Francisco Javier Enériz Olaechea

Defensor del Pueblo de Navarra

La protección de datos de carácter personal, en general. Los ficheros de las Fuerzas y Cuerpos de Seguridad, en particular.

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, EN GENERAL. LOS FICHEROS DE LAS FUERZAS Y CUERPOS DE SEGURIDAD, EN PARTICULAR

Francisco Javier Enériz Olaechea
Defensor del Pueblo de Navarra

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

Título**: La protección de datos de carácter personal, en general. Los ficheros de las Fuerzas y Cuerpos de Seguridad, en particular.**

Edita*:* Institución del Defensor del Pueblo de la Comunidad Foral de Navarra

Diseño y maquetación: Carlos Fernández Prego

SUMARIO

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

SUMARIO: I. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: OBJETO Y DEFINICIONES. 1.1. Objeto. 1.2. Ámbito de aplicación de la Ley Orgánica de protección de datos de carácter personal. 1.3. Definiciones. II. LOS PRINCIPIOS GENERALES APLICABLES AL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL. A) Principio de calidad de los datos: fin legítimo y proporcionalidad. B) Principio de consentimiento del afectado. Los datos especialmente protegidos. El derecho de oposición. C) Principio de veracidad del dato. El derecho a la rectificación y el derecho a la cancelación. D) Principio de licitud del dato. E) Principio de acceso al dato. F) Principio de vida útil del dato. Cancelación y conservación de los datos. III. LOS FICHEROS DE TITULARIDAD PÚBLICA. CREACIÓN, MODIFICACIÓN O SUPRESIÓN. IV. LA COMUNICACIÓN DE DATOS ENTRE LAS ADMINISTRACIONES PÚBLICAS. A) Régimen general: principio del consentimiento previo y excepciones. B) Régimen especial de comunicación de datos entre Administraciones públicas. V. FICHEROS DE LAS FUERZAS Y CUERPOS DE SEGURIDAD. 5.1. Reglas generales conforme a la LOPDP. 5.2. La grabación de imágenes por las Fuerzas y Cuerpos de Seguridad. 5.3. La denominada base de datos policial sobre identificadores obtenidos a partir del ADN.

1

La protección de datos de carácter personal: objeto y definiciones.

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

1. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: OBJETO Y DEFINICIONES.

1.1. OBJETO.

La protección de los datos de carácter personal se regula hoy en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPDP), y en su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

La LOPDP responde a lo dicho en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, que es un tratado vinculante para las instituciones de la UE y los Estados miembros cuando apliquen el Derecho de la UE:

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acce-

der a los datos recogidos que la conciernan y a su rectificación.

3. *El resto de estas normas quedará sujeto al control de una autoridad independiente."*

La LOPDP tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar (art. 1).

Se vincula, por tanto, con el derecho a la intimidad personal y familiar y con el derecho al honor de las personas físicas. A estos derechos ha de añadirse otro derecho más, también de protección constitucional: el derecho a la propia imagen.

En estos momentos, se tramita en la UE un proyecto de Reglamento General de Protección de Datos de Carácter Personal, que supondrá, cuando entre en vigor, la modificación de la LOPDP. El artículo 2.2 del proyecto de Reglamento prevé dejar fuera de su ámbito de aplicación material el tratamiento de datos personales "por parte de las autoridades competentes con fines de prevención, investigación, detec-

ción o enjuiciamiento de infracciones penales o de ejecución de sanciones penales".

1.2. ÁMBITO DE APLICACIÓN DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

El artículo 2 de la LOPDP establece su ámbito de aplicación.

Así, **la Ley se aplica** a:

a) Los datos de carácter personal registrados en soporte físico, que los hagan susceptibles de tratamiento, y a

b) Toda modalidad de uso posterior de estos datos por los sectores público y privado.

Por el contrario, **no se aplica la LOPDP** a:

a) Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) Los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, si bien el responsable del fichero debe comunicar previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos (AEDP).

