EL USO Y LA PROTECCIÓN DE LOS DATOS PERSONALES

ESTHER MITJANS PERELLÓ
Directora de la Agencia Catalana de Protección de Datos

1. LA NORMATIVA: GARANTÍAS Y LÍMITES

El derecho a la protección de datos personales es transversal, es decir, está implicado en todas las actividades que llevan a cabo las administraciones públicas, en el sentido más amplio del término. En el ámbito de la investigación penal, podríamos decir que está presente de manera aun más intensa, porque toda investigación se basa en la recopilación de información y, en este caso, en recopilación de información relativa a personas.

La normativa de protección de datos establece una serie de garantías para el derecho a la protección de datos, que buscan, en último término, que la persona pueda controlar lo que los demás —entidades públicas y privadas— hacen con la información referente a su vida; en definitiva, establece obligaciones para los que tratan con datos personales. En el caso de las administraciones públicas, la normativa de protección de datos establece obligaciones, pero también un gran número de prerrogativas, para que puedan desarrollar sus funciones.

El derecho a la protección de datos es autónomo y es también un instrumento de garantía del resto de derechos y libertades fundamentales. Muchas veces se vincula a la intimidad, el honor y la propia imagen, pero debemos recordar que con el tratamiento de datos puede vulnerarse todo un conjunto de derechos: libertad sindical, libertad de circulación, presunción de inocencia...

Una parte importante de los límites al derecho a la protección de datos se basa, justamente, en la defensa del Estado, la seguridad pública, la protección de los derechos y las libertades de terceros, las necesidades de las investigaciones que se llevan a cabo o la persecución de infracciones penales.

En concreto, en la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos personales (LOPD), encontramos una regulación específica sobre el tratamiento de datos para las fuerzas y los cuerpos de seguridad.

Pero, antes entrar en esta regulación específica, creo importante identificar dos cuestiones: por un lado, qué es un dato de carácter personal; por otro lado, qué es un fichero y un tratamiento de datos personales.

En cuanto a la primera cuestión, aunque en un primer momento pueda parecer una obviedad, creo que no lo es tanto. Seguramente, todo el mundo tiene presente cuál es la definición de dato personal de la LOPD:

> ...cualquier información referente a personas físicas identificadas o identificables.

No hay que insistir, pues, en que la normativa de protección de datos solo protege a las personas físicas.

Pero quizá sí es importante detenerse un momento en qué quiere decir *identificables* e incorporar la definición que nos ha dado, en su artículo 5.1.*o)*, el Real decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de despliegue de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD):

> Persona identificable: cualquier persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considera identificable si dicha identificación requiere términos o actividades desproporcionados.

Habría que delimitar, por tanto, qué quiere decir *términos o actividades desproporcionados.* Y, en el caso de las fuerzas y cuerpos de seguridad, la delimitación de este concepto quizás ha de generar una atención especial, en vista de las posibilidades de recopilación de información de que disponen, no solo de ámbito nacional sino también internacional.

La segunda cuestión que quiero señalar es la definición de *fichero* y de *tratamiento* de la LOPD:

> Fichero: cualquier conjunto organizado de datos de carácter personal, sea cual sea la forma o la modalidad de creación, almacenaje, organización y acceso.
>
> Tratamiento de datos: las operaciones y los procedimientos técnicos de carácter automatizado o no, que permiten recoger, grabar, conservar, elaborar, modificar, bloquear y cancelar, así como las cesiones de datos que deriven de comunicaciones, consultas, interconexiones y transferencias.

Pero, aparte de la conceptualización, quiero recordar que cuando hablamos de *ficheros* hablamos tanto de ficheros manuales como de ficheros automatizados. Y que cuando nos referimos a *tratamiento*, hablamos de cualquier acción que hacemos con datos personales, aunque sólo sea reunirlos.

2. LA NORMATIVA DE PROTECCIÓN EN EL TRATAMIENTO DE DATOS EN LAS FUERZAS Y LOS CUERPOS DE SEGURIDAD

Hechas las apreciaciones anteriores, me centraré en las particularidades que podemos encontrar en la normativa de protección de datos respecto del tratamiento de datos por parte de las fuerzas y cuerpos de seguridad.

