LA REGULACIÓN DE LOS FICHEROS POLICIALES EN ESPAÑA Y SU TRATAMIENTO EN LA CONVENCIÓN DE PRÜM. LA PERSPECTIVA DE LAS AUTORIDADES NACIONALES DE PROTECCIÓN DE DATOS

Esperanza Zambrano Gómez*

SUMARIO

1. EL RÉGIMEN DE PROTECCIÓN DE DATOS DE LOS FICHEROS DE CARÁCTER POLICIAL

El tratamiento de la información es una herramienta fundamental en el desarrollo de la labor de protección de la seguridad pública que llevan a cabo las Fuerzas y Cuerpos de Seguridad. Esta es una afirmación indiscutible que, no obstante, debe ser objeto de matizaciones en lo que al tratamiento de dicha información se refiere. Y ello por cuanto ese tratamiento supone, en última instancia, una incidencia en el derecho fundamental a la protección de datos de carácter personal de los ciudadanos.

Precisamente para evitar que la salvaguardia de la seguridad pública signifique una excesiva intromisión en el derecho del ciudadano a la protección de sus datos, el tratamiento de los ficheros en manos de las Fuerzas y Cuerpos de Seguridad está necesariamente sometido a una serie de disposiciones que, a la vez que tienen en cuenta las especiales caracterís-

* Asesora. Área Internacional. Agencia Española de Protección de Datos.

ticas de la labor de las fuerzas de orden público, regulan las garantías que se deben adoptar.

La Ley Orgánica 2/1986 regula las características y funciones de las Fuerzas y Cuerpos de Seguridad, entendiéndose en España como tales:

a) Las Fuerzas y Cuerpos de Seguridad del Estado dependientes del Gobierno de la Nación. Cuerpo Nacional de Policía y Guardia Civil.

b) Los Cuerpos de Policía dependientes de las Comunidades Autónomas. Mossos d´Esquadra (Cataluña), Ertaintza (País Vasco) y Policía Foral en Navarra.

c) Los Cuerpos de Policía dependientes de las Corporaciones Locales.

Desde el punto de vista competencial, y como consecuencia de la previsión contenida en la LOPD[1], cabe señalar que actualmente existen en España tres Agencias Autonómicas de Protección de Datos – en la Comunidad de Madrid, País Vasco y Cataluña - cuyas competencias se centran en los ficheros creados por los poderes públicos radicados en su ámbito territorial. Es por ello que todo lo expuesto a continuación deberá ser entendido desde la perspectiva de que estas tres Agencias serán responsables de los ficheros creados por las policías locales dentro de su ámbito territorial y que la Agencia del País Vasco y de Cataluña serán responsables de los ficheros de los que sean titulares la Ertaintza y los Mossos d´esquadra respectivamente.

La regulación específica de los ficheros de carácter policial comienza en 1987[2], con la aprobación por el Consejo de Europa de la Recomendación nº 15[3] por la que se regula el uso de los datos personales en el sector policial. Aunque en principio estaba dirigida al tratamiento automatizado de datos personales con fines policiales, esta Recomendación también podría extenderse a tratamientos no automatizados e incluso ser objeto de un desarrollo más amplio si el Estado signatario así lo decidía. Es importante señalar, asimismo, que supuso un punto de partida esencial a la hora de regular el tratamiento de los datos personales realizados por el sector policial, y ello mediante la indicación de los principios claves que debían ser observados en dicho tratamiento:

1. Control y notificación. La existencia de estos ficheros debe ser notificada a una autoridad no policial de control que tenga carácter independiente.

---

[1] Artículo 41 LO 15/1999 de protección de datos de carácter personal.

[2] El 17 de septiembre de 1987.

[3] Disponible en el siguiente enlace: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international_legal_instruments/Rec(87)15_EN.pdf

2. La recogida de los datos debe limitarse a aquellos casos en que sea necesario para la prevención de un peligro real o para la represión de un delito.

3. Los datos deben ser actualizados y almacenados el tiempo estrictamente necesario para permitir a la policía ejercer sus funciones. Asimismo, los datos basados en hechos deben diferenciarse de aquellos basados en opiniones o valoraciones, al igual que los datos recogidos por las Fuerzas y Cuerpos de Seguridad con fines administrativos deben almacenarse separadamente de aquellos que sean recabados con fines policiales.

