

UNIDAD DIDÁCTICA 20

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Autor: Departamento de Ciencias Jurídicas

Fecha: 28-10-2024

OBJETIVOS ESPECÍFICOS

- Conocer la legislación en materia de protección de datos de carácter personal.
- Analizar la Ley Orgánica 3/2018.
- Analizar la Ley Orgánica 7/2021.

CONTENIDOS

¿QUÉ SABE DEL TEMA?

- ¿Qué debe entenderse por “*datos personales*”?
- ¿Qué se conoce por “tratamiento”?
- ¿Qué principios regirán el tratamiento de los datos personales?
- ¿Cómo proceder ante la recogida y tratamiento de los datos para fines policiales por las Fuerzas y Cuerpos de Seguridad?

ÍNDICE DE CONTENIDOS

1.- LEY ORGÁNICA 3/2018, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.

- 1.1.- Disposiciones generales.
- 1.2.- Principios de protección de datos.
- 1.3.- Derechos de las personas:
- 1.4.- Disposiciones aplicables a tratamientos concretos.
- 1.5.- Responsable y encargado del tratamiento.
- 1.6.- Garantía de los derechos digitales.

2.- LEY ORGÁNICA 7/2021, DE PROTECCIÓN DE DATOS PERSONALES TRATADOS PARA FINES DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN Y ENJUICIAMIENTO DE INFRACCIONES PENALES Y DE EJECUCIÓN DE SANCIONES PENALES.

- 2.1.- Autoridades de protección de datos independientes.
- 2.2.- Régimen sancionador.

3.- ASPECTOS RELEVANTES

1.- LEY ORGÁNICA 3/2018, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.

1.1.- Disposiciones generales.

La presente ley orgánica tiene por objeto:

- a)** Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta LO.
- b)** Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Esta ley orgánica no será de aplicación:

- a)** A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.
- b)** A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.
- c)** A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se registrarán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, del Poder Judicial, que le sean aplicables.

El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se registrarán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, del Poder Judicial y de las normas procesales que le sean aplicables

1.2.- Principios de protección de datos.

- a) Exactitud de los datos:** Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

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

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

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable.

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

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

b) Deber de confidencialidad: Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679, lo que será complementario de los deberes de secreto profesional. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

c) Tratamiento basado en el consentimiento del afectado :De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

d) Consentimiento de los menores de edad: El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

e) Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos: El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

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

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

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

1.3.- Derechos de las personas:

Disposiciones generales sobre ejercicio de los derechos:

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

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

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

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

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

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

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

- a) **Derecho de acceso:** El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679. Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

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

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

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

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

- b) Derecho de rectificación:** Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.
- c) Derecho de supresión:** El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.
- d) Derecho a la limitación del tratamiento:** El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.
- e) Derecho a la portabilidad:** El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.
- f) Derecho de oposición:** El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

1.4.- Disposiciones aplicables a tratamientos concretos.

a) Tratamientos con fines de videovigilancia

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

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

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

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

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

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

También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio. Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

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

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

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

b) Tratamiento de datos relativos a infracciones y sanciones administrativas:

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

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

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

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

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

1.5.- Responsable y encargado del tratamiento.

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

a) Los colegios profesionales y sus consejos generales.

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

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

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

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

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

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

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

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

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

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

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

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

ñ) Las empresas de seguridad privada.

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

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

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

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

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

c) Cualificación del delegado de protección de datos

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

d) Posición del delegado de protección de datos

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

Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

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

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

e) Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame. En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes. Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

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

1.6.- Garantía de los derechos digitales.

Acerca de la “Era digital”, los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

- a) **Derecho a la neutralidad de Internet:** Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.
- b) **Derecho de acceso universal a Internet:** Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.

Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

- c) **Derecho a la seguridad digital:** Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.
- d) **Derecho a la educación digital:** El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

- e) Protección de los menores en Internet:** Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

- f) Protección de datos de los menores en Internet:** Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

2.- LEY ORGÁNICA 7/2021, DE PROTECCIÓN DE DATOS PERSONALES TRATADOS PARA FINES DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN Y ENJUICIAMIENTO DE INFRACCIONES PENALES Y DE EJECUCIÓN DE SANCIONES PENALES.