Ya en el momento de definir el ámbito de aplicación de la LOPD, se establece que los tratamientos de datos procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las fuerzas y los cuerpos de seguridad se rigen por sus disposiciones específicas, y por lo que prevea específicamente la LOPD. Per ayudar a la integración de las diferentes normas jurídicas, la Agencia publicó, en el año 2009, una Instrucción en esta materia con la que se pretende favorecer el cumplimiento de las obligaciones establecidas en la normativa de protección de datos. Esta Instrucción puede ser útil para todo lo que no esté regulado por la norma especial.

En cuanto al principio vertebrador del derecho a la protección de datos —el consentimiento—, también encontramos una serie de excepciones en relación a la necesidad o no de obtenerlo, cuando los datos son recogidos por las administraciones públicas en general y, particularmente, las fuerzas de seguridad.

Concretamente, el artículo 6 de la LOPD establece que las administraciones no han de obtener el consentimiento de las personas titulares de los datos, para su tratamiento, cuando sean necesarias para el ejercicio de sus funciones en el ámbito de sus competencias, ni cuando se refieran a las partes de una relación administrativa y sean necesarias para mantenerla o cumplirla.

Conviene añadir que tampoco haría falta el consentimiento cuando el tratamiento de los datos tenga como finalidad proteger un interés vital de la persona interesada.

Por otro lado, en el artículo 22 de la LOPD encontramos la regulación específica aplicable al tratamiento de datos por parte de las fuerzas de seguridad. En este caso, la normativa de protección de datos diferencia dos supuestos de tratamiento:

a) En primer lugar, los ficheros que contengan datos personales recogidos para finalidades administrativas. Estos ficheros están sujetos al régimen general de la normativa de protección de datos.

b) En segundo lugar, la recogida y el tratamiento de datos personales para finalidades policiales. Es en este segundo supuesto donde la LOPD establece una serie de requisitos para el tratamiento de los datos sin consentimiento de su titular, diferenciando el tratamiento de los datos especialmente protegidos (ideología, religión, creencias, afiliación sindical, salud, origen racial y vida sexual).

Cuando el tratamiento de los datos personales no se refiere a los especialmente protegidos, se permite la recogida y el tratamiento de los que sean estrictamente necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales. En estos casos, los datos tienen que

almacenarse en ficheros específicos establecidos a tal efecto y tienen que clasificarse por categorías en función del grado de fiabilidad.

Podemos observar que aparecen conceptos jurídicos indeterminados que dan un cierto margen de interpretación: «estrictamente necesarios», «peligro real»...

Pero también se prevé específicamente la excepción al consentimiento, cuando se trata de la recogida y el tratamiento de datos especialmente protegidos o sensibles. En este caso, pueden tratarse en los supuestos en que sea absolutamente necesario para las finalidades de una investigación concreta. Vemos que, también aquí, vuelven a utilizarse conceptos indeterminados como «absolutamente necesario».

3. PRINCIPIOS DE CUALIDAD DE LOS DATOS

Visto el amplio margen de interpretación, creo que es importante aplicar de manera rigurosa otros principios establecidos en la normativa de protección de datos. Hablo de los principios de cualidad de los datos, que pueden resumirse en:

— principio de finalidad
— principio de proporcionalidad
— principio de conservación
— principio de lealtad

Básicamente, se trataría de ser conscientes de que los datos sólo pueden ser recogidos y tratados cuando sean adecuados, pertinentes y no excesivos, en relación al ámbito y las finalidades determinadas, explícitas y legítimas para las que se han obtenido. Por tanto, hay que identificar con claridad las finalidades para las que se recogen los datos y no utilizarlos para finalidades diferentes.

Como este principio puede ser matizado en el ámbito de la investigación de delitos, hay que centrar la atención en el principio de proporcionalidad, en el sentido de pararnos a pensar cuáles son los datos que, efectivamente, son necesarios para la investigación que llevamos a cabo o para la prevención del peligro que queremos evitar. En definitiva, puede decirse que hay que utilizar siempre el mecanismo que sea menos intrusivo en los derechos de las personas.