4. El uso de los datos por la policía se rige por el principio de que los datos recogidos con fines policiales sólo deben usarse para la finalidad para la que fueron recabados.

5. La comunicación de los datos a otros cuerpos policiales nacionales debe limitarse a aquellos casos en que exista un interés legítimo. Otro tipo de transmisiones han de verse amparadas en una habilitación legal o en una autorización, y el tratamiento posterior debe ser compatible con aquél para el que fueron recabados los datos. Las únicas excepciones a estos requisitos serán cuando la transmisión sea en interés del titular de los datos o sea necesario para prevenir un peligro grave e inminente.

6. Publicidad, derecho de acceso a los ficheros policiales, derecho a la rectificación y al recurso. Los ficheros que se han notificado a la autoridad de control han de ser públicos y se le garantiza al titular de los datos el derecho de acceso a la información que, sobre él, contienen los ficheros policiales. El ejercicio del derecho de acceso, de rectificación de datos erróneos o la eliminación de los datos innecesarios está limitado, no obstante y por cuestiones obvias derivadas de las especificidades de la acción policial, a los casos en que no suponga una incidencia en la labor de la policía o no afecte a la protección de los derechos del titular de los datos o de terceros.

7. Los datos deberán eliminarse cuando no sean necesarios para el cumplimiento de la finalidad para la que fueron recogidos.

8. Por último, debe prevenirse el acceso, la comunicación o la alteración no autorizados a través de la adopción de medidas de seguridad por el responsable de los datos.

La Recomendación ha sido objeto de tres evaluaciones[4], la última de ellas en 2002, con vistas a analizar la vigencia de los principios en ella

[4] Se puede acceder a las evaluaciones en el siguiente link: http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/international_legal_instruments/2Recommendations%20and%20resolutions%20of%20the%20Committee%20of%20Ministers.asp#TopOfPage

contenidos y, en su caso, la conveniencia de actualizarla. En todas estas evaluaciones se concluyó que los principios de la Recomendación 87(15) continúan siendo la referencia en la regulación de los ficheros de carácter policial, proporcionando la base para las normativas nacionales en la materia y guiando el tratamiento de los datos personales en dicho ámbito de actividad.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[5] (LOPD) regula en sus artículos 22 a 24 este tipo de ficheros. De este articulado se desprende hacer, con carácter previo, dos precisiones:

En primer lugar, y siguiendo con la diferenciación establecida en la ya mencionada Recomendación 87 (15) del Consejo de Europa, la Ley española diferencia los tratamientos llevados a cabo por las Fuerzas y Cuerpos de Seguridad atendiendo a la finalidad de los mismos, para lo que distingue entre tratamientos efectuados con fines administrativos y tratamientos de datos con fines de investigación policial.

En efecto, todos sabemos que las Fuerzas y Cuerpos de Seguridad realizan también funciones de carácter puramente administrativo: la expedición del documento nacional de identidad o de los pasaportes, el control de entrada y salida en el territorio nacional (cuando no supone un control de las redes de inmigración ilegal), los ficheros de registros de extranjeros en territorio español o la vigilancia del cumplimiento de las normas de tráfico y seguridad vial. Respecto de los tratamientos de datos vinculados a estas actividades, la Ley española dispone terminantemente que estén sujetos al régimen general de la LOPD. En consecuencia, los principios generales de protección de datos aplicables a todos los tratamientos realizados en España son de plena aplicación a los ficheros de carácter administrativo creados por las Fuerzas y Cuerpos de Seguridad.

Esta circunstancia es reflejo de lo dispuesto en la Directiva 95/46/CE[6],- de la que es implementación nuestra LOPD- que, en su artículo 13, establece determinadas excepciones a su ámbito de aplicación respecto de las materias encuadradas en el denominado Tercer Pilar de la Unión Europea (cooperación policial y judicial en materia penal), pero no en lo referente a

[5] La predecesora de la LOPD, la Ley Orgánica 5/1992 de regulación de los Tratamientos Automatizados de Datos de Carácter Personal (LORTAD) también establecía normas específicas relacionadas con los ficheros policiales.