Esta Ley Orgánica tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

En cuanto al ámbito de aplicación, se aplicará al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

El tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, en el ámbito del artículo 1, se regirá por lo dispuesto en la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, del Poder Judicial, las leyes procesales que le sean aplicables y, en su caso, por la Ley 50/1981, por la que se regula el Estatuto Orgánico del Ministerio Fiscal. Las autoridades de protección de datos a las que se refiere el capítulo VI no serán competentes para controlar estas operaciones de tratamiento.

Quedan fuera del ámbito de aplicación de esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los realizados por las autoridades competentes para fines distintos de los previstos en el artículo 1, incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos. Estos tratamientos se someterán plenamente a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como en la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales.

b) Los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito de aplicación del capítulo II del título V del Tratado de la Unión Europea.

c) Los tratamientos que afecten a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea.

d) Los sometidos a la normativa sobre materias clasificadas, entre los que se encuentran los tratamientos relativos a la Defensa Nacional.

e) Los tratamientos realizados en las acciones civiles y procedimientos administrativos o de cualquier índole vinculados con los procesos penales que no tengan como objetivo directo ninguno de los fines del artículo 1.

4. Esta Ley Orgánica no se aplicará a los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo siguiente.

Autoridades competentes

Será autoridad competente, a los efectos de esta Ley Orgánica, toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos en el artículo 1. En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:

a) Las Fuerzas y Cuerpos de Seguridad.

b) Las Administraciones Penitenciarias.

c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria.

d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

2. También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Definiciones: A efectos de esta Ley Orgánica se entenderá por:

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

b) **«tratamiento»:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración,

conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

c) **«limitación del tratamiento»**: el marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro;

d) **«elaboración de perfiles»**: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

e) **«seudonimización»**: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

f) **«fichero»**: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o dispersado de forma funcional o geográfica;

g) **«responsable del tratamiento» o «responsable»**: la autoridad competente que sola o conjuntamente con otras, determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión Europea o por la legislación española, dichas normas podrán designar al responsable del tratamiento, o bien los criterios para su nombramiento.

h) **«encargado del tratamiento» o «encargado»**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

i) **«destinatario»**: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerará destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con la legislación española o de la Unión Europea; el tratamiento de tales datos por las citadas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Deber de colaboración: Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el artículo 549.1 de la

Ley Orgánica 6/1985 y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal.

La comunicación de datos, informes, antecedentes y justificantes por la Administración Tributaria, la Administración de la Seguridad Social y la Inspección de Trabajo y Seguridad Social, se efectuará de acuerdo con su legislación respectiva.

En los restantes casos, las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. La petición de la autoridad competente deberá ser concreta y específica y contener la motivación que acredite su relación con los indicados supuestos.

No será de aplicación lo dispuesto en los apartados anteriores cuando legalmente sea exigible la autorización judicial para recabar los datos necesarios para el cumplimiento de los fines del artículo 1.

En los supuestos contemplados en los apartados anteriores, el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.

Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga un deber específico de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1, no informarán al interesado de la transmisión de sus datos a dichas autoridades, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, en cumplimiento de sus obligaciones específicas.

Tratamiento de categorías especiales de datos personales: El 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, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:

a) Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.

b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.

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

Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Los datos de los menores de edad y de las personas con capacidad modificada judicialmente o que estén incurso en procesos de dicha naturaleza, se tratarán garantizando el interés superior de los mismos y con el nivel de seguridad adecuado.

Tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad: Sistemas de grabación de imágenes y sonido por las Fuerzas y Cuerpos de Seguridad: La captación, reproducción y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad en los términos previstos en esta Ley Orgánica, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

En la instalación de sistemas de grabación de imágenes y sonidos se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.

Instalación de sistemas fijos: En las vías o lugares públicos donde se instalen videocámaras fijas, el responsable del tratamiento deberá realizar una valoración del citado principio de proporcionalidad en su doble versión de idoneidad e intervención mínima. Asimismo, deberá llevar a cabo un análisis de los riesgos o una evaluación de impacto de protección de datos relativo al tratamiento que se pretenda realizar, en función del nivel de perjuicio que se pueda derivar para la ciudadanía y de la finalidad perseguida.

