar hasta qué punto existen tensiones entre el derecho a la protección de datos y la seguridad pública, y cómo el ordenamiento jurídico intenta equilibrar ambas necesidades y aportar soluciones y garantías a las inevitables limitaciones entre los derechos e intereses generales que se ven enfrentados.

1. El equilibrio entre privacidad y seguridad pública

Los derechos y libertades fundamentales en ningún modo son absolutos, ni ilimitados, ya que frecuentemente se encuentran enfrentados, o limitados con relación a otros derechos, siendo el contenido de las leyes y su aplicación lo que determina qué derecho debe prevalecer.

En un escenario de sociedades cada vez más complejas, se pueden dar también conflictos con otros bienes jurídicos protegidos por los ordenamientos jurídicos, y que no siempre tienen por qué venir recogidos de manera expresa en los textos constitucionales, o reconocidos inequívocamente como derechos y libertades fundamentales. Este podría ser el caso de la «seguridad pública».

La Declaración Universal de Derechos Humanos (DUDH), proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948, estableció por primera vez un conjunto de derechos humanos fundamentales que debían ser objeto de protección por parte de todos los Estados, por tanto, a nivel mundial.

La Declaración Universal de Derechos Humanos (DUDH)

Podéis consultarla en la página web de Naciones Unidas: https://www.un.org/es/universal-declaration-human-rights/

El artículo 3 de la DUDH dispone que: «Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona», es evidente que en este artículo se está reconociendo en términos muy generales un derecho individual, sin perjuicio de que las medidas que los Estados adopten para su protección puedan tener el carácter de colectivas o de interés general; por otro lado, el artículo 12 de la DUDH reconoce que «nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia».

Por supuesto, la Constitución española de 1978 (CE) recoge el ideal de «seguridad», primero en un sentido amplio, cuando en su preámbulo describe el objetivo general del texto constitucional, que no es otro que «establecer la justicia, la libertad y la seguridad y promover el bien», para después concretar en su artículo 17 que «toda persona tiene derecho a la libertad y a la seguridad»; no haciéndose una referencia expresa al concepto de seguridad pública, por tanto, se refiere a un concepto amplio de seguridad de las personas, de aplicación a cualquier ámbito en el que los individuos se desarrollen como personas.

En ese sentido resulta relevante tener en cuenta el artículo 10.1 de la CE, cuando dispone que «la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social», que conecta directamente con la DUDH cuando en su apartado 2 dispone que «las normas relativas a los derechos fundamentales y a las libertades que la

Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España».

A su vez, el artículo 18 de la CE garantiza «el derecho al honor, a la intimidad personal y familiar y a la propia imagen», así como «el secreto de las comunicaciones», a lo que se une el mandato constitucional de que la ley debe limitar «el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos», de lo que se deriva el reconocimiento como derecho fundamental de la protección de los datos personales y de la intimidad. Asimismo, la Carta de los Derechos Fundamentales de la Unión Europea (2000) reconoce el respeto de la vida privada y familiar (artículo 7) y la protección de datos de carácter personal (artículo 8), de modo que «toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan», que deberán ser tratados «de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley», quedando todo ello «sujeto al control de una autoridad independiente».

Carta de los Derechos Fundamentales de la Unión Europea

Podéis consultarla en EUR-Lex, el servicio de publicación en línea de textos legislativos de la Unión Europea: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:l33501&from=ES

Respecto de la seguridad pública, que es una manifestación concreta de ese concepto amplio de seguridad al que nos hemos referido, en el artículo 149.1 CE, cuando se identifican las materias sobre las que el Estado tienen competencia exclusiva, dispone que lo es la:

> «Seguridad pública, sin perjuicio de la posibilidad de creación de policías por las comunidades autónomas en la forma que se establezca en los respectivos estatutos en el marco de lo que disponga una ley orgánica».

Por tanto, la seguridad pública está relacionada con la actividad que llevan a cabo los cuerpos y fuerzas de seguridad, y precisamente esa actividad es la que a su vez puede ser origen de la restricción de derechos y libertades fundamentales, a veces muy graves.

Cabe mencionar que el artículo 104 CE se refiere a «seguridad ciudadana» cuando a su vez dispone que: «Las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana»; la doctrina y la jurisprudencia han interpretado que *seguridad pública* y *seguridad ciudadana* son sinónimos, aglutinando todas las actividades que tienen por objeto proteger a las personas y bienes.

Resulta muy ilustrativo lo que al respecto dice el «Alto Comisionado de Naciones Unidas para los Derechos Humanos» (ACNUDH), cuando se refiere a sus funciones de vigilancia con relación a la seguridad pública:

> «Estos temas [refiriéndose a la seguridad pública] tienen que ver con la forma en que los Estados y sus agentes e instituciones de seguridad (policías, militares, prisiones) responden al fenómeno de la violencia y la inseguridad pública. Se vigilan situaciones actuales de ejecuciones extrajudiciales, tortura, detenciones arbitrarias y otros abusos por agentes del Estado. Se incluyen situaciones de violencia de género, y aquellas orientadas a los pueblos indígenas, afrodescendientes o minorías».

Hay que distinguir, ya que así lo hace la CE, entre seguridad pública y seguridad nacional, entendiéndose esta última como todo aquello que «afecte a la seguridad y defensa del Estado», para la que se prevé que el Estado tenga la competencia exclusiva (art. 149.1 CE): «Defensa y Fuerzas Armadas».

La Ley 36/2015, de 28 de septiembre, de seguridad nacional, considera como tal las acciones que el Estado lleva a cabo para «proteger la libertad, los derechos y bienestar de los ciudadanos», desde la perspectiva de la garantía de la defensa del Estado (España), incluyendo la contribución a la seguridad internacional; por tanto, no se define como un derecho individual, sino en todo caso como un bien jurídico colectivo, dirigido en esencia a preservar la soberanía nacional.

Los objetivos clásicos de la seguridad nacional se han centrado en prevenir o rechazar amenazas militares de otros Estados (conflictos bélicos clásicos), ahora las amenazas a la seguridad nacional son más difusas, incluyendo el terrorismo, el narcotráfico, los riesgos medioambientales, los ataques en las redes (incluyendo aquellos que tienen su origen en la ciberdelincuencia), y fenómenos sociales de escala global como las migraciones masivas (resulta de interés lo recogido al respecto en la Estrategia de Seguridad Nacional, 2017). Aquí nos referimos exclusivamente a la seguridad pública o seguridad ciudadana, que con carácter general se regula en la Ley orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LSC), también conocida como «ley mordaza», que considera que la seguridad ciudadana es «un requisito indispensable para el pleno ejercicio de los derechos fundamentales y las libertades públicas» identificándola como un «bien jurídico de carácter colectivo», cuya protección debe ser asumida por el Estado, siendo objeto de la LSC (artículo 1) «la regulación de un conjunto plural y diversificado de actuaciones de distinta naturaleza orientadas a la tutela de la seguridad ciudadana, mediante la protección de personas y bienes y el mantenimiento de la tranquilidad de los ciudadanos».

Históricamente, las tensiones entre libertades y seguridad se han venido evidenciando, por ejemplo, en el periodo final de la república romana, un periodo políticamente convulso en Roma pero a la vez de consolidación de una base jurídica sólida (Derecho romano), se le atribuye a Marco Tulio Cicerón (entre 106 y 43 AEC) la frase: «Para ser libres hay que ser esclavos de la ley», poniendo de manifiesto los límites y restricciones que suponen las leyes, que a la vez son las que garantizan espacios de libertad.

Siglos después, encontramos una frase más conocida que también confronta libertad y seguridad: «Aquellos que cederían la libertad esencial para adquirir una pequeña seguridad temporal, no merecen ni libertad ni seguridad», de Benjamin Franklin (1706-1790, considerado uno de los padres fundadores de los Estados Unidos, que participó en la Declaración de Independencia y en la redacción de la Constitución de los Estados Unidos), un personaje público situado de pleno en un cambio de paradigma, fin de la era moderna e inicio de la era contemporánea, totalmente conectado con la revolución liberal, por tanto, situado en un escenario de lucha por el reconocimiento de derechos y libertades; una revolución política que incluye importantes cambios económicos, sobre la base de la revolución industrial y de componente social con la revolución burguesa.

Y como último ejemplo, y aunque sea de un personaje de ficción, tenemos la frase: «A veces tienes que pensar en algo más que en tu propia seguridad, a veces tienes que pensar en el bien mayor», pronunciada por Harry Potter, en el libro *Harry Potter y las reliquias de la muerte* (J. K. Rowling, 2008), por tanto, posterior a sucesos como los atentados a las Torres Gemelas (2001), y los ataques con bomba a trenes en Madrid (2004) y Londres (2005), que iniciaron un cambio en la percepción de la inseguridad, con relación a determinados ataques a la seguridad pública, con nuevos métodos, orígenes, magnitudes y motivaciones, y que desde la perspectiva de la limitación de derechos y libertades en occidente han constituido una causa-efecto indiscutible.

En un mundo globalizado e interconectado, ejercer esa función de seguridad pública por parte del Estado implica el uso intensivo y masivo de información (una buena parte de esa información serán datos personales) y por supuesto de tecnología, a fin de llevar a cabo las actividades de prevención e investigación de conductas delictivas o de comportamientos que implican amenazas de diversa índole para la seguridad.

El uso de tales tecnologías y, en particular, cuando estas se aplican al tratamiento masivo de datos personales de manera indiscriminada, hacen que ciertos principios y derechos fundamentales consolidados durante décadas entren en crisis, como por ejemplo, la presunción de inocencia, cuando de manera global se analiza la información que circula por la red a la «caza» de indicios de que tal vez se estén preparando acciones delictivas, sin que exista una investigación específica o centrada en individuos concretos.

Los cuerpos policiales y las autoridades judiciales han tenido que adaptar sus métodos de investigación y enjuiciamiento al nuevo escenario de comisión de delitos, adquiriendo nuevos conocimientos y organizándose específicamente para llevar a cabo la lucha contra ese tipo de actividades delictivas; por ejemplo, en España los diferentes cuerpos y fuerzas de seguridad, incluidas las policías autonómicas, disponen de unidades especialmente dedicadas a los ciberdelitos.

La persecución de los ciberdelitos en el ámbito judicial se completa con la denominada Fiscalía de Criminalidad Informática, que fue creada en el año 2011.