No podemos olvidar que en los últimos tiempos se ha tendido a la recopilación masiva de información sin establecer, probablemente, unos criterios para intentar definir la información relevante para el caso concreto en que se está trabajando.

Otro de los principios de protección de datos se refiere a su exactitud; principio que, también en el ámbito que hoy tratamos, a veces se diluye un poco, pero que la misma LOPD ya ha previsto, al referirse a los términos de conservación de la información y a la manera de conservarla. Así, debemos tener presente que los datos personales registrados con finalidades policiales deben cancelarse cuando no sean necesarios para las investigaciones que hayan motivado la recogida. Para delimitar esta cuestión, hay que valorar especialmente:

— la edad de la persona afectada y el carácter de los datos almacenados,
— la necesidad de mantener los datos hasta concluir una investigación o un procedimiento concreto,
— la resolución judicial firme, especialmente la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Es importante tener presente que *cancelar* no quiere decir necesariamente suprimir la información, sino que el RLOPD nos indica que la cancelación es el procedimiento en virtud del cual el responsable cesa en el uso de los datos. Así, la cancelación implica el bloqueo: identificar y reservar los datos, con la finalidad de impedir el tratamiento, excepto para ponerlos a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y solo durante el plazo de prescripción de las responsabilidades nombradas.

Otro de los principios que definen el derecho a la protección de datos es el derecho de información en el momento de la recogida de los datos. Este derecho comporta la obligación de aquellos que tratan los datos personales de informar a la persona titular de cuáles serán las circunstancias del tratamiento (responsable del fichero, fichero donde se incorporarán los datos, finalidades y usos, obligación o no de facilitar los datos y lugar donde ejercer los derechos de acceso, rectificación y cancelación, entre otras cuestiones). En definitiva, información que permita a la persona titular de los datos saber qué se hará con ellos.

En el caso del derecho de información hay pocas excepciones, incluso para las administraciones públicas. No obstante, la LOPD también ha introducido alguna particularidad en este sector, indicando que el derecho de información en el momento de la recogida de los datos no es aplicable cuando el hecho de informar a la persona interesada afecte a la defensa nacional, la seguridad pública o la persecución de infracciones penales.

Otro de los ámbitos donde también se introducen excepciones es el ejercicio de los derechos de acceso, rectificación y cancelación. La LOPD establece que los responsables de ficheros con finalidades policiales pueden denegar el acceso, la rectificación o la cancelación en función de los peligros que puedan derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y las libertades de terceros o las necesidades de las investigaciones que se estén llevando a cabo.

4. LAS CESIONES DE DATOS

Uno de los campos donde surgen más problemáticas es el de las cesiones de datos. Hemos visto que, cuando se trata de recoger y tratar datos con finalidades policiales, no hace falta el consentimiento de la persona interesada; por tanto, es particularmente importante que el resto de principios se apliquen de manera rigurosa. Es necesario pues, que las fuerzas y cuerpos de seguridad formulen la petición de información personal de acuerdo con lo que disponen las leyes aplicables,

ya que se trata de supuestos de excepción donde decae el consentimiento previo del titular por atender otros intereses públicos; es el caso, por ejemplo, de la protección de la seguridad ciudadana.

Así, la Agencia, en la resolución de una consulta que se le formuló, ya indicó que, en términos generales, la Administración pública o el personal funcionario al cual se le requieren determinados datos de carácter personal puede solicitar, a los efectos de poder justificar la comunicación de los datos, una aclaración del motivo que fundamenta la petición de las fuerzas y cuerpos de seguridad. Eso, si aparentemente no se trata de ninguno de los supuestos habilitados o si no se deduce claramente que son datos necesarios para la prevención de un peligro real para la seguridad pública, o para la represión de infracciones penales, sin perjuicio de que corresponda a las fuerzas y cuerpos de seguridad la apreciación de los hechos o de las circunstancias de su actuación.