Se entenderá por videocámara fija aquella anclada a un soporte fijo o fachada, aunque el sistema de grabación se pueda mover en cualquier dirección.

Esta disposición se aplicará asimismo cuando las Fuerzas y Cuerpos de Seguridad utilicen instalaciones fijas de videocámaras de las que no sean titulares y exista, por su parte, un control y dirección efectiva del proceso completo de tratamiento. Estas instalaciones fijas de videocámaras no estarán sujetas al control preventivo de las entidades locales previsto en su legislación reguladora básica, ni al ejercicio de las competencias de las diferentes Administraciones públicas, sin perjuicio de que deban

respetar los principios de la legislación vigente en cada ámbito material de la actuación administrativa.

Los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por estas instalaciones, o quienes los posean por cualquier título, están obligados a facilitar y permitir su instalación y mantenimiento, sin perjuicio de las indemnizaciones que procedan.

Los ciudadanos serán informados de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos.

Dispositivos móviles: Podrán utilizarse dispositivos de toma de imágenes y sonido de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley Orgánica, conforme a las competencias específicas de las Fuerzas y Cuerpos de Seguridad. La toma de imagen y sonido, que ha de ser conjunta, queda supeditada, en todo caso, a la concurrencia de un peligro o evento concreto. El uso de los dispositivos móviles deberá estar autorizado por la persona titular de la Delegación o Subdelegación del Gobierno, quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización de dichos dispositivos a los principios de tratamiento y al de proporcionalidad.

En el caso de los Cuerpos de Policía propios de las Comunidades Autónomas que tengan y ejerzan competencias asumidas para la protección de las personas y bienes y para el mantenimiento del orden público, serán sus órganos correspondientes los que autorizarán este tipo de actuaciones para sus fuerzas policiales, así como para las dependientes de las Corporaciones locales radicadas en su territorio.

En estos supuestos de dispositivos móviles, las autorizaciones no se podrán conceder en ningún caso con carácter indefinido o permanente, siendo otorgadas por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro.

En casos de urgencia o necesidad inaplazable será el responsable operativo de las Fuerzas y Cuerpos de Seguridad competentes el que podrá determinar su uso, siendo comunicada tal actuación con la mayor brevedad posible, y siempre en el plazo de 24 horas, al Delegado o Subdelegado del Gobierno o autoridad competente de las comunidades autónomas.

Tratamiento y conservación de las imágenes: Realizada la filmación de acuerdo con los requisitos establecidos en esta Ley Orgánica, si la grabación captara la comisión de hechos que pudieran ser constitutivos de infracciones penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación.

De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

Si se captaran hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad pública, se remitirán al órgano competente, de inmediato, para el inicio del oportuno procedimiento sancionador. Las grabaciones serán destruidas en el plazo máximo de tres meses desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

Régimen disciplinario: Sin perjuicio de las responsabilidades penales en las que pudieran incurrir, las infracciones a lo dispuesto en esta Ley Orgánica por los miembros de las Fuerzas y Cuerpos de Seguridad, serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de protección de datos de carácter personal establecido en esta Ley Orgánica. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:

- a) Alterar o manipular los registros de imágenes y sonidos, siempre que no constituya delito.
- b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar estos para fines distintos de los previstos legalmente.
- c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley Orgánica.
- d) Utilizar los medios técnicos regulados en esta Ley Orgánica para fines distintos de los previstos en la misma.

Información que debe ponerse a disposición del interesado: El responsable del tratamiento de los datos pondrá a disposición del interesado, al menos, la siguiente información:

La identificación del responsable del tratamiento y sus datos de contacto. Los datos de contacto del delegado de protección de datos, en su caso. Los fines del tratamiento a los que se destinen los datos personales. El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma. El derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o la limitación de su tratamiento.

Además de la información a la que se refiere el apartado 1, atendiendo a las circunstancias del caso concreto, el responsable del tratamiento proporcionará al interesado la siguiente información adicional para permitir el ejercicio de sus derechos:

a) La base jurídica del tratamiento.

b) El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo.

c) Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.

d) Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado.