Se **rigen por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica** los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

También se aplica plenamente la LOPDP a los tratamientos de imágenes de personas físicas con fines de vigilancia, obtenidas con sistemas de cámaras y videocámaras, cuando dicha vigilancia ya no se hace por las Fuerzas y Cuerpos de Seguridad, sino por otros sistemas públicos o privados. Este tratamiento se somete a lo dispuesto en la Instrucción 1/2006, de 8 de noviembre, de la AEPD. Esta instrucción obliga a los responsables de los sistemas de videovigilancia a colocar, en las zonas videovigiladas, un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados, y tener a disposición de los interesados impresos en los que se detalle la información que requiere la LOPDP.

Las cámaras instaladas en espacios privados no pueden obtener imágenes de espacios públicos, salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En la práctica, por tanto, sí que pueden obtenerse esas imágenes de los espacios públicos.

En todo caso, debe evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida. La finalidad es la protección del edificio frente a posibles ataques a las personas, la propiedad privada, la integridad de los elementos físicos, etcétera.

Los datos han de cancelarse en el plazo máximo de un mes desde su captación.

La creación de esos ficheros de videovigilancia, cada vez más abundantes, debe notificarse previamente a la AEPD, para su inscripción en el Registro General de Protección de Datos. Si el fichero es público, ha de crearse mediante una disposición general. Lo aquí dispuesto no se aplica si el tratamiento consiste exclusivamente en la reproducción o emisiones de imágenes en tiempo real.

1.3. DEFINICIONES.

El artículo 3 de la LOPDP establece algunas definiciones de interés. Se entiende por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento de datos.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al

grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

2

Los principios generales aplicables al tratamiento de los datos de carácter personal.

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

2. LOS PRINCIPIOS GENERALES APLICABLES AL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL.

El tratamiento de los datos de carácter personal está sujeto a varios principios.

Tales principios son los siguientes:

A) Principio de calidad de los datos: fin legítimo y proporcionalidad (artículo 4, números 1 y 2).

Conforme a este principio, los datos de carácter personal sólo se pueden recogerse para su tratamiento y tratados cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Estos datos no pueden usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido

recogidos. No se considera incompatible el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

B) Principio de consentimiento del afectado (artículos 6, 7 y 8). Los datos especiales protegidos. El derecho de oposición.

El tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

No se precisa el consentimiento:

- Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.

- Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7.6 de la LOPDP.

- Cuando los datos figuren en fuentes accesibles al público (guía telefónica, guía de colegios profesionales, etcétera) y su tratamiento sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

El consentimiento puede ser revocado cuando exista causa justificada para ello, pero sin efectos retroactivos.

En los casos en los que no es necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que la ley no disponga lo contrario, el interesado puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. Es el denominado derecho de oposición. En tal supuesto, el responsable del fichero debe excluir del tratamiento los datos relativos al afectado.

Está también relacionado con el equivocadamente denominado “derecho al olvido”.

Hay **datos especialmente protegidos**, que requieren para su tratamiento el consentimiento **expreso y por escrito** del afectado. Son los datos que revelan la ideología, la afiliación sindical, la religión y las creencias. La ley parte de que nadie puede ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar su consentimiento, ha de advertirse al interesado acerca de su derecho a no prestarlo.

Se exceptúan de lo anterior los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros. Pero la cesión de estos datos sí que precisa siempre el previo consentimiento del afectado.

También son **datos especialmente protegidos** los que hagan referencia al origen racial, a la salud y a la vida

sexual. Estos solo pueden recabarse, tratarse y cederse cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

Están prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas solo pueden ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Pueden tratarse sin consentimiento del interesado datos personales cuando el tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También pueden ser objeto de tratamiento los datos personales cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Por ello, el artículo 8 de la LOPDP permite a las instituciones, centros sanitarios públicos y privados y profesionales correspondientes el tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

C) Principio de veracidad del dato (artículo 4.3). El derecho a la rectificación y el derecho a la cancelación.

Los datos de carácter personal han de ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Consecuencia de ello es que el afectado tiene derecho a su rectificación.

Es más, si los datos de carácter personal registrados resultan ser inexactos, en todo o en parte, o incompletos,

deben ser cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16 para su rectificación.

El artículo 16 de la LOPDP regula los derechos de rectificación o cancelación del afectado.