Por supuesto, esa actividad de investigación de actividades delictivas con componente tecnológica no se limita exclusivamente a la investigación de ciberdelitos, ya que otras conductas que llevan a la comisión de delitos no estrictamente vinculados al uso de las tecnologías también utilizan las tecnologías de la información y la comunicación como herramientas de apoyo o que facilitan estructuralmente la comisión de esos delitos comunes, por ejemplo, las actividades terroristas o el tráfico de estupefacientes.

En definitiva, la tensión entre privacidad y seguridad es evidente, y el marco jurídico es el que tiene que poner los límites y las garantías para que no se cometan abusos o la vulneración de los derechos fundamentales de manera «gratuita», o por una falta de reflexión sobre la necesidad y proporcionalidad de las medidas de control que pueden aplicarse sobre el conjunto de la población.

1.1. La proporcionalidad en la restricción de derechos fundamentales

Sin perjuicio de lo expresado anteriormente, la garantía de los derechos fundamentales también puede verse afectada cuando las personas pretenden hacer valer sus derechos frente a otras personas, sean físicas o jurídicas, reconociéndose la posibilidad de que se produzcan restricciones sobre la base de la necesaria tutela de otros bienes, o incluso de valores o principios.

La decisión sobre qué derecho prevalece cuando existe tal confrontación, precisa de una ponderación para la que los tribunales recurren al concepto de «proporcionalidad», que si bien con carácter general debe calificarse como un concepto jurídico indeterminado, en cuanto a que su significado solo puede ser genérico o abstracto en términos jurídicos, la Sentencia del Tribunal Constitucional 207/1996 estableció que atender a la proporcionalidad es «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas, las que supongan una injerencia en los derechos a la integridad física y a la intimidad».

Para ponderar hasta qué punto es aceptable «una medida restrictiva de un derecho fundamental», esta deberá superar el denominado «juicio de proporcionalidad», que implica valorar:

1) «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad);

2) sí, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad);

3) y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Por ejemplo, la proporcionalidad ha sido especialmente tratada en el ámbito de la videovigilancia, por lo que nos puede resultar útil para comprender su alcance, tener en cuenta cómo se aborda esa proporcionalidad en las instrucciones de videovigilancia de las autoridades de control.

Así, en la instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, de la Autoridad Catalana de Protección de Datos, se hace referencia a los tres requisitos que deben ser valorados en el juicio de proporcionalidad al que ya hemos aludido:

> «(...) una medida intrusiva como la que estamos analizando solo se puede considerar constitucionalmente legítima si resulta proporcionada a través de un triple análisis de la necesidad de la medida, su idoneidad y su carácter proporcional en sentido estricto. Es decir, cuando no se pueda alcanzar la misma finalidad mediante medidas menos intrusivas o que comporten menos riesgos para las personas».

Concretamente, en el art. 7.2 de la instrucción se describe el proceso de ponderación que debe llevarse a cabo respecto de los diferentes derechos y bienes jurídicos que pueden entrar en conflicto, por lo que obliga a analizar respecto de un sistema de videovigilancia:

a) La necesidad de utilizar ese sistema de vigilancia.

b) La idoneidad de la instalación de sistemas de videovigilancia para alcanzar la finalidad perseguida.

c) El riesgo que puede suponer para los derechos de las personas, teniendo en cuenta las características del sistema de videovigilancia, las circunstancias de la captación y las personas afectadas.

d) La ausencia de medidas de vigilancia alternativas que comporten un riesgo menor, en relación con posibles intromisiones en los derechos fundamentales.

e) Se hace referencia, en la mencionada instrucción, también al principio de intervención mínima, que debe ser aplicado al seleccionar las tecnologías utilizadas.

En términos similares se recoge en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocá-

maras, si bien añade otro elemento que nos puede resultar de utilidad al referirse al «juicio de proporcionalidad en sentido estricto», es decir, si la medida adoptada es ponderada o equilibrada, en razón de que puedan derivarse de esta más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (la videovigilancia se considera vinculada a un interés público).

De tal modo que las imágenes solo podrán ser tratadas cuando sean «adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras», admitiéndose la instalación de esos sistemas exclusivamente cuando «la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal».

La seguridad en todo caso es un instrumento al servicio de la garantía del ejercicio de derechos y libertades, no debería ser un fin en sí misma, y para ello, en los estados de derecho se aplican diversos instrumentos, que en esencia serían: el ordenamiento jurídico, el Poder Judicial y los Cuerpos y Fuerzas de Seguridad del Estado.

1.2. La vigilancia global

Las actividades de seguridad pública implican cada vez más una vigilancia global y coordinada entre los Estados. De ello tenemos diversos ejemplos, como el tratado de seguridad entre el Reino Unido y los Estados Unidos (en inglés: *United Kingdom-United States Security Agreement*, conocido como UKUSA).

UKUSA

Se trata de una alianza de naciones de habla inglesa formada en 1946, con el propósito de recolectar información de inteligencia. Está formada por: Estados Unidos (mediante la Agencia de Seguridad Nacional), Reino Unido (mediante el Cuartel General de Comunicaciones del Gobierno), Canadá, (mediante el Communications Security Establishment), Australia (mediante el Defence Signals Directorate) y Nueva Zelanda (mediante el Government Communications Security Bureau).

UKUSA controla el sistema de monitorización ECHELON (creado en 1971) que, a partir del asunto Snowden y sus revelaciones en el 2013, fue acusado de interferir en las comunicaciones de otros gobiernos, mediante el programa de vigilancia electrónica PRISM, operado por la NSA.

Son diversas las herramientas utilizadas en esa vigilancia global que pone en riesgo derechos y libertades individuales. Tan solo a título de ejemplo se pueden mencionar las más «famosas» utilizadas por los Estados Unidos:

- **ECHELON (NSA-1971):**
  - Comunicaciones por radio y satélite
  - Llamadas de teléfonos y fax
  - Correos electrónicos

- **Carnivore (FBI-1997):**
  - Correos
  - Comunicaciones electrónicas

- **PRISM (NSA-2007):**
  - Recoge y almacena comunicaciones electrónicas de proveedores de internet

Pero también en Europa se llevan a cabo ese tipo de actividades de vigilancia global:

- **ENFOPOL (1995-UE):**
  - Interceptación de comunicaciones telefónicas
  - Internet, satélites y otras formas de comunicación (1998)

- **SITEL (2001-ES):**
  - Interceptación de comunicaciones telefónicas (sistema español)

Ese tipo de herramientas, que implican una vigilancia masiva, en muchos casos de tipo preventivo, puede no tener en cuenta la distinción entre la vigilancia a ciudadanos que no suponen un riesgo, de los que sí que pueden suponerlo, pero es evidente que, por ejemplo, los procesos de radicalización llevados a cabo a través de redes sociales son una realidad, y que de alguna manera debe abordarse ese tipo de actividad desde la perspectiva policial.

De este modo, se han venido manifestando reservas, no solo sobre las herramientas utilizadas, incluso respecto de algunas de las normas que les dan cobertura legal. Por ejemplo, en la «Conferencia Internacional de Conservación de Datos», que se celebró en Madrid en 2009, el fiscal Pedro Martínez afirmó que «La directiva nos convierte a todos los ciudadanos en sospechosos, no diferencia entre personas honestas y delincuentes; por consiguiente, su objetivo no es controlar al delincuente, sino al ciudadano. Es pues una norma de control social como han denunciado numerosas asociaciones de derechos civiles y nosotros aprovechamos para reiterarlo», en referencia a la Directiva 2006/24/EC del Parlamento Europeo y del Consejo de 15 de marzo del 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas.

Directiva 2006/24/EC

Podéis consultarla en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2006-80647.

Esa Directiva fue anulada por una sentencia del Tribunal de Justicia de la Unión Europea (TJUE), de 8 de abril de 2014, lo que se une a la preocupación en Europa por las posibilidades de vigilancia excesiva que prevé la Resolución Enfopol (1999).

Sentencia del Tribunal de Justicia de 8 de abril de 2014

Podéis consultarla en: http://curia.europa.eu/juris/document/ document.jsf?docid=150642&doclang=ES

La ley 25/2007 que transpuso en España la Directiva anulada sigue vigente, puesto que la sentencia del TJUE no deroga las leyes de los Estados miembros de transposición de la Directiva, pero es evidente que su aplicación en procedimientos judiciales podría provocar que se planteen incidentes de nulidad, en tanto se utilicen preceptos que pudieran verse afectados por el contenido de la sentencia, aunque fuera de manera indirecta.

Ley 25/2007

Podéis consultarla en: https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

Por tanto, se plantea el dilema de si estamos ante un escenario de medidas de protección, o más bien de vigilancia indiscriminada de la población, con la consiguiente vulneración de derechos y libertades, y los riesgos que ello implica para las personas.

El activismo de personajes públicos como Julian Assange o Edward Snowden no dejan de ser «dos caras de la misma moneda». En 2007, WIKILEAKS puso en crisis precisamente la acumulación de información de vigilancia, poniendo en evidencia el riesgo de filtraciones, mientras que en 2013, Snowden filtró precisamente la vigilancia global que se estaba llevando a cabo. Hacía ya tiempo que tal vigilancia era más que sospechada, pero no fue hasta que se hicieron públicas sus revelaciones, cuando la opinión pública no empezó a tomar conciencia de ese espionaje global que afectaba a todos. El hecho de que la NSA y el FBI estaban recabando datos utilizando PRISM, obtenidos de los servidores de empresas como Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube y Apple, es lo que hizo saltar todas las alarmas.

En este sentido, resulta de interés mencionar que ahora existen los denominados informes de transparencia, en los que ese tipo de compañías explican públicamente qué datos les han sido solicitados por las autoridades gubernamentales. A título de ejemplo, se puede acceder a los informes de Google, Facebook y Microsoft en los siguientes enlaces:

- **Informe de transparencia de Google:**
  https://transparencyreport.google.com/?hl=es

- **Facebook Transparency Report:**
  https://transparency.facebook.com/

- **Privacidad en Microsoft:**
  https://www.microsoft.com/es/trust-center/privacy

Se trata de informes muy completos, si bien de tipo principalmente estadístico, esto es, no filtran qué peticiones concretas se han hecho, solo el tipo de peticiones y el resultado, ya que a veces los proveedores de servicios se niegan a proporcionar la información solicitada. En cualquier caso, son suficientemente indicativos de la actividad de las autoridades en lo que respecta a solicitudes de información relacionada con la actividad de los usuarios en ese tipo de servicios.