Derecho de acceso del interesado a sus datos personales: El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen. En caso de que se confirme el tratamiento, el interesado tendrá derecho a acceder a dichos datos personales, así como a la siguiente información:

a) Los fines y la base jurídica del tratamiento.

b) Las categorías de datos personales de que se trate.

c) Los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular, los destinatarios establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.

d) El plazo de conservación de los datos personales, cuando sea posible, o, en caso contrario, los criterios utilizados para determinar dicho plazo.

e) La existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado o la limitación de su tratamiento.

f) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma.

g) La comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen, sin revelar la identidad de ninguna persona física, en especial en el caso de fuentes confidenciales.

Cuando el responsable trate una gran cantidad de información relativa al interesado y éste ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá requerir al interesado que concrete la solicitud en el plazo de diez días.

Se entenderá concedido el derecho de acceso si el responsable del tratamiento facilita al interesado un sistema remoto, directo y seguro que garantice, de modo permanente, el acceso a la totalidad de sus datos personales. La notificación informando al interesado del procedimiento puesto en marcha a través de este sistema, permitirá denegar su solicitud de acceso efectuada por otras vías.

Si el acceso remoto no facilita la totalidad de la información contenida en el apartado 1, el interesado tendrá derecho a solicitarla.

Cuando el interesado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho interesado asumirá el exceso de coste que su elección comporte. En este caso, sólo será exigible al responsable del tratamiento que la satisfacción del derecho de acceso a través del medio propuesto se produzca sin dilaciones indebidas. Si el interesado no asumiera el exceso de coste, se le facilitará el acceso por el medio inicialmente propuesto por el responsable del tratamiento.

Restricciones a los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento: El responsable del tratamiento podrá aplazar, limitar u omitir la información a la que se refiere el artículo 21.2, así como denegar, total o parcialmente, las solicitudes de ejercicio de los derechos contemplados en los artículos 22 y 23, siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, resulte necesario y proporcional para la consecución de los siguientes fines:

- a) Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales.
- b) Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.
- c) Proteger la seguridad pública.
- d) Proteger la Seguridad Nacional.
- e) Proteger los derechos y libertades de otras personas.

En caso de restricción de los derechos contemplados en los artículos 22 y 23, el responsable del tratamiento informará por escrito al interesado sin dilación indebida, y en todo caso, en el plazo de un mes a contar desde que tenga conocimiento, de dicha restricción, de las razones de la misma, así como de las posibilidades de presentar una reclamación ante la autoridad de protección de datos, sin perjuicio de las restantes acciones judiciales que pueda ejercer en virtud de lo dispuesto en esta Ley Orgánica.

Las razones de la restricción podrán ser omitidas o ser sustituidas por una redacción neutra cuando la revelación de los motivos de la restricción pueda poner en riesgo los fines a los que se refiere el apartado anterior.

El responsable del tratamiento documentará los fundamentos de hecho o de derecho en los que se sustente la decisión denegatoria del ejercicio del derecho de acceso. Dicha información estará a disposición de las autoridades de protección de datos.

Ejercicio de los derechos del interesado a través de la autoridad de protección de datos: En los casos en que se produzca un aplazamiento, limitación u omisión de la información a que se refiere el artículo 21 o una restricción del ejercicio de los derechos contemplados en los artículos 22 y 23, en los términos previstos en el artículo 24, el interesado podrá ejercer sus derechos a través de la autoridad de protección de datos competente. El responsable del tratamiento informará al interesado de esta posibilidad.

Cuando, en virtud de lo establecido en el apartado anterior, se ejerciten los derechos a través de la autoridad de protección de datos, esta deberá informar al interesado, al menos, de la realización de todas las comprobaciones necesarias o la revisión correspondiente y de su derecho a interponer recurso contencioso-administrativo.

Derechos de los interesados como consecuencia de investigaciones y procesos penales: El ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento se llevará a cabo de conformidad con las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales. Cuando los datos sean objeto de un tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional penal, o el Ministerio Fiscal, el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento se realizará de conformidad con lo previsto en la Ley Orgánica 6/1985, en las normas procesales y en su caso, el Estatuto Orgánico del Ministerio Fiscal. En defecto de regulación del ejercicio de estos derechos en dichas normas, se aplicará lo dispuesto en esta Ley Orgánica.

2.1.- Autoridades de protección de datos independientes.

