PROTECCIÓN DE DATOS PERSONALES E INVESTIGACIÓN CRIMINAL

1. INTRODUCCIÓN:

Los diferentes cuerpos policiales, en el ejercicio de sus funciones, tratan una gran cantidad de información y diferentes tipos de datos. Cuando estos datos son considerados datos personales, las Fuerzas y Cuerpos de Seguridad, deben tener en cuenta las normas de Derecho Penal y de Enjuiciamiento Criminal aplicables en cada territorio o Estado y además la normativa reguladora del derecho a la protección de los datos personales.

En este trabajo se trata de analizar si la normativa de protección de los datos personales encaja de manera correcta con la función policial consistente en la prevención e investigación de delitos, es decir, si las medidas establecidas como garantía del derecho a la protección de los datos personales contribuyen a mejorar la función policial de investigación criminal o, si por el contrario, esta última normativa implica una merma o lacra para el ejercicio de esa función policial.

En este punto hay que señalar qué se entiende por investigación criminal y por datos personales a los efectos de esta presentación:

- bajo el término investigación criminal se hace referencia a la averiguación del delito ya cometido así como a la prevención del delito futuro. Es decir, esta expresión debe entenderse en un sentido amplio que abarque tanto la investigación criminal en sentido estricto como lo que se conoce como inteligencia criminal o información.
- por dato personal debe entenderse toda información relativa a una persona física determinada o determinable. Actualmente se interpreta el concepto de dato personal en una acepción muy amplia ya que comprende datos o informaciones que van más allá del nombre y apellidos de una persona física. Concretamente, se considera dato personal una dirección postal, un número de teléfono, la matrícula de un vehículo…

2. BREVE EXPOSICIÓN DE LOS PRINCIPIOS BASICOS DE LA NORMATIVA DE PROTECCIÓN DE LOS DATOS PERSONALES:

Conviene señalar que la normativa de protección de datos, en lo que se consideran sus bases fundamentales, es prácticamente la misma en todos los Estados Miembros de la Unión Europea, ya que se trata de leyes internas elaboradas para dar cumplimiento a normas europeas.

Concretamente, al Convenio 108 del Consejo de Europa para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal de 28 de Enero de 1981 y a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas con relación al tratamiento de los datos personales y a la libre circulación de estos datos.

La normativa de protección de datos tiene como finalidad garantizar el derecho fundamental a la privacidad de las personas frente al peligro que supone para este derecho la sociedad de la información, es decir, la posibilidad de acumular, tratar y ceder de forma masiva y con facilidad gran cantidad de datos personales.
Con este objetivo y, conforme a lo dispuesto en las dos normas comunitarias arriba indicadas, se instauran como bases ineludibles del derecho fundamental a la protección de los datos personales, los siguientes principios:

1- que no pueden recogerse o tratarse datos personales sin que exista el consentimiento inequívoco del afectado. Por afectado o interesado debe entenderse siempre el titular de los datos personales. Este es el que se conoce como **principio del consentimiento**. Este principio tiene excepciones, es decir, supuestos en que pueden recogerse y tratarse datos personales sin el consentimiento del titular de los mismos, como pueden ser los casos en que exista una ley que permita el tratamiento sin consentimiento, o cuando se recogen y tratan datos personales para el ejercicio de las competencias propias de las Administraciones Públicas etc..

2- que toda persona a la cual se le soliciten los datos personales debe ser informada previamente de la existencia del fichero, de su finalidad y de quien es el responsable del mismo. **Principio de información.**

3- que los datos personales sólo pueden ser recogidos y tratados para fines legítimos y específicos y, por lo tanto, no podrán ser utilizados para fines incompatibles con aquellos para los que fueron recogidos. Además, los datos personales tratados deben ser adecuados y no excesivos para la finalidad para la cual se recogieron. **Principio de calidad de los datos.**

4- los datos personales, una vez tratados, deben ser cancelados cuando ya no sean necesarios para la finalidad para la que se recogieron, es decir, que los datos personales no pueden conservarse más del tiempo estrictamente necesario. **Principio de conservación.**

5- toda persona física, nacional o no de un Estado miembro, como titular de sus datos personales, tiene la posibilidad de pedir el acceso a los mismos, es decir, tiene derecho a conocer qué datos se están tratando de él. Todo interesado puede pedir también la rectificación y cancelación de sus propios datos personales, así como oponerse a que sus datos sean tratados. Estos son los que se conocen como **derechos de acceso, rectificación, cancelación y oposición**. También conocidos como derechos ARCO.