En definitiva, es evidente que las actividades que se desarrollan en el marco de la seguridad ciudadana afectan a los derechos y libertades de los ciudadanos, y es con relación a esas consecuencias restrictivas donde las leyes, y su aplicación, deben aportar el necesario equilibrio.

2. Directiva 2016/680: tratamiento de datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales

En mayo del 2016 la Unión Europea aprobó un paquete de medidas sobre el derecho fundamental a la protección de datos, que incluía el Reglamento general de protección de datos (RGPD) y a la Directiva (UE) 2016/680, 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 derogaba la Decisión Marco 2008/977/JAI del Consejo (la Directiva aprobada se conoce como «Directiva sobre la policía»); ambos instrumentos regulatorios fueron aprobados al mismo tiempo.

Aunque no la vamos a tratar en este módulo, resulta conveniente mencionar que, junto con el RGPD y la Directiva 680, también se aprobó otra Directiva, la 2016/681, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

El RGPD se aplica desde el 25 de mayo del 2018, mientras que la Directiva 680, que entró en vigor el 5 de mayo del 2016, está pendiente de transposición al ordenamiento jurídico español. Estuvo prevista esa transposición para el 2018 en el «Plan anual normativo del Gobierno», mediante una «Ley orgánica sobre el tratamiento de datos personales para fines policiales y judiciales penales». Como consecuencia de la situación política derivada de la moción de censura al Gobierno en junio de 2018, y posteriormente el avance de convocatoria de elecciones generales (28 abril 2019), ese proyecto de ley orgánica quedó a la espera de que se volviera a plantear su tramitación.

Cabe mencionar que el artículo 63 de la Directiva 680 regula su transposición, para lo que dispone que «los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo del 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva»; el mencionado plazo ha sido superado sin que exista la mencionada norma de transposición.

Transposición en España

La Comisión Europea en julio de 2018 incoó un procedimiento de infracción a España por la falta de transposición de la Directiva 680, y ante la falta de respuesta por parte del estado español, en julio de 2019 solicitó al Tribunal de Justicia de la Unión Europea que España fuera sancionada por esa falta de transposición.

La Directiva 680 tiene por objeto proteger el derecho fundamental a la protección de los datos personales cuando estos sean utilizados por las autoridades policiales y judiciales; en concreto la Directiva garantiza la protección adecuada de los datos personales de víctimas, testigos y sospechosos de delitos, y además regula cuestiones tendentes a facilitar a las autoridades competentes la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo.

En la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD) se hace referencia a la Directiva 680, en particular en uno de sus artículos, y en la disposición transitoria cuarta.

En el artículo 22 de la LOPDGDD, dedicado a los tratamientos con fines de videovigilancia, se dispone que el tratamiento de los datos personales, cuyo origen sea imágenes y sonidos captados mediante sistemas de videovigilancia o cámaras usadas por «las Fuerzas y Cuerpos de Seguridad del Estado 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 regulará mediante la ley que tenga por objeto la transposición de la Directiva (UE) 2016/680, en tanto la finalidad de ese tratamiento sea la «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», en otros casos el tratamiento atenderá a lo dispuesto en legislación específica y, de manera supletoria, a lo previsto en el RGPD y en la LOPDGDD.

Por su parte, la Disposición transitoria cuarta dispone que los tratamientos sujetos a la Directiva 680, se continuarán regulando por la Ley orgánica 15/1999 (LOPD), en particular por su artículo 22, y disposiciones de desarrollo, hasta que no entre en vigor la norma de transposición de la Directiva 680.

2.1. Antecedentes: la Decisión Marco 2008/977/JAI del Consejo de la Unión Europea

La Decisión Marco 2008/977/JAI ha sido derogada por la Directiva 680, como fuente del Derecho en la Unión Europea. Las decisiones marco forman parte del denominado «derecho derivado», frente a la otra posible fuente que es el «derecho primario».

El **derecho primario** es el contenido en los tratados, que tienen por objeto establecer el marco jurídico de la Unión Europea (principalmente: el Tratado de la Unión Europea, el Tratado de funcionamiento de la Unión Europea y el Tratado constitutivo de la Comunidad Europea de la energía atómica), mientras que el **derecho derivado** está formado por instrumentos jurídicos que se derivan de esos Tratados. Por supuesto, hay otras fuentes del Derecho de

la Unión Europea, como «los principios generales del Derecho de la Unión Europea, la jurisprudencia del Tribunal de Justicia de la Unión Europea y el Derecho internacional».

El **derecho derivado** está formado por los denominados actos unilaterales y los acuerdos internacionales. En cuanto a los actos unilaterales, están regulados en el artículo 288 del Tratado de funcionamiento de la UE y, principalmente, pueden ser: reglamentos, directivas, decisiones, recomendaciones y dictámenes. Entre esos actos se incluyen también algunos muy concretos, basados en tratados anteriores, como por ejemplo, aquellos relacionados con la materia penal para la que se continúan aplicando las «decisiones marco», que se adoptaron antes de la entrada en vigor del Tratado de Lisboa. Puesto que la cooperación judicial y policial en materia penal, antes del Tratado de Lisboa, tenía un estatuto especial, entre esas decisiones marco se encontraba la Decisión Marco 2008/977/JAI.

Por tanto, una Decisión Marco es un tipo de acto legislativo de la Unión Europea, que se utilizaba con relación a las competencias de la Unión Europea en materia de cooperación policial y judicial penal. Las decisiones marco se crearon mediante el Tratado de Ámsterdam, y fueron suprimidas a partir del Tratado de Lisboa, ya que, a partir de la entrada en vigor de este, la Unión Europea ya podía regular la materia de justicia penal mediante directivas y reglamentos.

Las decisiones marco tenían como objetivo aproximar las disposiciones legales y reglamentarias de los Estados miembros, y obligaban a los Estados miembros en cuanto al resultado que debía obtenerse, dejando a las autoridades nacionales la forma y los medios para alcanzarlo.

Por lo que respecta al objetivo de la Decisión Marco 2008/977/JAI, no era otro que «garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas, y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal», eso sí, teniendo en cuenta que esa garantía de protección de los derechos y libertades no debía ir en menoscabo de la garantía de un alto nivel de seguridad pública.

La Decisión Marco era de aplicación tanto a tratamientos automatizados como no automatizados, y se disponía que no podía afectar a «los intereses esenciales de seguridad del Estado ni a las actividades específicas de inteligencia en el sector de la seguridad del Estado».

En cuanto a los tratamientos de datos personales a los cuales se aplicaba, eran todos aquellos relacionados con «la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales los datos personales», en tanto esos datos fueran transmitidos o pues-

tos a disposición entre los Estados miembros, ya fuera sobre la base de sistemas de información creados en virtud de los Tratados o como resultado de la cooperación con las autoridades competentes de los Estados miembros.

El contenido de la Decisión Marco se estructura sobre la base de la identificación de unos principios, unos derechos y unas obligaciones, que se alinean en cuanto a su concreción con la tradición de la protección de datos europea.

Como principios se identificaban los de licitud, proporcionalidad y finalidad, de manera que las autoridades competentes solo pueden tratar los datos personales para unas finalidades determinadas, explícitas y legítimas, teniendo en cuenta sus funciones, sin que puedan tratarlos para otros fines.

Aparte de reconocer la posibilidad del ejercicio de los típicos derechos por parte de los interesados respecto de los datos objeto de tratamiento, como el derecho de acceso, o los de rectificación, supresión o bloqueo, también los interesados debían ser informados de las características de los tratamientos llevados a cabo, e incluso se contemplaba la posibilidad de ejercer el derecho a reparación, en el caso de que, en determinadas circunstancias, se ocasionaran daños y perjuicios.

Entre otras cuestiones, la Decisión Marco establecía la necesidad de fijar plazos de supresión y comprobación de los datos, y hacía referencia al tratamiento de categorías especiales de datos, de modo que solo se permitía el tratamiento de datos personales que pudieran revelar «el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, de datos relativos a la salud o a la vida sexual» cuando fuera estrictamente necesario y, en todo caso, estableciendo garantías adecuadas mediante el derecho de cada Estado miembro.

También se hacía mención expresa a las decisiones automatizadas que pudieran producir «efectos jurídicos adversos en el interesado o le afectaran de manera significativa», en tanto se pudieran basar únicamente en un tratamiento automatizado de datos, permitiéndose tal decisión solo cuando una ley lo autorizara, y siempre estableciendo medidas de garantía de los intereses legítimos de las personas afectadas por los tratamientos.

Además se establecían específicamente medidas de control de calidad de los datos transmitidos o disponibles, y otras de carácter general en cuanto a la transferencia de datos a terceros Estados y organismos internacionales, así como con relación a la seguridad en el tratamiento de los datos personales, o en la selección de encargados de tratamiento, incluyendo algunas medidas preventivas como la consulta previa a las autoridades de control competentes, en el caso de creación de nuevos tratamientos de datos personales.

Finalmente, hay que destacar que existía la previsión de aplicar sanciones, y que las autoridades de protección de datos podían actuar para controlar el cumplimiento respecto de los tratamientos objeto de la Decisión Marco.

De lo descrito se deduce que se trataba de una Decisión Marco muy alineada con la normativa general de protección de datos, tal y como veremos que también sucede con la Directiva 680 que deroga esta Decisión Marco.

2.2. Fundamentos y principios de la Directiva

El punto de partida de la Directiva 680 es que la protección de las personas físicas en relación con el tratamiento de los datos de carácter personal es un derecho fundamental, en tanto viene reconocido en el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea. La finalidad de los datos a los que aplica la Directiva no desvirtúa en ningún caso la consideración de que son datos personales que deben ser protegidos.

Asimismo, la protección que proporciona la Directiva en lo que se refiere al tratamiento de los datos personales aplica a todas las personas físicas con independencia de su nacionalidad o lugar de residencia.

La Directiva se plantea como un instrumento que contribuye a «la consecución de un espacio de libertad, seguridad y justicia», y se alude en los considerandos de la Directiva al hecho de que los desarrollos tecnológicos y la globalización están generando nuevos retos y riesgos en lo que respecta al tratamiento de datos personales, lo que incluye también el uso de tecnologías que permiten que ese tratamiento se realice a «una escala sin precedentes», para actividades relacionadas con «la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales» (considerando número 3).