A los efectos de esta Ley Orgánica son autoridades de protección de datos independientes:

a) La Agencia Española de Protección de Datos.

b) Las autoridades autonómicas de protección de datos, exclusivamente en relación a aquellos tratamientos de los que sean responsables en su ámbito de competencia, y conforme a lo dispuesto en el artículo 57.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en la normativa autonómica aplicable.

Dichas autoridades se regirán por esta Ley Orgánica respecto de los tratamientos sometidos a la misma, de acuerdo con los principios de cooperación institucional, coordinación de criterios e información mutua, y por lo establecido en el Título VII de la Ley Orgánica 3/2018, de 5 de diciembre, y en sus normas de creación, así como por lo que establezcan sus normas de desarrollo.

La Agencia Española de Protección de Datos actuará como representante de las autoridades de protección de datos en el Comité Europeo de Protección de Datos. Las autoridades de protección de datos ejercerán, respecto de los tratamientos sometidos a esta Ley Orgánica, las siguientes funciones:

a) Supervisar y hacer cumplir las disposiciones adoptadas con arreglo a esta Ley Orgánica.

b) Promover la sensibilización y la comprensión de la ciudadanía acerca de los riesgos, normas, garantías y derechos relativos al tratamiento.

c) Asesorar a las Cortes Generales, al Gobierno de la Nación y a los organismos dependientes o vinculados a la Administración General del Estado, así como, de acuerdo con su ámbito competencial, a las Asambleas Legislativas de las comunidades autónomas, los Consejos de Gobierno y los organismos dependientes o vinculados a la Administración de las comunidades autónomas, acerca de las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.

d) Promover la sensibilización de los responsables y encargados del tratamiento en relación con las obligaciones que les incumben.

e) Facilitar la información solicitada por los interesados sobre el ejercicio de sus derechos en virtud de esta Ley Orgánica y, en su caso, cooperar a tal fin con las autoridades de protección de datos de otros Estados miembros de la Unión Europea.

f) Tramitar y responder las reclamaciones presentadas por un interesado o por una entidad, organización o asociación de conformidad con el artículo 55, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.

g) Controlar, de acuerdo con lo dispuesto en el artículo 25, la licitud del tratamiento e informar al interesado en un plazo razonable sobre el resultado del control o sobre los motivos por los que no se ha llevado a cabo.

h) Cooperar, en particular compartiendo información, con otras autoridades de protección de datos y prestarse asistencia mutua.

i) Llevar a cabo investigaciones sobre la aplicación de esta Ley Orgánica, en particular basándose en la información recibida de otra autoridad de protección de datos u otra autoridad pública.

j) Realizar un seguimiento de acontecimientos que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, de manera concreta sobre el desarrollo de las tecnologías de la información y la comunicación.

k) Prestar asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36.

l) Contribuir a las actividades del Comité Europeo de Protección de Datos.

m) Informar todas las disposiciones legales o reglamentarias que afecten a tratamientos sometidos a esta Ley Orgánica.

2. Las autoridades de protección de datos adoptarán medidas tendentes a facilitar la formulación de las reclamaciones incluidas en el párrafo 1f), tales como proporcionar formularios que puedan cumplimentarse electrónicamente, sin excluir otros medios.

3. El desempeño de las funciones de las autoridades de control no implicará coste alguno para el interesado ni para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de protección de datos podrá negarse a actuar respecto de la solicitud. La carga de la demostración del carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de protección de datos.

Potestades: Las autoridades de protección de datos tendrán atribuidas, en el ámbito de esta Ley Orgánica, las siguientes potestades:

a) De investigación, incluyendo el acceso a todos los datos que estén siendo tratados por el responsable o el encargado del tratamiento, en los términos previstos por la legislación vigente.

b) De advertencia y control de lo exigido en esta Ley Orgánica, incluida la sanción de las infracciones cometidas, la elaboración de recomendaciones, órdenes de rectificación, supresión o limitación del tratamiento de datos personales o de limitación temporal o definitiva del tratamiento, incluida su prohibición, así como la orden a los responsables del tratamiento de comunicar las vulneraciones de seguridad de los datos a los interesados.

c) De asesoramiento, que comprende la consulta previa prevista en el artículo 36 y la emisión, por propia iniciativa o previa solicitud, de dictámenes destinados a las Cortes Generales o al Gobierno, a otras instituciones u organismos, así como al público en general, acerca de todo asunto relacionado con la protección de datos personales sujeto a esta Ley Orgánica.