Ejercido este derecho, si el dato resulta inexacto o incompleto, el responsable del tratamiento tiene la obligación de hacer efectiva la rectificación o cancelación en el plazo de diez días.

La cancelación da lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de estas. Cumplido el citado plazo, debe procederse a la supresión.

Si los datos rectificados o cancelados han sido comunicados a terceros, el responsable del tratamiento debe notificar a estos la rectificación o cancelación efectuada, quienes también deben proceder a la cancelación en el caso de que mantengan el tratamiento.

D) Principio de licitud del dato (artículo 4.7).

La LOPDP prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. Estos datos no son válidos.

E) Principio de acceso al dato (artículo 4.6).

Los datos de carácter personal deben almacenarse de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

F) Principio de vida útil del dato (artículo 4.5). Cancelación y conservación de los datos.

Los datos de carácter personal deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No deben conservarse en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Pero pueden conservarse íntegramente, con determinadas garantías, los datos que sirven a valores históricos, estadísticos o científicos de acuerdo con la legislación específica.

3

Los ficheros de titularidad pública. Creación, modificación o supresión.

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

3. LOS FICHEROS DE TITULARIDAD PÚBLICA. CREACIÓN, MODIFICACIÓN O SUPRESIÓN.

Como es lógico, las Administraciones públicas pueden crear ficheros para el cumplimiento de sus fines.

El artículo 20.1 de la LOPDP dispone que tanto la creación de estos ficheros, como su modificación o supresión, solo pueden hacerse por medio de una disposición general publicada en el Boletín Oficial del Estado o en el Diario Oficial correspondiente.

Las disposiciones de creación o de modificación de ficheros deben tener el contenido que les exige el artículo 20.2 de la LOPDP e indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Además, en las disposiciones que se dicten para la supresión de los ficheros, ha de establecerse el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

4

La comunicación de datos entre las administraciones públicas.

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

4. LA COMUNICACIÓN DE DATOS ENTRE LAS ADMINISTRACIONES PÚBLICAS.

De todo lo anterior, se extraen las siguientes conclusiones:

Distinto del tratamiento de los datos de carácter personal, que es su recogida y explotación, es la cesión o comunicación de los datos a terceros.

El artículo 11 de la LOPDP establece el régimen general de las comunicaciones de los datos a terceros.

Pero, además, para el caso de las comunicaciones de datos entre Administraciones públicas, el artículo 21 establece unas reglas especiales.

A) Régimen general: principio del consentimiento previo y excepciones.

El régimen general parte del principio general de que los datos de carácter personal objeto del tratamiento solo pueden comunicarse a un tercero con el previo consentimiento del interesado y para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario (artículo 11.1 LOPDP).

Pero también la Ley establece excepciones al principio del consentimiento. Este no es preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso, la comunicación solo es legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el

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

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

g) Si la comunicación se efectúa previo procedimiento de disociación.

El consentimiento es:

- Nulo cuando la información que se facilita al interesado no le permita conocer la finalidad a que destinan los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

- Revocable, pero sin efectos retroactivos.

- Válido igualmente para el cesionario o persona o entidad a quien se le comuniquen los datos de carácter personal. Esta se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la LOPDP.

B) Régimen especial de comunicación de datos entre Administraciones públicas.

Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no se pueden comunicar a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas.

Este principio encuentra excepciones que permiten la comunicación sin el consentimiento del afectado cuando:

- Tal comunicación tiene por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

- Una Administración pública obtiene o elabora datos con destino a otra.

También prohíbe la Ley la comunicación de datos recogidos de fuentes accesibles al público a ficheros de titularidad privada sin el consentimiento del interesado o cuando una ley no lo prevea.

5

Ficheros de las fuerzas y cuerpos de seguridad.

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

5. FICHEROS DE LAS FUERZAS Y CUERPOS DE SEGURIDAD.

5.1. REGLAS GENERALES CONFORME A LA LOPDP.

Para que no haya ninguna duda sobre su aplicación, el artículo 22.1 de la LOPDP dispone que los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, están sujetos al régimen general de esa Ley.