6- que todo tratamiento de datos personales, automatizado o no, debe contar con las medidas de seguridad necesarias, tanto físicas como lógicas para impedir que puedan producirse accesos, alteraciones, cesiones o pérdidas de datos no autorizadas. Este es el que se conoce como **principio de seguridad de los datos.**

7- por último, la normativa de protección de datos prevé que, en cada Estado miembro, debe existir una **Autoridad de Control Independiente** encargada de supervisar el cumplimiento de todos estos principios. Cada Estado miembro ha determinado su propia Autoridad de Control como son, en España, al Agencia Española de Protección de Datos o las diferentes Agencias Autonómicas, la Comisión Nacional de Protección de Datos de Portugal, Garante italiano, la CNIL en el modelo francés etc…

Una vez analizados los pilares básicos de la protección de datos en toda Europa cabe preguntarnos: **¿Los diferentes cuerpos policiales, al realizar sus funciones de prevención e investigación del delito deben aplicar todos los principios mencionados de la normativa de protección de datos?**
¿Cuándo la policía investiga un delito y/o a una persona tiene sentido decir que el interesado debe ser informado de ese hecho y de que la policía debe obtener su consentimiento? ¿Tiene sentido decir que las personas pueden acceder, es decir conocer, los datos que la policía tiene de ellas cuando éstas están siendo investigadas por su relación con un delito? ¿Cuándo dejan de ser necesarios los datos personales relacionados con una investigación criminal? ¿Puede la policía utilizar los datos recogidos para una investigación policial para una investigación delictiva diferente?

Se trata en definitiva de analizar si la normativa de protección de datos personales debe aplicarse a rajatabla en el ámbito policial de la investigación criminal o si, por el contrario, deben existir importantes excepciones al régimen jurídico general.
Sobre este punto indicar que, **desde un principio**, **en el ámbito europeo**, se consideró que el tratamiento de datos personales por parte de policía implicaba la existencia de **un régimen excepcional, como así se recogía ya en el artículo 9.2. del Convenio 108 del Consejo de Europa indicado anteriormente**.

3. EVOLUCIÓN DE LA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS EN MATERIA POLICIAL:

La Unión Europea tiene, entre sus objetivos, la creación de un espacio común de Libertad, Seguridad y Justicia. Este espacio es el que se conoce como III Pilar de la Unión y es en este ámbito en el que se mueve la cooperación policial entre los diferentes Estados Miembros. Por lo tanto, es en el III Pilar en el que se produce el intercambio de información entre cuerpos policiales y la cesión de datos personales con fines de prevención e investigación criminal.

En los últimos años ha ido incrementando la necesidad de cooperación policial con otros Estados al entenderse que es un instrumento indispensable para poder luchar de forma eficaz contra el terrorismo y la delincuencia organizada.

3.1. En el III Pilar cada Estado tiene su propio Derecho Penal y sus propias leyes de enjuiciamiento criminal.
Sin embargo, en cuanto a normativa de protección de datos, sí que existe un sustrato jurídico común que son, desde sus inicios hasta hoy en día, el Convenio 108 del Consejo de Europa de 28 de Enero de 1981 ya ciado y la Recomendación (87)15 del Consejo de Europa de 17 de septiembre de 1987 sobre el Uso de Datos Personales en el Sector Policial:

- Se trata de normas que son aplicables a cualquier tratamiento de datos personales, por lo tanto, también a datos policiales y a todos los que constituyen materia del III Pilar. Aunque son normas del Consejo de Europa son aplicables a todos los Estados Miembros de la Unión porque todos ellos son también miembros del Consejo de Europa. Y además, esas normas han sido incorporadas a los Estados de la Unión Europea porque a ellas se remiten, como condición necesaria, los Convenios de Schengen y Europol.

- Son normas muy genéricas, que se refieren sólo a los datos personales que sean objeto de tratamiento automatizado y no regulan la cesión a terceros Estados o Instituciones.

- El Convenio se limita a establecer que tiene un régimen excepcional el tratamiento de datos personales cuando sea necesario en una sociedad democrática para garantizar la seguridad pública o para la represión de infracciones penales.

- La Recomendación (87) 15 es la que detalla ese régimen excepcional de los datos policiales que, básicamente, supone:

    a) Se refiere a los datos con finalidad policial entendiendo por tales los que sean necesarios para prevenir un peligro real para la seguridad pública o para la represión de infracciones penales. En este caso se pueden recoger y tratar datos personales sin el consentimiento de los afectados. Sin embargo, reconoce el derecho de información siempre que no perjudique las actividades de investigación que lleve a cabo la policía.
    b) Que debe existir una Autoridad de Control independiente que supervisará el tratamiento de los datos personales por parte de los cuerpos policiales y a la que se notificarán los ficheros que utilice la policía.
    c) Establece la obligación de que la información policial se almacene según su grado de fiabilidad o exactitud, concretamente, debe diferenciarse la información basada en hechos de la basada en opiniones personales. Debe distinguirse entre los datos con finalidad administrativa y los datos con finalidad policial.