Los principales objetivos de la Directiva se centran, en primer lugar, en facilitar la libre circulación de datos personales para fines de prevención, investigación, detección o enjuiciamiento, entre las diferentes autoridades competentes en materia penal de los Estados miembros, y en segundo lugar, la protección y la prevención frente a las amenazas para la seguridad pública en la Unión Europea, junto con la necesidad de transferir esos datos personales a terceros países y organizaciones internacionales para luchar más eficazmente contra las conductas que ponen en riesgo la seguridad pública, siempre garantizando «un alto nivel de protección de los datos personales».

Para garantizar la eficacia de la cooperación judicial en materia penal y de la cooperación policial, la protección de los datos personales debe ser equivalente en todos los Estados miembros, por lo que la Directiva refuerza los derechos de los interesados y las obligaciones de los responsables, para el tratamiento de los datos personales necesarios para los fines a los que aplica la Directiva.

A continuación se analizan las principales características de la Directiva 2016/680 y se ponen de relieve aquellos aspectos que son distintos respecto al RGPD. Sin embargo, al hacer este ejercicio comparativo debe tenerse en cuenta en todo caso que Directiva y Reglamento son dos instrumentos jurídicos distintos.

La Directiva requiere de una transposición en cada Estado miembro, por lo tanto, muchos aspectos quedan abiertos o bien tienen menos concreción que en el caso del Reglamento, que es de aplicación directa. En consecuencia, podría darse la circunstancia de que en la Ley de transposición el legislador optara por aproximarse a lo que prevé el RGPD o bien que se alejara de dicha regulación. Este ejercicio de comparación, que es útil para tener una visión general del tratamiento de la información personal, debe tomarse con ciertas cautelas, a la espera del resultado final mediante la legislación interna que haga la transposición de la Directiva.

En la Directiva se concreta qué autoridades son las competentes para los tratamientos a los que esta se aplica (artículo 3, punto 7), por un lado, será cualquier «autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública» (es decir, autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad), o bien «cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública».

A los efectos de lo mencionado en el párrafo anterior, en el segundo de los supuestos debe tenerse en cuenta que, si ese «órgano o entidad» trata los datos para otros fines distintos a los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, a ese tratamiento le será de aplicación el Reglamento 679/2016 (RGPD).

Las autoridades competentes serán «responsables del tratamiento», en tanto determinen los fines y medios del tratamiento, y si estos vienen determinados por el Derecho de la Unión o del Estado miembro, «el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho de la Unión o del Estado miembro».

Se prevé la existencia de encargados de tratamiento, es decir, que una «persona física o jurídica, autoridad pública, servicio u otro organismo» trate datos personales por cuenta de la autoridad competente (responsable del tratamiento), obviamente siempre sobre la base de un contrato o instrumento que vincule jurídicamente a encargado y responsable (artículo 22 de la Directiva), y en el

que se establezcan las condiciones en las que se efectuará el tratamiento de datos personales que deberá llevarse a cabo por el encargado del tratamiento, por cuenta del responsable.

La Directiva tiene presente que las actividades realizadas por las Fuerzas y Cuerpos de Seguridad del Estado están dirigidas principalmente a la prevención, investigación, detección o enjuiciamiento de infracciones penales.

Ahora bien, esas mismas autoridades también llevan a cabo actuaciones policiales en las que aún no hay constancia de que una situación o conducta sea constitutiva de infracción penal, o bien en su actividad policial aplican medidas coercitivas, por ejemplo, la intervención en el caso de manifestaciones, acontecimientos deportivos o disturbios, o en general, tienen encomendado el mantenimiento del orden público, de este modo, en esos casos en los que los fines no sean aquellos a los que aplica la Directiva (prevención, investigación, detección o enjuiciamiento), aunque se traten datos por esas mismas autoridades a las que aplica la Directiva, resultará de aplicación el RGPD.

En el artículo 10 del RGPD se regula brevemente el tratamiento de datos personales relativos a condenas e infracciones penales, que serían los tratamientos posteriores a los que se llevarían a cabo en el marco de la Directiva 680 (prevención, investigación, detección o enjuiciamiento); así, el RGPD dispone que ese tipo de datos solo pueden ser tratados bajo la supervisión de las autoridades públicas competentes, y que «solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas».

El artículo 10 de la LOPDGDD regula lo que denomina datos de naturaleza penal, añadiendo a lo ya previsto en el RGPD la referencia a que también podrán tratarse esos datos por abogados y procuradores cuando la finalidad sea «recoger la información facilitada por sus clientes para el ejercicio de sus funciones».

El artículo 4 describe los principios que deben ser tenidos en cuenta al llevar a cabo los tratamientos a los que aplica la Directiva, que son altamente coincidentes con los recogidos en el RGPD, si bien cabe destacar que hay algunos matices que hay que tener en cuenta; se reproducen a continuación tal cual los recoge la Directiva, comparándolos en su caso con lo dispuesto por el RGPD en cuanto a principios:

a) tratados de manera lícita y leal; en el RGPD además se recoge el principio de «transparencia», que por razones evidentes no puede constituir un principio que aplique a los tratamientos de datos objeto de la Directiva, o al menos no en toda su extensión;

b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;

c) adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados; en este caso, en el RGPD se usa la expresión «limitados en relación con los fines», lo que a priori se podrían considerar expresiones equivalentes;

d) exactos y, si fuera necesario, actualizados; deberán adoptarse todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados;

e) conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados;

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas.

En cuanto a la licitud de los tratamientos de datos personales, a diferencia del RGPD, existe una única base que legitime los tratamientos sujetos a la Directiva, ya que en su artículo 8 dispone que tales tratamientos solo serán lícitos en tanto sean necesarios para los «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», obviamente, siempre teniendo en cuenta que ese tratamiento debe ser llevado a cabo por una autoridad competente, y que deberá estar «basado en el Derecho de la Unión o del Estado miembro».

Respecto del desarrollo de los principios, también resulta de especial relevancia lo previsto en el artículo 7.2 de la Directiva en cuanto a la exactitud y actualización de los datos personales, para lo que dispone que las autoridades competentes deben adoptar medidas para garantizar que los datos personales que puedan ser «inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros».

Con relación a la conservación de los datos personales (artículo 4.1.e), la Directiva dispone que los Estados miembros fijarán unos plazos de supresión de los datos personales que resulten apropiados, o bien harán previsiones para revisar periódicamente hasta qué punto es necesario conservar los datos personales (artículo 5).

Una cuestión importante, que establece una diferencia con el RGPD, es que la Directiva dispone que, a la hora de tratar los datos, se distinga claramente entre los datos personales de las distintas categorías de interesados que puedan incluirse en los tratamientos (artículo 6).

A título orientativo, la Directiva establece una serie de categorías de interesados que pueden llegar a estar afectados por los tratamientos: personas sospechosas, personas condenadas, víctimas y terceras partes relacionadas con infracciones penales (por ejemplo: testigos, informantes o personas relacionadas con sospechosos y condenados).

Tal y como ya se ha mencionado, la Directiva está alineada con los aspectos esenciales del derecho a la protección de datos, por lo que también recoge el concepto de categoría especial de datos (artículo 10), para los que dispone la limitación del «tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física», siendo los mismos tipos de datos que se consideran especiales en el RGPD.

Respecto de las categorías especiales de datos, solo deberá permitirse su tratamiento cuando sea «estrictamente necesario», a diferencia del RGPD que prohíbe su tratamiento, y siempre deben tratarse sobre la base de garantías que resulten adecuadas para salvaguardar los derechos y libertades de los interesados, y en todo caso cumpliendo con el requisito de que:

a) lo autorice el Derecho de la Unión o del Estado miembro;

b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o

c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

Las condiciones que permiten el tratamiento de categorías especiales en el ámbito de aplicación de la Directiva son muy concretas, con menos supuestos que los previstos en el artículo 9 del RGPD, para compensar que su tratamiento no está prohibido.

Esto es, en el caso de la Directiva 2016/680, no existe propiamente una prohibición, sino exclusivamente la valoración de tratar los datos considerados como especiales solo cuando sea «estrictamente necesario», compensándose con el hecho de limitar los supuestos en que pueden ser tratados.

Se establece con carácter general la prohibición de la toma de decisiones basadas únicamente en un tratamiento automatizado (artículo 11 de la Directiva), en tanto tal decisión produzca efectos jurídicos negativos para el interesado o bien le afecte de manera significativa. Se puede excepcionar esa prohibición si lo autoriza el Derecho de la Unión o de los Estados miembros, en tanto se establezcan medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo como mínimo el derecho a que exista una intervención humana por parte del responsable del tratamiento.

En el RGPD no se establece una prohibición de carácter general con relación a la toma automatizada de decisiones, sino que se reconoce un derecho a que no se tomen tales decisiones de manera exclusivamente automatizada, a no ser que concurran las circunstancias del artículo 22.2 del RGPD; en la Directiva solo se plantea en términos de prohibición, la elaboración de perfiles que tenga como consecuencia una discriminación de las personas, sobre la base del tratamiento de categorías especiales de datos.

Finalmente, con carácter general, la Directiva pone énfasis en asegurar la calidad de los datos que se tratan (correctos y actualizados), así como en que se establezca, en la medida de lo posible, la distinción entre «datos personales basados en hechos» y «datos personales basados en apreciaciones personales» (artículo 7.1). Esa distinción es muy importante, ya que las finalidades de los tratamientos a los que aplica la Directiva se refieren a conductas penales, en las que deben evitarse valoraciones subjetivas, aunque puedan llegar a incluirse entre los datos tratados, de ahí que se disponga que unos y otros estén diferenciados.

2.3. Derechos de los interesados

El capítulo III (artículos 12 a 18), recoge los derechos que los interesados tienen reconocidos con relación al tratamiento de sus datos personales, y el ejercicio de tales derechos.

Una vez más, la Directiva se alinea con el RGPD, y recoge prácticamente todos los derechos previstos en la regulación general del derecho a la protección de datos, sin perjuicio de que se prevean algunas peculiaridades, como por ejemplo, que se puedan establecer limitaciones al derecho de acceso (artículo 15), las condiciones en las que se puede ejercer el derecho de supresión (artículo 16), o que en determinadas condiciones se puedan ejercer los derechos a través de las autoridad de control (artículo 17); además, no se reconoce el derecho a la portabilidad de los datos ni el derecho de oposición.

En síntesis, se reconocen los siguientes derechos:

- Obtener información sobre los tratamientos.