Este artículo 21 y los artículos siguientes establecen reglas especiales aplicables a los ficheros de las fuerzas y cuerpos de seguridad:

a) La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad puede hacerse sin consentimiento de las personas afectadas solo en aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

No vulnera el derecho a la protección de datos el hecho de que las Fuerzas y Cuerpos de Seguridad hagan constar en sus informes determinados datos personales sin que hayan solicitado la previa autorización de las personas afectadas cuando tales datos han sido obtenidos de fuentes accesibles al público (como los Boletines Oficiales) y, menos aún, si los datos son de candidatos a un proceso electoral, ya que la adscripción política de un candidato es y debe ser un dato público en una sociedad democrática y, por ello, no puede reclamarse sobre ese dato ningún poder de disposición (SSTC 43/2009 y 44/2009, de 12 de febrero, con cita de otras).

b) Estos datos deben almacenarse en ficheros específicos establecidos al efecto, que deben clasificarse por categorías en función de su grado de fiabilidad.

c) La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos especialmente protegidos solo pueden realizarse ("exclusivamente", dispone el precepto) en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta. Lo aquí dispuesto no puede perjudicar el control de

legalidad de la actuación administrativa o la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

d) Los datos personales registrados con fines policiales han de cancelarse cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, han de considerarse especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

e) Los responsables de estos ficheros pueden denegar el acceso, la rectificación o cancelación en función de los peligros que puedan derivarse para:

- La defensa del Estado.

- La seguridad pública.

- La protección de los derechos y libertades de terceros, o

- Las necesidades de las investigaciones que se estén realizando.

Dicha denegación debe estar en todo caso motivada de forma suficiente. Como destaca la sentencia de 30 de junio de 2011, de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª):

"(…) no cabe duda que la autoridad administrativa podrá justificar adecuadamente las razones por las que se restringe o deniega el derecho de acceso solicitado, pero habrá de motivar y justificar esa cancelación sin que baste el mero silencio ni la utilización de fórmulas genéricas o esteriotipadas que no permitan apreciar las razones en las que se sustenta la limitación. Y este es el caso que nos ocupa en el que la falta de respuesta y, por lo tanto, la negativa a cancelar los datos personales obrantes en los ficheros policiales, (en todos los que se incorporaron datos), no se justificó en algunos de los supuestos antes mencionados, lo cual no satisface debidamente el derecho de cancelación.

Ha de concluirse, por tanto, que se ha vulnerado el derecho de cancelación del recurrente en relación con los datos personales obrantes en los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado que identificó y, en consecuencia procede reconocer su derecho a la cancelación pretendida en relación con los antecedentes policiales solicitados y respecto de todos los ficheros policiales en los que figuren tales antecedentes.

No procede acceder a la petición de indemnización de daños y perjuicios pues no ha resultado acreditado que la denegación de la tutela de su derecho le causara daños y perjuicios susceptibles de reparación, sin que baste la mera alegación de tales perjuicios carente de prueba alguna que los avale".

f) No es preciso informar a los interesados de que se están recogiendo datos personales suyos cuando la información afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales.

g) El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, rectificación o cancelación, puede ponerlo en conocimiento del Director

de la Agencia Española de Protección de Datos, quien debe asegurarse de la procedencia o improcedencia de la denegación.

Precisamente, una de las vías más eficaces de que disponen los ciudadanos para la protección de sus datos de carácter personal es, sin duda, la reclamación ante la AEPD. Esta vía se regula en los arts. 117 a 119 del Reglamento de la LOPDP, bajo la denominación de "procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición", que, a su vez, desarrollan el art. 18.3 de la LOPDP.

Se trata, por tanto, de un procedimiento administrativo singular, que se deja en manos únicamente de los titulares de los derechos de acceso, rectificación, cancelación y oposición, que, recordemos, son derechos personalísimos, por lo que solo pueden ser ejercidos por el afectado, directamente o mediante representante, y de ejercicio gratuito.