[6] Directiva de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

las restantes actividades que puedan llevar a cabo las fuerzas del orden público.

En segundo lugar, y ya respecto de los ficheros que hemos denominado policiales, la Ley española de protección de datos establece una excepción dentro de su ámbito de aplicación al indicar[7] que el régimen general de protección de datos de carácter personal no será de aplicación a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Sin embargo, esta excepción no implica la absoluta desvinculación de dichos ficheros al cumplimiento de las normas de protección de datos por un lado, y a la intervención de la Agencia Española de Protección de Datos como autoridad de control en la materia, por otro, y ello por cuanto el propio precepto establece la obligatoria comunicación de la existencia de este tipo de ficheros, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Respecto de los ficheros constituidos para llevar a cabo investigaciones concretas con vistas a la represión de infracciones penales o para la prevención de un peligro real para la seguridad pública, ficheros «policiales» o «de investigación», es importante señalar que sus especiales características determinan, en cierta manera, su regulación. En efecto, las condiciones en que se llevan a cabo dichos tratamientos- van referidos a personas concretas sometidas a investigación, pueden tener un gran impacto en el titular de los datos y el tratamiento es normalmente desconocido por el sujeto - son tenidas en cuenta, aplicándose un régimen especial que incluye excepciones a las reglas previstas en la legislación general en materia de protección de datos, pero que también impone sobre dichos tratamientos la aplicación de garantías más severas.

Estas previsiones aparecen recogidas esencialmente en los apartados 2 a 4 del artículo 22, el artículo 23.1 y el artículo 24 de la Ley Orgánica, de los que se desprende lo siguiente:

1. Limitación objetiva: el tratamiento debe limitarse a aquellos supuestos y categorías de datos necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2. Los datos se incluirán en ficheros específicos que serán clasificados por categorías en función de su grado de fiabilidad. Estos datos serán cancelados cuando no sean necesarios para los fines para los que fueron almacenados.

---

[7] Artículo 2.2 c) LOPD.

3. Principio de proporcionalidad y tratamiento de los datos sensibles: los datos calificados como especialmente protegidos, es decir, aquellos que revelen la «ideología», «afiliación sindical», «religión», «origen racial o étnico», «salud» o «vida sexual»[8] sólo podrán recabarse y tratarse en aquellos casos en que sea absolutamente necesario para los fines de una investigación concreta.

4. Derechos de acceso, rectificación y cancelación: como ya hemos tenido ocasión de mencionar, las especiales características de este tratamiento hace necesario el establecimiento de ciertos límites a los derechos del titular de los datos. En efecto, carecería de sentido informar a un presunto delincuente de que está siendo investigado, puesto que ello podría implicar su evasión de la justicia o la ocultación de pruebas necesarias para la adecuada investigación policial. Es por ello que la LOPD establece que el acceso, la rectificación o la cancelación podrán denegarse «en función de los peligros que puedan derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros, o las necesidades de las investigaciones que se estén realizando». Estos límites no suponen, sin embargo, la indefensión del interesado, puesto que, en último término, podrá dirigirse a la Agencia Española de Protección de Datos, o al organismo competente en cada Comunidad Autónoma, que analizará la procedencia o no de la limitación de estos derechos. También es objeto de limitación el denominado derecho de información, por el cual toda persona a la que se solicite información puede conocer acerca del eventual tratamiento previsto para sus datos, las condiciones en las que se llevaría a cabo y los derechos que le asisten. Este derecho podrá limitarse, igualmente, cuando su ejercicio afecte a la Defensa Nacional, la seguridad pública o la persecución de infracciones penales[9].

5. Medidas de seguridad. Por último, como garantía adicional de la existencia de tratamientos o accesos no deseados a los datos contenidos en los ficheros de investigación policial, la legislación española exige la imposición sobre los mencionados ficheros de medidas de seguridad de nivel alto, y, por tanto, de mayor rigor a las impuestas a la generalidad de

[8] Artículo 7 LOPD.