- Derecho a acceso.
- Derecho de rectificación o supresión de datos personales.
- Derecho de limitación del tratamiento.

En lo que respecta a la información de los tratamientos, esta deberá proporcionarse a título gratuito, y de manera «concisa, inteligible y de fácil acceso, con un lenguaje claro y sencillo», pudiendo facilitarse por cualquier medio que resulte adecuado.

El artículo 13 de la Directiva establece qué información como mínimo debe ponerse a disposición de los interesados:

- La identidad y los datos de contacto del responsable del tratamiento.
- Los datos de contacto del delegado de protección de datos.
- Las finalidades del tratamiento.
- El derecho a presentar una reclamación ante la autoridad de control, así como los datos de contacto de esta.
- La existencia los derechos que puede ejercer (acceso, rectificación o su supresión, o la limitación de tratamiento).

Además, se añade que, en casos concretos, se facilite la siguiente información adicional:

- La base jurídica del tratamiento.
- El plazo de conservación de los datos personales o los criterios utilizados para determinar ese plazo.
- Cuando se vayan a comunicar datos a terceros, las categorías de destinatarios, en particular si se trata de terceros países o de organizaciones internacionales.
- Y cuando sea necesario, más información, especialmente cuando los datos personales se hayan recogido sin conocimiento del interesado (en el ámbito policial esto puede suponer algunos inconvenientes vinculados a las prácticas de investigación y revelación de fuentes de información).

Hay algunas diferencias con la información que debe proporcionarse, derivadas de las finalidades de los tratamientos a los que aplica la Directiva, por ejemplo, no se refiere a la «información que deberá facilitarse cuando los datos

personales se obtengan del interesado» o cuando «no se hayan obtenido del interesado», sino «información que debe ponerse a disposición del interesado o que se le debe proporcionar».

No se incluye que deba informarse de posibles representantes, puesto que no aplica a las circunstancias de los tratamientos, ni sobre la base jurídica del tratamiento, que solo deberá ser informada cuando así lo disponga una ley, como tampoco aplica informar sobre interés legítimo o cuestiones relacionadas con el consentimiento, puesto que no pueden ser base de licitud de los tratamientos, etc. En definitiva, la información que debe proporcionarse viene limitada por las propias finalidades y características de los tratamientos a los que aplica la Directiva.

Como la puesta a disposición de ciertas informaciones y, en general, el ejercicio de los derechos reconocidos pueden afectar a la propia finalidad de los tratamientos, se prevén algunas limitaciones generales al ejercicio de esos derechos, y en particular con relación al derecho de acceso, de modo que se pueden plantear limitaciones de ese ejercicio para:

- Evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales.
- Evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.
- Proteger la seguridad pública.
- Proteger la seguridad nacional.
- Proteger los derechos y libertades de otras personas.

Adicionalmente se prevé la posibilidad de que los derechos de los interesados sean ejercidos a través de la autoridad de protección de datos competente.

2.4. Obligaciones de los responsables de tratamientos

En cuanto a las obligaciones respecto del tratamiento de datos personales, la Directiva sigue el enfoque del RGPD, en el sentido de que todas las decisiones relacionados con el tratamiento de los datos personales deberán tomarse teniendo en cuenta, con carácter general, las características del tratamiento y, en particular, los riesgos a los que puedan estar expuestas las personas cuyos datos son objeto de tratamiento (riesgo para sus derechos y libertades), en definitiva, no hay diferencias sustanciales entre el RGPD y la Directiva, en cuanto a las obligaciones previstas para la protección de los datos personales.

La Directiva dispone en su artículo 24.1, que los Estados miembros deberán establecer que los responsables del tratamiento: «teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, aplique las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento se lleva a cabo de conformidad con la presente Directiva».

De manera sintética, las obligaciones que deben asumir los responsables de tratamiento serían:

- Con carácter general: adoptar medidas técnicas y organizativas, sobre la base del riesgo, para garantizar y demostrar que el tratamiento se lleva a cabo según la Directiva.

- En la adopción de las medidas debe tener en cuenta aplicar los principios de protección de datos desde el diseño y por defecto.

- Seleccionar encargados de tratamiento que ofrezcan garantías de capacidad en la aplicación de las medidas técnicas y organizativas.

- Mantener un registro de actividades de tratamiento, disponible para la autoridad de control (se establece un contenido mínimo).

- Mantener un registro de operaciones de tratamiento (artículo 25), es decir, deberá conservarse un registro de las operaciones de tratamiento que hayan sido realizadas sobre los sistemas de tratamiento automatizados, al menos de las siguientes operaciones: «recogida, alteración, consulta, comunicación, incluidas las transferencias, combinación o supresión»; esos registros deberán permitir conocer los motivos de la operación, la fecha y la hora y, cuando sea posible, el nombre de quien consultó o comunicó datos personales, y la identidad de los destinatarios de dichos datos personales.

- La cooperación con la autoridad de control.

- Hacer evaluaciones de impacto de las operaciones previstas en la protección de los datos personales (siguiendo el modelo del RGPD).

- Aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

- Notificaciones y comunicaciones de violaciones de la seguridad.

- Designación del delegado de protección de datos; los Estados miembros podrán eximir esa designación «a los tribunales y demás autoridades ju-

diciales independientes cuando actúen en ejercicio de sus competencias judiciales».

- Aplicar un régimen de transferencias internacionales de datos, que es análogo al previsto en el RGPD en cuanto al sistema de garantías y situaciones que permiten transferir los datos personales a terceros países, si bien siempre debe tenerse en cuenta la finalidad de los tratamientos a los que aplica la Directiva (se regulan en los artículos 35 a 39 de la Directiva).

2.5. Seguridad de los datos personales

A diferencia de lo previsto en el RGPD, que en cuanto a la seguridad de los datos solo establece unos mínimos a tener en cuenta, sobre la base del resultado que deben dar tales medidas con relación a la protección de los datos personales y de las operaciones de tratamiento, en el caso de la Directiva se ofrece un mayor detalle de las medidas de seguridad técnicas y organizativas que deben adoptarse en el marco de los tratamientos de datos personales a los que aplica la Directiva.

Así, el artículo 29, dispone que, para los tratamientos automatizados, los Estados miembros deberán regular que tanto responsables como encargados de tratamientos, a partir de una evaluación de los riesgos (será por tanto un requisito previo para la fundamentación de las medidas de seguridad, como en el RGPD), deberán adoptar medidas destinadas a:

a) Denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento (control de acceso a los equipamientos);

b) Impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas (control de los soportes de datos);

c) Impedir que se introduzcan sin autorización datos personales conservados, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización (control del almacenamiento);

d) Impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de los usuarios);

e) Garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado solo puedan tener acceso a los datos personales para los que han sido autorizados (control del acceso a los datos);

f) Garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos (control de la transmisión);

g) Garantizar que pueda verificarse y constatarse *a posteriori* qué datos personales se han introducido en los sistemas de tratamiento automatizado y en qué momento y por qué persona han sido introducidos (control de la introducción);

h) Impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);

i) Garantizar que los sistemas instalados puedan restablecerse en caso de interrupción (restablecimiento);

j) Garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema (integridad).

Se ha reproducido lo dispuesto en el artículo 29.2 por ser lo suficientemente directo y claro en cuanto al tipo de medidas que deben adoptarse.

Con relación a las medidas de seguridad, en particular, en cuanto a que no proporcionen el resultado de protección esperado, y que un incidente pueda afectar a la seguridad de los datos personales, prevé la Directiva obligaciones de notificación y comunicación de potenciales brechas de seguridad, que se regulan del mismo modo que en el RGPD, con la única diferencia de que deberá notificarse también a las autoridades competentes a las que se hayan transmitido los datos o de las que se hayan recibido datos afectados por la brecha de seguridad.

El artículo 30 de la Directiva se dedica a la obligación de notificar a la autoridad de control que se ha producido una brecha en la seguridad de los datos personales, es decir, deberá ponerse en conocimiento de la autoridad de protección de datos aquellos sucesos que hayan afectado, con carácter general, a la confidencialidad, integridad y disponibilidad de los datos personales.

El responsable del tratamiento deberá hacer la notificación a la autoridad de control sin dilación indebida, y si es posible, en un plazo no superior a 72 horas, contado a partir del momento en que haya tenido conocimiento de tal circunstancia, salvo que sea improbable que la brecha de seguridad suponga un riesgo para los derechos y las libertades de las personas cuyos datos se han

visto afectados por el incidente de seguridad; en el caso de que sea el encargado de tratamiento quien detecte la brecha, deberá ponerlo en conocimiento del responsable a la mayor brevedad posible.

La notificación a la autoridad de control deberá incluir información sobre la brecha de seguridad, según los mínimos que se detallan en el artículo 30.3:

- Naturaleza de la brecha de seguridad.
- Categorías y número aproximado de interesados afectados.
- Las categorías y el número aproximado de registros de datos personales afectados.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto.
- La descripción de las posibles consecuencias de la brecha.
- La descripción de las medidas adoptadas o propuestas por el responsable del tratamiento ante el incidente ocurrido.

La información sobre la brecha de seguridad se podrá notificar de una sola vez, o a medida que se vaya disponiendo de información; cualquier dilación en la entrega de esa información deberá estar convenientemente justificada.

Las brechas de seguridad deberán quedar documentadas, en particular deberán registrarse los hechos relativos a la brecha de seguridad, sus efectos y las medidas correctivas adoptadas, quedando toda esa información a disposición de la autoridad de control.

La otra obligación relacionada con brechas de seguridad es la de la comunicación de estas a las personas cuyos datos se hayan visto afectados.

El artículo 31 de la Directiva prevé la comunicación de las brechas de la seguridad de los datos personales a los interesados, que deberá hacerse cuando sea probable que el incidente que ha afectado a sus datos personales pueda dar lugar a un alto riesgo para sus derechos y libertades.

El responsable del tratamiento deberá hacer esa comunicación sin dilación indebida, puesto que se entiende que existe un alto riesgo provocado por la afectación a la seguridad de los datos personales, por lo que conviene actuar cuanto antes para limitar al máximo la gravedad de lo ocurrido.

Como en el caso de las notificaciones, se prevé un contenido mínimo de la comunicación que debe hacerse a los interesados, que deberá describir «con un lenguaje claro y sencillo» la naturaleza de la violación de la seguridad de

los datos personales y contendrá prácticamente la misma información que la prevista para la notificación, con especial énfasis en las medidas que puede adoptar el propio interesado.