d) regula de manera amplia la cesión de datos y, además, la admite en muchos supuestos diferentes, tanto a nivel nacional como internacional.
e) Recoge el principio de finalidad, es decir, que la policía sólo puede usar los datos para la finalidad para la que fueron recogidos salvo que sea necesario para una investigación concreta y hay autorización de la Autoridad de Control o una previsión legal que lo autorice.
f) Reconoce los derechos de acceso, rectificación y cancelación. Estos pueden ser denegados si es indispensable para la ejecución de las tareas policiales o si es necesario para la protección del afectado o de terceros.
g) Necesidad de revisión periódica de la información para decidir si su mantenimiento sigue siendo necesario para la finalidad que motivó su recogida. Parte de la idea de la necesidad de establecer intervalos de tiempo tras los cuales es necesario revisar esa necesidad.
h) Que deben adoptarse las medidas de seguridad necesarias, tanto lógicas como físicas.

3.2. La década de los 90 se caracteriza por la implantación, en materia de cooperación entre las diferentes policías europeas, de dos Convenios Internacionales con sus respectivos sistemas de información y que facilitan el intercambio de información policial: el Convenio Schengen y el Convenio Europol.
Ambos Convenios se remiten en materia de protección de datos al Convenio 108 y a la Recomendación (87) 15 antes indicadas.

3.3. Las Decisiones del Siglo XXI se caracterizan porque tienen como objetivo incrementar la cooperación policial y el intercambio de información entre los diferentes Estados europeos:

La Decisión 2007/533 JAI por la que se regulan aspectos policiales y se crea el denominado SIS II (agrupa a 31 Estados europeos aunque cuatro de ellos no son parte de la Unión Europea)**.** Este sistema supone un gran avance en determinados aspectos pero aún no ha entrado en vigor. Se prevé su puesta en funcionamiento en el año 2012.

SIS II amplia el ámbito de aplicación del Convenio anterior al hacer hincapié en su finalidad de garantizar la seguridad pública en la Unión Europea y en el territorio de sus Estados Miembros y, además, incorpora el intercambio de información complementaria para la cooperación policial y judicial en materia penal. Es decir, pasa de ser un sistema basado en asegurar la libre circulación de personas para convertirlo en un sistema de soporte a la investigación criminal en general.
Incorporará sistemas de enlace con otras informaciones de SIS II, hecho que refuerza la tesis de su mayor aproximación a un sistema de investigación policial.

El régimen de protección de datos personales sigue siendo el del Convenio 108 y la Recomendación (87) 15 porque la Decisión Marco 2008/977/JAI, del 27 de Noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial, finalmente, sólo es aplicable a los intercambios de datos entre Estados Miembros. Schengen y Europol quedan excluidos de su ámbito de aplicación.

La Decisión 2009/371/JAI, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía, que ha entrado en vigor el 1 de Enero de 2010 y que viene a sustituir al Convenio Europol. Esta Decisión supone integrar Europol en el entramado institucional europeo, aunque sigue sin atribuir funciones ejecutivas a sus agentes.

Tiene como finalidad incrementar la cooperación policial entre los Estados miembros a través de los Equipos Conjuntos de Investigación y la mejora del acceso a la información. Simplifica el procedimiento para ampliar la lista de los delitos para los que Europol es competente y, en cuanto al régimen aplicable en materia de protección de datos, sigue siendo el acervo del Consejo de Europa, o sea, el Convenio 108 y la Recomendación (87) 15.

El principio de disponibilidad:

El **Programa de la Haya de 2004** recogió, entre sus conclusiones, que para mejorar la lucha contra el terrorismo y la delincuencia organizada debía ponerse en marcha el llamado principio de disponibilidad y que quiere decir que todo funcionario de policía que necesite información para el cumplimiento de sus obligaciones en el territorio de la Unión Europea podrá obtenerla de otro Estado Miembro. Es decir, se prevé el **intercambio directo de información entre Estados Miembros y que éstos tienen la obligación de compartirla o entregarla al Estado que se la solicite.**

Un claro ejemplo de este principio es la **Decisión Marco 2006/960/JAI de 18 de Diciembre de 2006 sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados Miembros de la Unión Europea.**

Esta Decisión Marco ha sido incorporada al derecho español mediante la reciente Ley 31/2010 de 27 de julio y su complementaria Ley Orgánica 6/2010, también de 27 de julio.