En síntesis, quienes consideren que uno de estos derechos ha sido vulnerado (el "afectado" o "afectados"), *pueden* acudir a la Agencia y presentar una reclama-

ción. Recibida la reclamación, la Agencia debe dar traslado de la misma al responsable del fichero, para que, en el plazo de quince días hábiles, formule las alegaciones que estime pertinentes. Recibidas las alegaciones o transcurrido el plazo dado, la Agencia, previos los informes, pruebas y otros actos de instrucción que considere necesario, incluida la audiencia del afectado y nuevamente del responsable del fichero, si así lo ve debido, ha de dictar su resolución sobre la reclamación.

El plazo máximo para dictar y notificar resolución en este procedimiento de tutela de derechos es de seis meses, que se cuenta desde la entrada en la Agencia de la reclamación. Si en ese plazo no se hubiese dictado y notificado resolución expresa (los dos actos), el afectado puede considerar estimada su reclamación por silencio administrativo positivo, con los efectos que de ello se derivan.

Cuando la resolución es estimatoria, la Agencia debe requerir al responsable del fichero para que, en el plazo de diez días siguientes a la notificación de la resolución, haga efectivo el ejercicio de los derechos tutelados, debiendo dar cuenta dicho responsable por escrito del cumplimiento a la Agencia en el plazo de diez días.

5.2. LA GRABACIÓN DE IMÁGENES POR LAS FUERZAS Y CUERPOS DE SEGURIDAD.

El artículo 22 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, faculta a la autoridad gubernativa y, en su caso, a las Fuerzas y Cuerpos de Seguridad para "proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia".

Dicha legislación vigente en la materia es la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad Ciudadana en lugares públicos.

Esta Ley Orgánica autoriza a las Fuerzas y Cuerpos de Seguridad la utilización de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

La captación, reproducción y tratamiento de las imágenes y sonidos no se consideran intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Para autorizar la instalación de videocámaras por la autoridad competente (el Consejero competente en el caso de la policía foral y de la policía local) se han de tener en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes.

También pueden autorizarse videocámaras móviles en las vías o lugares públicos donde se haya autorizado la instalación de videocámaras fijas, para su uso simultáneo, quedando, en todo caso, supeditada la toma, que ha de ser conjunta, de imagen y sonido, a la concurrencia de un peligro concreto. En los restantes lugares públicos pueden utilizarse videocámaras móviles, correspondiendo la autorización al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad.

En casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización en razón del momento de producción de los hechos o de las circunstancias concurrentes, se pueden obtener imágenes y sonidos con videocámaras móviles, dando cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión creada al efecto, la cual, si lo estima oportuno, puede requerir la entrega del soporte físico original y emitir el correspondiente informe. En el supuesto de que los informes de la Comisión sean negativos, la autoridad encargada de la custodia de la grabación ha de proceder a su destrucción inmediata.

Las autorizaciones de instalaciones fijas de videocámaras constituyen actividades de protección de la seguridad pública que no están sujetas al control preventivo de las Corporaciones locales previsto en su legislación reguladora básica, ni al ejercicio de las competencias de las diferentes Administraciones públicas.

Los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por las instalaciones, están obligados a facilitar y permitir su colocación y mantenimien-

to, sin perjuicio de la necesidad de obtener, en su caso, la autorización judicial y de las indemnizaciones que procedan según las leyes.

La utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad está presidida por los principios de:

a) Proporcionalidad, en su doble versión de idoneidad y de intervención mínima. La idoneidad determina que solo puede emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana. La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.

b) La existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles.

c) Inviolabilidad de domicilio. No se pueden utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento

del titular o autorización judicial, ni de los lugares públicos cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deben destruirse inmediatamente, por quien tenga la responsabilidad de su custodia.

En cuanto al tratamiento de las grabaciones, se rige en general por la LOPDP y por las siguientes reglas:

a) Las grabaciones deben ser destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

b) Están prohibidas la cesión o la copia de las imágenes y sonidos, salvo en los supuestos previstos en la letra anterior.

c) Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones debe observar

la debida reserva, confidencialidad y sigilo en relación con las mismas.

d) El público debe ser informado de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable.