En determinadas circunstancias tal comunicación no será necesaria, concretamente si se cumple alguna de las siguientes condiciones:

a) Si el responsable del tratamiento adoptó medidas de protección técnicas y organizativas, que se hayan aplicado a los datos personales afectados por la brecha de seguridad, en particular, medidas que hagan «ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos», por ejemplo, que los datos personales estuvieran cifrados.

b) Si el responsable del tratamiento ha adoptado medidas, con posterioridad al incidente, que garanticen que no sea probable que concurra un alto riesgo para los derechos y libertades del interesado.

c) O que la comunicación a los interesados suponga un esfuerzo desproporcionado; se podrá optar por una comunicación pública o una medida equivalente, que permita informar a los interesados de manera efectiva, como si la comunicación se les hubiera enviado directamente.

2.6. Autoridades de control

La Directiva no introduce modificaciones relevantes en lo que respecta a las autoridades de control que deben supervisar el cumplimiento de las normas nacionales de transposición de la Directiva; el régimen jurídico que describe la Directiva para estas instituciones es el mismo que el previsto en el RGPD.

De manera sintética, las cuestiones que prevé la Directiva en relación con las autoridades de control son las siguientes:

- Al menos debe existir una autoridad de control en cada Estado miembro que supervise la aplicación de la Directiva; puede designarse más de una.

- Debe ser una autoridad de carácter independiente, estableciéndose el proceso de nombramiento de sus miembros, duración del nombramiento, etc.

- Puede ser la misma autoridad designada para supervisar el cumplimiento del RGPD.

- Los interesados le podrán presentar reclamaciones con relación al tratamiento de sus datos personales en el marco de la Directiva.

- Dispone de poderes de investigación y correctivos, como en el caso del RGPD, y se les asigna un conjunto de funciones que deben permitirles

supervisar la adecuación de los tratamientos a lo previsto en la Directiva (artículo 46, «Funciones»).

- El régimen sancionador que aplicará la autoridad de control será el previsto por cada Estado miembro (artículo 57[1]).

- Además, podrán estar facultadas para poner en conocimiento de las autoridades judiciales las infracciones.

- Se establecen mecanismos de cooperación y asistencia mutua entre autoridades de control, así como su participación en el Comité Europeo de Protección de Datos creado por el RGPD. A diferencia de lo que sucede con el RGPD, no se establecen mecanismos de coherencia.

(1)Recuérdese que, al tratarse de una Directiva, esta requiere de transposición. La Ley de transposición deberá regular el régimen sancionador. El legislador podría optar por establecer el mismo régimen que el de la LOPDGDD. En la medida en que cada Estado miembro debe transponer esta Directiva, y que los Estados miembros tienen más margen para regular, pueden existir diferentes regímenes sancionadores en la UE en relación con los tratamientos contemplados por la Directiva.

En el caso del Estado español, dado que existen diferentes autoridades de control –la Agencia Española de Protección de Datos, y las autonómicas–, es de suponer que asuman el control del cumplimiento de la Directiva tal y como lo venían haciendo hasta el momento en sus respectivos ámbitos competenciales; por ejemplo, en lo que respecta a los tratamientos de datos realizados por los cuerpos policiales de cada territorio, en tanto son administraciones públicas, en todo caso la ley de transposición deberá concretar esta cuestión.

2.7. Reclamaciones, responsabilidades y sanciones

El incumplimiento de lo previsto en la Directiva, por supuesto con relación a la norma de transposición, podrá ser objeto de reclamación ante la autoridad de control competente, reconociéndose tal derecho en el artículo 52 de la Directiva.

Obviamente, esa reclamación podrá presentarse sin perjuicio de recurrir a cualquier otro «recurso administrativo o acción judicial». Ese derecho puede ejercerse por el interesado si se considera que el tratamiento de sus datos personales está infringiendo las disposiciones adoptadas en virtud de la Directiva.

La autoridad de control ante la que se haya presentado la reclamación deberá proporcionar la asistencia que le pueda solicitar el interesado a raíz de su reclamación, que deberá estar informado del desarrollo del procedimiento y del resultado de su reclamación.

Si fuera el caso, el interesado que presentó la reclamación podrá recurrir a la tutela de los tribunales si no está de acuerdo con la decisión de la autoridad de control, o si su reclamación no es atendida; eso mismo aplica a los responsables y encargados de tratamiento sobre los cuales resuelva la autoridad de control el posible incumplimiento de sus obligaciones o, en general, sobre la declaración de infracciones cometidas respecto de las disposiciones adoptadas por los Estados miembros con relación a la Directiva.

Las acciones contra una autoridad de control deberán ejercitarse ante los órganos jurisdiccionales del Estado miembro en que esté establecida la autoridad de control.

Se prevé que los Estados miembros regulen que, si un interesado sufre daños y perjuicios materiales o inmateriales, que tengan su origen en el tratamiento ilícito de sus datos personales, o como consecuencia de actos que vulneren las disposiciones nacionales adoptadas en virtud de la Directiva, el interesado tendrá «derecho a recibir una indemnización del responsable o de cualquier autoridad competente», según lo previsto en cada Estado miembro, por los daños y perjuicios sufridos (artículo 56).

Por otro lado, los Estados miembros establecerán las normas aplicables en materia de sanciones derivadas de las infracciones de las normas de transposición de la Directiva, debiendo estas ser efectivas, proporcionadas y disuasorias, y garantizándose su cumplimiento.

3. Autoridades de control para el tratamiento de datos personales: ámbito policial y judicial

Las autoridades de protección de datos, por definición, son entidades muy especializadas puesto que centran su actividad en un derecho fundamental muy concreto que, además, tiene un alto componente tecnológico y de seguridad de la información, que supone la aplicación de criterios tanto jurídicos como tecnológicos, todo y que su base de actuación obviamente esté centrada en el cumplimiento normativo.

Otro aspecto, de carácter general, muy relevante con relación a las autoridades de control, es que deben actuar con independencia en el ejercicio de sus funciones, por lo que se configuran como autoridades públicas independientes y reconocidas como tales en cada ordenamiento jurídico nacional. En consecuencia, los miembros de cada autoridad de control no deben recibir ninguna orden, ni instrucción interna o externa, en el desarrollo de sus funciones.

Además, el RGPD ha supuesto un cambio de paradigma con relación a cómo debe cumplirse con lo dispuesto en la regulación, sobre la base de un enfoque a riesgos y una responsabilidad proactiva (*accountability*), lo que supone que el cumplimiento debe construirse teniendo en cuenta los riesgos derivados de los tratamientos de datos personales, en tanto podrían perjudicar a las personas, con lo que las autoridades de protección de datos también deben ser capaces de asumir ese nuevo enfoque en el desarrollo de sus competencias y funciones.

A la mencionada especialidad por la materia, debe añadirse en el caso de datos personales relacionados con la actividad policial y judicial, otra especialización que deben asumir las autoridades de control o, en su caso, áreas de control, que desempeñan sus funciones de manera exclusiva en el contexto de organizaciones dedicadas a esos ámbitos policiales y judiciales.

Tanto Europol como Eurojust prestan una especial atención hacia el respeto al derecho a la protección de datos y, en el caso del orden jurisdiccional español, es el Consejo General del Poder Judicial quien asume las funciones de autoridad de control en el ámbito de la administración de justicia.

Como veremos, cada supuesto tiene sus propias características, pero todos ellos confluyen en la idea de que el RGPD resulta de aplicación a esos ámbitos de actuación, sin perjuicio de la analizada Directiva 680, y que se tiene muy en cuenta la cooperación con las autoridades de protección de datos de carácter general.

3.1. La protección de datos en Europol: funciones y controles

Europol es la agencia de la Unión Europea en materia policial, que, aparte de trabajar en aras de un objetivo amplio como el de «contribuir a la consecución de una Europa más segura para beneficio de todos los ciudadanos de la UE», ejerce otras actividades centradas en objetivos de carácter operativo.

Europol tienen su sede principal en La Haya, y presta asistencia a los Estados miembros de la Unión, en particular, en la lucha contra la delincuencia internacional a gran escala y el terrorismo, lo que implica que también colabora con Estados que no pertenecen a la Unión Europea y, por supuesto, con organizaciones internacionales con intereses comunes en la persecución de ese tipo de delincuencia.

Las redes de delincuencia y de terrorismo, a nivel global, amenazan a la seguridad de la Unión Europea, y por tanto, a sus ciudadanos; según Europol, las más graves amenazas tienen que ver con el terrorismo, el tráfico de drogas, el blanqueo de dinero a escala internacional, el fraude organizado, la falsificación de dinero (euros) y la trata de seres humanos, sin dejar de lado conductas delictivas cada vez más relevantes como la ciberdelincuencia.

Las actividades que desarrolla Europol implican manejar grandes volúmenes de información, en tanto que resulta necesario para los servicios que presta, que se centran particularmente en:

- Servir de centro de apoyo a operaciones policiales.
- Actuar como eje para la información sobre actividades delictivas.
- Constituirse en un centro de conocimientos policiales especializados.

La plantilla está formada por más de 1.000 profesionales, con 220 funcionarios de enlace de Europol, y unos 100 analistas de actividades delictivas, prestando apoyo a más de 40.000 investigaciones internacionales cada año. Europol es un centro operativo que desarrolla su labor de manera ininterrumpida (fuente: Europol, mayo de 2019).

El análisis de las actividades delictivas es la base de los servicios de Europol, lo que implica el uso de herramientas avanzadas de análisis de información para apoyar las investigaciones que llevan a cabo los cuerpos policiales de los Estados miembros.

Así, Europol lleva a cabo evaluaciones periódicas que proporcionan análisis prospectivos exhaustivos de las actividades delictivas y del terrorismo en la Unión Europea, elaborándose informes, por ejemplo, sobre la evaluación de la

amenaza de la delincuencia grave y organizada en la Unión Europea (SOCTA) o sobre la situación y las tendencias del terrorismo en la Unión Europea (TE-SAT).

La actividad de Europol implica la recogida, análisis e intercambio con los cuerpos policiales de los Estados miembros, de grandes volúmenes de datos personales, por lo que tienen implantadas, y aplican, rigurosas normas en materia de protección y seguridad de los datos.