En materia de protección de datos la Decisión Marco se acaba remitiendo también al Convenio 108 y a la Recomendación (87) 15, a pesar de que las Autoridades europeas de protección de datos proclamaban que le fuese de aplicación el régimen previsto en la Decisión Marco 2008/977/JAI relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

En este sentido, debe indicarse que la **Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008,** antes mencionada debía sustituir a la Recomendación (87)15 y supondría una mayor concreción y actualización de la protección de datos en el ámbito policial.
Esta Decisión debía ser el mecanismo de unificación de la protección de datos en el III Pilar al ser de aplicación al tratamiento de la información policial por parte de cada Estado Miembro, también debía aplicarse al intercambio de información entre Estados Miembros y entre éstos y terceros u otras instituciones.

Sin embargo, la Decisión Marco 2008/977 ha sido aprobada con un ámbito de aplicación muy reducido porque sólo es aplicable a los intercambios de información policial entre Estados Miembros, siempre que no se intercambien a través de SIS o Europol ni se trate de intercambio de inteligencia criminal, y también se aplica a las transferencias a terceros Estados o a organismos internacionales cuando la información ha sido recibida de otro Estado miembro (no cuando haya sido generada por el propio Estado que realiza la transferencia internacional).

Por lo tanto, la trascendencia y aplicación de este Decisión Marco dependerá de si los Estados Miembros, en la transposición de esta norma, deciden acatar sus preceptos de forma voluntaria para su ordenamiento interno o si se limitan a transponerla para el ámbito de intercambio de información entre Estados Miembros.

CONCLUSIÓN: en los últimos años, en el ámbito europeo, se han establecido mecanismos que facilitan el intercambio de información policial con el objetivo de conseguir una mayor eficacia en la lucha contra el crimen, sin embargo, estos mecanismos no han ido acompañados, de forma paralela, de nuevos instrumentos de protección de datos personales que garanticen que ese intercambio de información policial se realiza con pleno respeto a la privacidad de las personas.
Es decir, se ha producido una evolución para incrementar la eficacia policial pero no ha evolucionado ni incrementado de igual manera la protección de los datos personales que son tratados por los diferentes cuerpos policiales europeos.

4. EL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES EN EL DERECHO ESPAÑOL:

Los ficheros de las Fuerzas y Cuerpos de Seguridad tienen su brevísima regulación en el artículo 22 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de Diciembre (en adelante LOPD).

Este precepto regula el régimen de los ficheros policiales, estableciendo una diferenciación en función de si éstos tienen una finalidad administrativa o policial. Es decir, cuando los ficheros tengan finalidad administrativa, van a seguir el régimen ordinario previsto por la LOPD para los tratamientos de datos personales realizados por la administración pública; por el contrario, los ficheros con finalidad policial, van a tener un régimen especial, desde el punto de vista de protección de datos.

La distinción entre una u otra categoría no resulta, por lo tanto, una cuestión baladí, ya que de ella depende el régimen legal que tendrán dichos ficheros.

A pesar de la importancia de este tema, ni la normativa reguladora de protección de datos, ni la normativa policial de carácter sustantivo, ni los debates parlamentarios que se suscitaron durante la tramitación de la LORTAD y de la LOPD, dan una definición o concepto de lo que debe entenderse por finalidad administrativa y finalidad policial a efectos de la normativa reguladora de protección de datos. [1]

[1] Diario de Sesiones del Congreso de los Diputados. Pleno y Diputación Permanente. Año 1991. IV legislatura. Núm. 151.

Tampoco ofrecen una definición sobre qué debe entenderse por ficheros de las Fuerzas y Cuerpos de Seguridad. Una definición posible sería la de entender el fichero policial como aquel conjunto organizado de datos, automatizado o manual, creado para dar apoyo a la gestión, organización o actividad de las Fuerzas y Cuerpos de Seguridad, a fin de que puedan ejercer las competencias y funciones que legalmente tienen encomendadas.

Por último, debe tenerse en cuenta que la propia LOPD prevé unas especificidades en relación con determinados ficheros de las Fuerzas y Cuerpos de Seguridad:

- Los ficheros dedicados a la investigación del terrorismo y formas graves de delincuencia organizada se encuentran excluidos del ámbito de aplicación de la LOPD con una salvedad, ya que previamente a su creación deberá comunicarse su existencia, características generales y finalidad a la Autoridad de control competente (art. 2.2.c) de la LOPD).

- Los ficheros procedentes de imágenes y sonidos obtenidos mediante videocámaras por las Fuerzas y Cuerpos de Seguridad se regularán por su normativa específica, así como por las previsiones que la LOPD efectúe cuando así proceda (art. 2.3.e) de la LOPD).

Diario de Sesiones del Congreso de los Diputados. Comisiones. Año 1992. IV legislatura. Núm. 425.
Diario de Sesiones del Senado. Año 1992. IV legislatura. Núm. 129
Diario de Sesiones del Congreso de los Diputados. Comisiones. Año 1999. VI legislatura. Núm. 744.