Toda persona interesada puede ejercer los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura. No obstante, el ejercicio de estos derechos puede ser denegado por quien custodie las imágenes y sonidos, en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

5.3. LA DENOMINADA BASE DE DATOS POLICIAL SOBRE IDENTIFICADORES OBTENIDOS A PARTIR DEL ADN.

Esta base de datos **se regula en la Ley Orgánica 10/2007, de 8 de octubre**, la cual se inscribe, conforme a sus propias prescripciones, en el marco global de la LOPDP, resultando esta de aplicación directa y siendo los preceptos de la LO

10/2007 especificidades de la LOPDP (disposición adicional segunda).

Se trata de una **base de datos de titularidad de las Fuerzas y Cuerpos de Seguridad del Estado**, que depende del Ministerio de Interior.

Sirve para:

a) La investigación y averiguación de delitos.

b) La identificación de restos cadavéricos o la averiguación de personas desaparecidas.

La base de datos integra los ficheros de identificadores obtenidos a partir del ADN en el marco de una investigación criminal, que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo.

Se inscriben en la base:

- Los datos identificativos extraídos a partir del ADN de muestras o fluidos que, en el marco de una investigación criminal, hayan sido hallados u obtenidos a partir del aná-

lisis de las muestras biológicas del sospechoso, detenido o imputado, cuando se trate de delitos graves y, en todo caso, los delitos que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada.

- Los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de averiguación de personas desconocidas.

La **inscripción en esta base de datos no precisa el consentimiento del afectado**. No obstante, este debe ser informado por escrito de todos los derechos que le asisten respecto a la inclusión en la base, quedando constancia de ello en el procedimiento. También pueden inscribirse los datos identificativos obtenidos a partir del ADN cuando el afectado haya prestado expresamente su consentimiento.

Los datos contenidos en la base de datos **solo pueden utilizarse por las unidades de la Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado**. No obstante, los datos **pueden cederse** a:

a´) Las autoridades judiciales, fiscales o policiales de terceros países, de acuerdo con lo previsto en los convenios internacionales vigentes.

b´) Las policías autonómicas con competencia estatutaria para la protección de personas y bienes y para el mantenimiento de la seguridad pública, que únicamente pueden utilizar los datos para la investigación de los delitos o, en su caso, para la identificación de cadáveres o averiguación de personas desaparecidas; y

c´) El Centro Nacional de Inteligencia (CNI).

Todos los ficheros están sometidos al nivel de seguridad alto, de acuerdo con la LOPDP.

La conservación de los identificadores obtenidos a partir del ADN en la base de datos no puede superar el tiempo señalado en la Ley para la prescripción del delito, ni el tiempo señalado en la Ley para la cancelación de antecedentes penales, si se hubiese dictado sentencia condenatoria firma, o absolutoria por la concurrencia de causas eximentes por falta de imputabilidad o culpabilidad, salvo resolución judicial en contrario.

La cancelación procede cuando se haya dictado auto de sobreseimiento libre o sentencia absolutoria por causas distintas de las mencionadas en el punto anterior, una vez que sean firmes dichas resoluciones. En el caso de sospechosos no imputados, la cancelación de los identificadores inscritos se ha de producir transcurrido el tiempo señalado en la Ley para la prescripción del delito.

En los supuestos en que, en la base de datos existan diversas inscripciones de una misma persona, correspondientes a diversos delitos, los datos y patrones identificativos inscritos se han de mantener hasta que finalice el plazo de cancelación más amplio.

Los datos pertenecientes a personas fallecidas han de cancelarse una vez el encargado de la base de datos tenga conocimiento del fallecimiento.

El ejercicio de los derechos de acceso, rectificación y cancelación en relación con esta base de datos se sujeta a la LOPDP.

Por lo que respecta a la **toma de muestra y fluidos** del sospechoso, detenido o imputado, así como del lugar del delito, esta de hacerse por la policía judicial en el marco de la inves-

tigación de los delitos. En todo caso, la toma de muestras que requieran inspecciones, reconocimientos o intervenciones corporales, sin consentimiento del afectado, precisa autorización judicial mediante auto motivado (disposición adicional tercera).

Pamplona, 24 de abril de 2015

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa

Defensor del Pueblo
de Navarra
Nafarroako Arartekoa