Uno de los retos que precisamente se plantea Europol como organización es «equilibrar las necesidades operativas de Europol y el derecho de las personas a la protección de datos», ya que proporciona una innovadora plataforma que interconecta a más de 500 agencias, que permite no solo acceder a información, sino también recopilarla para su posterior análisis.

Por supuesto, el tratamiento de datos personales es una de las principales actividades de análisis de información, lo que obliga a la organización a aplicar, en palabras de la propia Europol: «los más altos estándares de protección de datos y seguridad de datos».

La función de protección de datos (por sus siglas en inglés DPF) en Europol se encuentra ubicada en una posición del organigrama que le permite garantizar la legalidad de las operaciones de tratamiento de datos personales, según la normativa europea de protección de datos; así, a las actividades desempeñadas por su delegado de protección de datos (responsable de la DPF) se añade el control ejercido por el supervisor europeo de protección de datos.

Supervisor europeo de protección de datos (SEPD)

Para más información sobre el SEPD podéis visitar la página: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_es

Como ya se ha expresado, la función de protección de datos está totalmente integrada en el organigrama de Europol, siendo el punto de contacto inicial para todas las cuestiones relacionadas con la protección de datos. La unidad de protección de datos está dirigida por el delegado de protección de datos, que es designado por el Consejo de Administración de Europol.

La unidad de protección de datos actúa con total independencia funcional, colaborando estrechamente con el conjunto de miembros que forman parte de Europol, asesorando y orientando respecto de las mejores prácticas en el tratamiento de datos personales y en el cumplimiento de la regulación; en particular, interviene en el tratamiento e intercambio de datos entre Europol y los Estados miembros de la Unión Europea, garantizando que se efectúan aplicando las normas de protección de datos.

Para desarrollar su función, la unidad de protección de datos tiene acceso a todos los datos que trata Europol, así como acceso a todas las dependencias y oficinas. Como actividad principal debe garantizar el cumplimiento del «Reglamento Europol», que refuerza desde el 1 de mayo de 2017 el régimen de protección de datos aplicable a las actividades de Europol con respecto al pro-

cesamiento de datos, tanto operativos como administrativos, es decir, incluyendo los datos personales necesarios para el desarrollo de sus actividades y los del propio personal de Europol.

A partir del RGPD, Europol ha sincronizado la función de protección de datos con la reforma del derecho a la protección de los datos personales en Europa, de modo que sobre la base del Reglamento Europol: «la agencia no solo intensifica sus esfuerzos para combatir el terrorismo, los delitos informáticos y otras formas de delincuencia grave y organizada, sino que también aumenta las salvaguardias de protección de datos, el control democrático, el control parlamentario y su función como la central de inteligencia criminal e intercambio de información».

Los protocolos de Europol incluyen la posibilidad de que cualquier persona pueda obtener información respecto de si sus datos personales son tratados por Europol, de modo que está previsto que se pueda ejercer el derecho de acceso, presentando una solicitud a Europol a través de la autoridad competente de cada Estado miembro; la petición es gestionada por la Unidad de Protección de Datos de Europol.

El delegado de protección de datos desempeña sus funciones de manera independiente, aunque forme parte de la organización, a lo que se añade el control externo del supervisor europeo de protección de datos, que proporciona asesoramiento sobre cuestiones de protección de datos a Europol y realiza inspecciones e investiga las quejas de particulares.

El supervisor europeo de protección de datos puede inspeccionar todos los archivos de Europol cuando lo considere conveniente, sus visitas de inspección a Europol se llevan a cabo en estrecha colaboración con la unidad de protección de datos de Europol.

Con independencia de los controles realizados por el delegado de protección de datos y el supervisor europeo, las autoridades de control de los Estados miembros, según su legislación nacional, también pueden verificar la transmisión de datos personales desde y hacia Europol.

Además, el Reglamento de Europol creó un «Consejo de Cooperación», con funciones de asesoramiento, que actúa de forma independiente, y está formado por un representante de cada autoridad nacional de protección de los Estados miembros de la Unión Europea, junto con el supervisor europeo de protección de datos.

3.2. La protección de datos en Eurojust: funciones y controles

Eurojust

Podéis visitar la página oficial de este órgano de la Unión Europea en:
http://eurojust.europa.eu/Pages/languages/ es.aspx

Eurojust se creó en el año 2002 mediante la «Decisión del Consejo de 28 de febrero de 2002 por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia». El objetivo de su creación era «apoyar y reforzar la coordinación y la cooperación entre las autoridades nacionales», en particular en la lucha contra las formas graves de delincuencia transfronteriza en la Unión Europea, es decir, en el territorio de la Unión Europea.

Posteriormente, mediante la Decisión 2009/426/JAI del Consejo, de 16 de diciembre de 2008, se modificaron algunos aspectos de Eurojust, con el objetivo de reforzar su actividad.

Su función principal es la de aumentar la eficacia de las autoridades nacionales de los Estados miembros de la Unión Europea, en la «investigación y persecución de las formas graves de delincuencia organizada y transfronteriza», con el objetivo de poner a los delincuentes, de forma rápida y eficaz, ante la Administración de Justicia.

Para desarrollar esa función, Eurojust se constituye en un centro de cooperación, de conocimiento y de experiencia a nivel judicial, en la lucha efectiva contra la delincuencia organizada, en el marco territorial de la Unión Europea.

Los Estados miembros de la Unión Europea designan a un representante en Eurojust, que tiene su sede en la Haya; los representantes puede ser fiscales, jueces o funcionarios de cuerpos policiales, que dispongan de las conocimientos y competencias especializadas, así como un alto grado de experiencia, en el ámbito de la investigación y persecución de formas graves de delincuencia organizada.

Los representantes de cada Estado miembro coordinan a las diferentes autoridades nacionales en sus investigaciones y en la persecución de los delitos, y además también abordan los posibles conflictos y problemas prácticos derivados de los diferentes sistemas legales de los Estados miembros.

En Eurojust también están integrados magistrados de enlace con terceros países, por tanto, que no son Estados miembros de la Unión Europea, en tanto Eurojust tenga un acuerdo de cooperación; por ejemplo, hay magistrados de enlace de Noruega y Estados Unidos. Eurojust tiene una plantilla de 260 personas (datos de Eurojust, mayo de 2019).

Además, en Eurojust se encuentran también las «Secretarías de la Red judicial europea, la Red de puntos de contacto en relación con personas responsables de genocidio, crímenes contra la humanidad y crímenes de guerra, y la Red de equipos conjuntos de investigación».

En Eurojust se tramitan unos 2.000 casos anualmente, y se hacen unas 200 reuniones de coordinación cada año, en las que participan autoridades nacionales judiciales y fiscales de los Estados miembros y, si es necesario, de terceros Estados, con el objeto de tratar las cuestiones relacionadas con la tramitación de los asuntos, adoptándose decisiones respecto de las acciones operativas necesarias para llevar a cabo las investigaciones, como por ejemplo, la planificación de detenciones o registros que deban llevarse a cabo de manera coordinada o en un mismo momento.

Por tanto, en esas reuniones se tratan asuntos concretos, en particular sobre delitos considerados como prioritarios por el Consejo de la Unión Europea, como pueden ser: «el terrorismo, narcotráfico, tráfico de seres humanos, fraude, corrupción, delito informático, blanqueo de capitales y otras actividades ilegales relacionadas con la presencia de grupos delictivos organizados en la economía».

Otro tipo de actividades que asume Eurojust tienen que ver con la resolución de conflictos de jurisdicción, cuando más de una autoridad nacional considera que es competente para investigar un asunto, o para llevar a cabo una actuación judicial concreta.

Eurojust facilita la ejecución de órdenes europeas de detención, y financia la creación y las necesidades operativas de los equipos conjuntos de investigación.

Eurojust lleva a cabo sus actividades en colaboración con otras entidades y organismos, como la Red judicial europea, Europol, OLAF, Frontex, Sitcen, CEPOL y la Red europea de escuelas judiciales, etc.; una colaboración que resulta esencial para abordar la lucha en común contra la delincuencia transfronteriza, donde el intercambio de información entre autoridades es imprescindible.

Por todo lo mencionado anteriormente, para asumir sus funciones Eurojust debe tratar un importante volumen de información, en muchos casos datos de carácter personal, ya sea de condenados, sospechosos, testigos o víctimas.

La denominada Autoridad Común de Control (ACC), es un organismo de supervisión independiente, previsto en el artículo 23 de la Decisión Eurojust, que supervisa las actividades de Eurojust relacionadas con el tratamiento de datos personales y controla que esos tratamientos de datos personales se lleven a cabo de conformidad con la mencionada Decisión Eurojust.

A diferencia del modelo de Europol, en el que la función de protección de datos está configurada sobre la base de un área de la propia organización, que da soporte al delegado de protección de datos, en el caso de Eurojust, la ACC es una autoridad de control, como pueden serlo las autoridades de protección de datos designadas por los Estados miembros.

Los miembros de la ACC suelen ser jueces o personas que tienen amplia experiencia en los campos de la protección de datos y la cooperación judicial, en ocasiones miembros de autoridades de protección de datos.

En el ejercicio de sus funciones de supervisión, la ACC tiene acceso a todos los datos personales tratados por Eurojust, además de a toda la información relacionada con las operaciones de tratamiento de esos datos, y Eurojust debe ayudar a la ACC con los medios e informaciones que en cada caso resulten más adecuados con relación al control que debe ejercer sobre los tratamientos de datos personales realizados en el marco de las actividades de Eurojust.

La función de supervisión incluye el control de cumplimiento de la normativa, por lo que la ACC efectúa inspecciones periódicas, incluyendo la verificación de la aplicación de todas las recomendaciones y conclusiones recogidas en los informes de inspección.

La ACC anualmente elabora un estudio sobre el nivel de cumplimiento en materia de protección de datos de Eurojust, que comparte con el responsable de la protección de datos de Eurojust (en adelante RPD), a fin de mejorar el nivel de cumplimiento por parte de la organización.

La ACC, con relación al responsable de protección de datos, es una instancia de recurso, cuando habiéndose detectado un incumplimiento, Eurojust no lo haya resuelto en un plazo de tiempo razonable; si la ACC considera que una decisión tomada por Eurojust, o un tratamiento de datos personales realizado por Eurojust, no cumple con la regulación, la ACC decidirá sobre ese asunto, de modo que Eurojust deberá aceptar esa decisión, ya que es definitiva y vinculante.