Asimismo, quiero recordar que la normativa de protección de datos establece otros supuestos que legitiman la cesión de datos sin el consentimiento previo de sus titulares. Por un lado, encontramos el artículo 11.2 de la LOPD, donde se establecen una serie de excepciones, de las cuales creo importante mencionar dos:

a) cuando la cesión está autorizada en una ley;
b) cuando la comunicación que se deba efectuar tenga como destinatario el Síndic de Greuges,[1] el Ministerio Fiscal, los jueces o tribunales o la Sindicatura de Cuentas, en el ejercicio de las funciones que tienen atribuidas.

Y, con respecto a las cesiones de datos entre administraciones públicas, el artículo 21 de la LOPD establece esta posibilidad, sin el consentimiento de su titular, cuando se comuniquen para el ejercicio de las mismas competencias o de competencias que traten las mismas materias.

5. EL PRINCIPIO DE SEGURIDAD

Finalmente, en cuanto a las obligaciones derivadas de la normativa de protección de datos, hay que recordar que los ficheros o tratamientos de datos han de cumplir con el principio de seguridad, es decir, prever aquellas medidas que eviten la alteración, la pérdida, el tratamiento o el acceso no autorizado. En el título VIII del RLOPD, encontramos el estándar mínimo de seguridad a aplicar en los ficheros automatizados y en los ficheros manuales. Concretamente, en la definición de los niveles de seguridad aplicables, el Reglamento establece que corresponde el nivel alto de seguridad a los ficheros o tratamientos de datos que:

1. Persona nombrada para la defensa de los derechos y libertades de la ciudadanía, en el ámbito de Cataluña, que se corresponde con la figura de defensor del pueblo.

a) se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual;
b) los que contengan datos derivados de actos de violencia de género;
c) y todos los que contengan o se refieran a datos obtenidos para fines policiales.

Por tanto, el nivel de seguridad a aplicar, por defecto, ha de ser el más elevado que se regula en el RLOPD.

En el ámbito de la seguridad pública, el derecho a la protección de datos personales está notablemente limitado y entra en conflicto constante con los intereses que se persiguen en materia de seguridad. Precisamente en este marco, como hemos visto, dos de los ejes principales del derecho a la protección de datos están muy restringidos: el derecho a la información en el momento de la recogida de los datos y el consentimiento para su tratamiento.

6. CONCLUSIÓN

La Agencia Catalana de Protección de Datos ya hace unos años que está trabajando en lo que llaman el modelo catalán de protección de datos, que ha permitido definir una serie de medidas que tienden a la prevención. Partiendo de la idea de que el derecho a la protección de datos es de difícil reparación una vez vulnerado, de lo que se trataría es de establecer mecanismos técnicos, organizativos y de procedimiento que garanticen el cumplimiento de los principios reguladores del derecho a la protección de datos y, a la vez, mejoren la gestión de la información y, por tanto, de las actuaciones que se lleven a cabo.

El derecho a la protección de datos no es sólo un conjunto de obligaciones para las entidades, sino que también puede ser un importante instrumento para generar la confianza de la ciudadanía. Eso puede reforzar el principio previsto en el artículo 104 de la Constitución, según el cual las fuerzas y cuerpos de seguridad tienen como misión proteger el libre ejercicio de los derechos y libertades, además de garantizar la seguridad ciudadana.

Esta confianza sólo puede crearse si diseñamos entornos colaborativos que tengan en cuenta la privacidad y la protección de datos personales, atendiendo a la especial relevancia que adquiere la seguridad de la información en el entorno analizado, ya que otros principios quedan muy limitados. También es importante un cambio de, podríamos decir, «conciencia» respecto al tratamiento de los datos personales, que pasa por la formación y la información de todos aquellos que han de gestionar datos personales para el desarrollo de sus funciones.

En definitiva, se trata de gestionar correctamente la información que estamos legitimados a tratar, sin olvidar que ningún derecho es absoluto pero que tampoco puede verse tan limitado que deje de tener virtualidad. Como en muchos otros ámbitos, tendremos que hacer un esfuerzo de ponderación.