2.2.- Régimen sancionador.

La responsabilidad por las infracciones cometidas recaerá directamente en los sujetos obligados que, por acción u omisión, realizaran la conducta en que consista la infracción. Están sujetos al régimen sancionador:

- a) Los responsables de los tratamientos.
- b) Los encargados de los tratamientos.
- c) Los representantes de los encargados no establecidos en el territorio de la Unión Europea.
- d) El resto de las personas físicas o jurídicas obligadas por el contenido del deber de colaboración establecido en el artículo 7.

No será de aplicación el régimen sancionador establecido en este capítulo al delegado de protección de datos.

Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra Ley, siempre que no constituyan infracciones al Reglamento General de Protección de Datos, ni a la Ley Orgánica 3/2018, se sancionarán observando las siguientes reglas:

- a) El precepto especial se aplicará con preferencia al general.
- b) El precepto más amplio o complejo absorberá el que sancione las infracciones subsumidas en aquel.
- c) En defecto de los criterios anteriores, se aplicará el precepto que sancione los hechos con la sanción mayor.

En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción que conlleve una mayor sanción.

Régimen jurídico: El ejercicio de la potestad sancionadora, que corresponde a las Autoridades de protección de datos competentes, se regirá por lo dispuesto en el presente Capítulo, por los títulos VII y IX de la Ley Orgánica 3/2018 y en cuanto no las contradigan, con carácter supletorio, por la normativa sobre procedimiento administrativo común de las Administraciones públicas y el régimen jurídico del sector público.

Carácter subsidiario del procedimiento administrativo sancionador respecto del penal: No podrán sancionarse los hechos que hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, de hecho y de fundamento.

En los supuestos en que las conductas pudieran ser constitutivas de delito, el órgano administrativo pasará el tanto de culpa a la autoridad judicial o al Ministerio Fiscal y se abstendrá de seguir el procedimiento sancionador mientras la autoridad judicial no dicte sentencia firme o resolución que de otro modo ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o proseguir las actuaciones en vía penal, quedando hasta entonces interrumpido el plazo de prescripción.

La autoridad judicial y el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que hubieran adoptado. De no haberse estimado la existencia de ilícito penal, o en el caso de haberse dictado resolución de otro tipo que ponga fin al procedimiento penal, podrá iniciarse o proseguir el procedimiento sancionador. En todo caso, el órgano administrativo quedará vinculado por los hechos declarados probados en vía judicial. Las medidas cautelares adoptadas antes de la intervención judicial podrán mantenerse mientras la autoridad judicial no resuelva otra cosa.

3.- ASPECTOS RELEVANTES

- La LO 3/2018, PDPGDD tiene por objeto: a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones, y b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.
- Según la LO 3/2018, PDPGDD, el tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.
- La LO 7/2021 tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.
- En la LO 7/2021 se establece que sin perjuicio de las responsabilidades penales en las que pudieran incurrir, las infracciones a lo dispuesto en esta Ley Orgánica por los miembros de las Fuerzas y Cuerpos de Seguridad, serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de protección de datos de carácter personal establecido en esta Ley Orgánica.

EVALUACIÓN

1.- El art. 1 de la LO 3/2018, declara que el objeto de la ley es:

- a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo.
- b) Adaptar el ordenamiento jurídico español a la Directiva (UE) 2016/680, del Parlamento Europeo y el Consejo.
- c) Ninguno de los anteriores.

2.- En la LO 3/2018 se establece que los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos. A esto se le conoce como:

- a) Derecho a la asimetría de Internet.
- b) Derecho a mutabilidad de Internet.
- c) Derecho a la neutralidad de Internet.

3.- En las vías o lugares públicos donde se instalen videocámaras fijas, el responsable del tratamiento deberá realizar una valoración del citado principio de proporcionalidad en su doble versión:

- a) De mínima intervención y de oportunidad.
- b) De intervención mínima y de idoneidad.
- c) De oportunidad y proporcionalidad.

SOLUCIONES

Pregunta número	Respuesta
1	a
2	c
3	b