La ACC se acreditó como autoridad de supervisión independiente, y miembro de la Conferencia Internacional de Protección de Datos y Privacidad, durante la 32.ª conferencia celebrada en Israel los días 27 a 29 de octubre de 2010.

Por supuesto, se reconoce la posibilidad de que los interesados puedan ejercer derechos con relación a sus datos personales, como el derecho de acceso, de modo que se puede solicitar el acceso a cualquier información que Eurojust disponga del interesado.

Eurojust tiene un plazo de tres meses para responder, si bien puede negarse a proporcionar acceso a la información, si resulta necesario, para: «permitir que Eurojust cumpla sus tareas y obligaciones; proteger una investigación nacional

en curso; o proteger los derechos y libertades de terceros»; en el caso de que la persona interesada no considere adecuada la respuesta de Eurojust al ejercer su derecho de acceso podrá recurrir a la ACC para que resuelva al respecto.

Asimismo, se reconoce el derecho a pedir a Eurojust que corrija, elimine o bloquee datos personales que sean incorrectos o incompletos, si no se atiende tal solicitud, también se podrá recurrir a la ACC para que decida sobre la petición realizada.

3.3. Administración de Justicia: Consejo General del Poder judicial

En el contexto de la administración de justicia, y con relación al ejercicio de funciones de supervisión en materia de protección de datos personales, se da una casuística de una cierta complejidad que requiere ser analizada pormenorizadamente.

El artículo 236 nonies, de la Ley orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ) regula aspectos relacionados con el ejercicio de las funciones de autoridad de protección de datos en el ámbito de la administración de justicia, siendo el punto de partida lo previsto en su apartado 1, que dispone que las competencias de la Agencia Española de Protección de Datos «serán ejercidas, respecto de los tratamientos efectuados con fines jurisdiccionales y los ficheros de esta naturaleza, por el Consejo General del Poder Judicial».

Lo dispuesto en ese apartado 1 debe conectarse con lo previsto en el artículo 55.3 del RGPD, ya que establece que: «Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial».

Ese apartado 3 del artículo 55 debe completarse con el considerando 20 del RGPD, que, si bien se establece por un lado que el RGPD aplica a las actividades de los tribunales, también señala que debe preservarse la independencia del poder judicial en el desempeño de sus funciones, por lo que «la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial».

Así, considera que el control de esas operaciones de tratamiento debe atribuirse a organismos específicos, situados dentro del sistema judicial de cada Estado miembro, que deberán garantizar el cumplimiento del RGPD, concienciar a los miembros del poder judicial acerca de sus obligaciones en materia de protección de datos personales y atender las reclamaciones que en relación con esas operaciones de tratamiento planteen los interesados.

A su vez, en el apartado 2, del artículo 236 nonies, de la LOPJ, se dispone que: «Los tratamientos de datos llevados a cabo con fines no jurisdiccionales y sus correspondientes ficheros quedarán sometidos a la competencia de la Agencia Española de Protección de Datos, prestando el Consejo General del Poder Judicial a la misma la colaboración que al efecto precise».

Por tanto, en el contexto de la administración de justicia pueden llegar a actuar dos autoridades de control: el Consejo General del Poder Judicial y la Agencia Española de Protección de Datos.

Dado que la intervención de una u otra autoridad de control depende de que el tratamiento se realice con «fines jurisdiccionales», o no, conviene tener en cuenta lo previsto en el Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial, por el que se aprueba el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales, que en su artículo 87 dispone que los tratamientos de datos personales que se llevan a cabo en el ámbito de la administración de justicia están formados por «los datos de carácter personal que figuren en los procesos de los que conozcan y con los que consten en los procedimientos gubernativos. Los primeros se denominarán ficheros de datos jurisdiccionales y los segundos, ficheros de datos no jurisdiccionales».

En el apartado 2 del mencionado artículo 87 se refiere a que en los «ficheros» de datos jurisdiccionales solamente se contendrán los datos de carácter personal que se deriven de las actuaciones jurisdiccionales y, en particular, los siguientes:

a) Los que en atención a lo dispuesto en las leyes procesales sean necesarios para el registro e identificación del procedimiento o asunto jurisdiccional con el que se relacionan.

b) Los que sean necesarios para la identificación y localización de quienes pudieran tener derecho a intervenir como parte.

c) Los necesarios para la identificación de quienes asuman las labores de defensa o representación procesal o intervengan en cualquier otra calidad en el procedimiento o asunto.

d) Los que exterioricen las resoluciones dictadas y las actuaciones en él realizadas.

e) Los derivados de la instrucción o tramitación de las diligencias judiciales.

Por tanto, el control de cumplimiento de la normativa de protección de datos respecto de las operaciones de tratamiento de datos personales derivados de la actividad jurisdiccional, o siguiendo la expresión del RGPD, las operaciones «efectuadas por los tribunales en el ejercicio de su función judicial», debe ser realizado por el Consejo General del Poder Judicial.

Para el resto de los tratamientos de datos personales efectuados en el contexto de los órganos judiciales que no se deriven de la función judicial, será competente la Agencia Española de Protección de Datos.

Según el artículo 87.3 del Reglamento 1/2005: «en los ficheros de datos no jurisdiccionales solamente se contendrán los datos de carácter personal que deriven de los procedimientos gubernativos, así como los que, con arreglo a las normas administrativas aplicables, sean definitorios de la relación funcionarial o laboral de las personas destinadas en tales órganos y de las situaciones e incidencias que en ella acontezcan».

Los procedimientos gubernativos son aquellos que tramita y resuelve un juez, sin ejercitar sus potestades jurisdiccionales (por ejemplo, inscripciones registrales), en virtud del mencionado artículo 87.3 también quedan excluidos del ámbito jurisdiccional los datos personales relacionados con la gestión de recursos humanos en la Administración de Justicia.

Además, el artículo 560 de la LOPJ, entre las atribuciones que asigna al Consejo General del Poder Judicial, está la de «colaborar con la Autoridad de Control en materia de protección de datos en el ámbito de la administración de justicia. Asimismo, asumirá las competencias propias de aquella, únicamente respecto a la actuación de Jueces y Magistrados con ocasión del uso de ficheros judiciales».

En esa colaboración prevista en la LOPJ se sitúa el «Convenio de colaboración entre el Consejo General del Poder Judicial y la Agencia Española de Protección de Datos sobre colaboración en el ejercicio de las funciones propias de las autoridades de control en materia de protección de datos», publicado mediante la resolución de 6 de julio de 2017, de la Agencia Española de Protección de Datos.

El objeto de ese convenio es definir los ámbitos y mecanismos de mutua colaboración entre la Agencia Española de Protección de Datos y el Consejo General del Poder Judicial en las diversas funciones, que, como autoridades de control en sus respectivos ámbitos de actuación, deben llevar a cabo, centrándose en particular en las potestades de inspección, en materia de protección de datos, sobre órganos jurisdiccionales.

El artículo 53.3 de la LOPDGDD dispone, respecto del alcance de la actividad de investigación, que «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».

Posteriormente, la LOPDGDD ha recogido esa colaboración, cuando en su artículo 44.3 dispone que 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».

El RGPD prevé en su artículo 51.1 que, en cada Estado miembro, pueda existir más de una autoridad de control para supervisar la aplicación del Reglamento, por tanto, la posibilidad de que exista una autoridad de control específica para los tratamientos de datos personales relacionados con la función jurisdiccional está alineada con el RGPD, máxime si tenemos en cuenta lo ya mencionado con relación al artículo 55.3 del RGPD.

En el Convenio de julio de 2017, además de cuestiones relacionadas con la inspección, se prevén también acciones con relación a la generación de instrumentos para mejorar el cumplimiento de las obligaciones de protección de datos, sobre la base de códigos de buenas prácticas, el establecimiento de criterios generales para la seguridad de los datos y para la adopción de las medidas de responsabilidad activa previstas en el RGPD.

Además, se incluyen acuerdos en materia de formación para llevar a cabo actuaciones conjuntas, en particular mediante la celebración de seminarios al objeto de concienciar e informar al Poder Judicial sobre el RGPD.

Finalmente, el artículo 49, cuando regula la composición del Consejo Consultivo de la Agencia Española de Protección de Datos, prevé que en el mismo participe un representante designado por el Consejo General del Poder Judicial.

Resumen

El punto de partida del módulo es la descripción del escenario en que privacidad y seguridad pública se enfrentan, partiendo en primer lugar de la manera en la que el ordenamiento jurídico afronta el tratamiento de datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de la ejecución de las sanciones penales, ofreciendo garantías no solo sobre la base de las normas, también desde la perspectiva de la garantía institucional que representan las autoridades de control.

Una buena parte del módulo se ha ocupado de entender las necesidades policiales con relación a la investigación de delitos que afectan a los datos personales, en particular a aquellos datos que están situados en la red. A esta se aplican conceptos como ciberdelitos y ciberdelincuencia, y se examina de qué modo debe ser respetado el derecho fundamental para evitar que el enjuiciamiento de esas conductas vulnere dicho derecho y en todo caso se adopten las debidas garantías.

Bibliografía

Lectura obligatoria

Piñar Mañas, José Luis (2009). «Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio» [en línea]. Documentos de trabajo (núm. 147, págs. 16-30). Fundación Alternativas. ISBN: 978-84-92424-66-5. http://bit.ly/32Paw2W

Lecturas recomendadas

Alonso Moreda, Nicolás (2012, enero-abril). «EUROJUST, a la vanguardia de la cooperación judicial en materia penal de la Unión Europea» [en línea]. Revista de Derecho Comunitario Europeo (núm. 41, págs. 119-157). http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=1285&IDA=36305

Black, Edwin (2001). *IBM y el holocausto*. Buenos Aires: Editorial Atlántida. ISBN 9789500824668.

Santos Vara, Juan (2003, enero-abril). «El desarrollo de las competencias de la Oficina Europea de Policía (EUROPOL): el control democrático y judicial» [en línea]. Revista de Derecho Comunitario Europeo (núm. 14, págs. 141-179). https://recyt.fecyt.es/index.php/RDCE/article/view/48381/29854

Troncoso Reigada, Antonio (2011). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch. ISBN 9788498769807.

Warren, Samuel D.; Brandeis, Louis D. (1890). «The right to privacy» [en línea]. Harvard Law Review (vol. 4, núm. 5, págs. 193-220). http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Otros recursos

Eurojust: http://www.eurojust.europa.eu/Pages/home.aspx

Europol: https://www.europol.europa.eu/