[9] En relación con el alcance del mencionado derecho, es opinión de la AEPD que la verificación de la información se referirá a los extremos planteados por el interesado, si bien la respuesta que se dé al mismo se limitaría, en principio, a indicar que se ha llevado a cabo la verificación y que el tratamiento que se ha realizado es conforme a la Ley, en su caso, puesto que una respuesta más amplia podría dar lugar a resultados no pretendidos por la norma.

los tratamientos de datos de carácter personal[10]. Estas medidas de seguridad de nivel alto se caracterizan, además de por exigir la elaboración de un documento de seguridad, de establecer mecanismos para la identificación y autenticación del acceso, realizar auditorias periódicas o llevar un registro de incidencias, por exigir el cifrado de los datos en caso de que sean transmitidos así como un registro de los accesos que deberá conservarse como mínimo dos años.

Debe también mencionarse que, al tratarse de ficheros en manos de una Administración Pública, los creados por la policía deben ser objeto de una disposición general- normalmente una orden ministerial- publicada en el Boletín Oficial del Estado[11].

En los últimos tiempos, diversas propuestas que afectaban a este tipo de información han sido sometidas a la consideración de la Agencia Española de Protección de Datos.

En primer lugar, como hemos visto, la Ley precisa la existencia real de un peligro para la seguridad pública que justifique el tratamiento de los datos o que el mismo sea llevado a cabo en relación con la investigación de un delito ya cometido. No obstante, en España se ha planteado la posibilidad de que las Fuerzas y Cuerpos de Seguridad puedan efectuar tratamientos de meros sospechosos de la comisión de delitos. En efecto, en 1998 fue presentada en el Congreso de los Diputados una proposición no de Ley[12] por la que se solicitaba la introducción en el ordenamiento español de la posibilidad de recabar información genética de individuos sospechosos que tuvieran una vinculación específica con el delito que fuese objeto de investigación. En 2003, la reforma de la Ley de Enjuiciamiento Criminal[13] añadió un párrafo por el cual se habilitaba al Juez de Instrucción, «siempre

---

[10] Artículo 4.3 del Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio. «*Los ficheros que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto*».

[11] Artículo 20 LOPD.

[12] Diario de Sesiones nº 172 de 23 de junio de 1998. Proposición no de Ley del Grupo Parlamentario Popular en el Congreso *por la que se insta al Gobierno a que introduzca en nuestro ordenamiento jurídico la regulación sobre el uso del análisis de ADN dentro de la estructura del derecho penal y en la investigación de la paternidad.*

[13] Ley Orgánica 15/2003 de 25 de noviembre. Artículo 363: «*siempre que concurran acreditadas razones que lo justifiquen el Juez de Instrucción podrá acordar, en resolución motivada, la obtención de muestras biológicas del sospechoso que resulten indispensables para la determinación de su perfil de ADN. A tal fin, podrán decidir la práctica de aquellos actos de inspección, reconocimiento o intervención que resulten adecuados a los principios de proporcionalidad y razonabilidad».*

que concurran acreditadas razones que lo justifiquen» a solicitar muestras biológicas del sospechoso con vistas a la determinación de su perfil de ADN.

Tras la reforma, en España este tipo de tratamiento de datos de ADN sólo se puede realizar respecto a restos encontrados en el lugar en que se haya producido el hecho delictivo y siempre que se haya obtenido el consentimiento del interesado o en virtud de resolución judicial por la que se acuerde la obtención de muestras de un determinado sospechoso.

Por otro lado, un ejemplo de la aplicación de la garantía que supone el principio de proporcionalidad lo supuso el informe emitido por la Agencia Española de Protección de Datos respecto de la reforma prevista de la Ley de Extranjería por la que se pretendía el tratamiento de datos de carácter personal con la finalidad de control de las redes de inmigración ilegal. La reforma inicial preveía el suministro de toda información referente a los pasajeros que, como destino final o de tránsito, se dirigieran a España, incluyendo los datos de aquellos extranjeros que no hicieran uso de su billete de regreso. A estos últimos se les presuponía que habrían permanecido en España en situación ilegal o que iban a permanecer por un período de tiempo superior a los 90 días de vigencia del visado turístico.

En este caso concreto, el tratamiento de los datos de extranjeros que se encontrasen en dicha situación sólo podría quedar exceptuado del régimen general, especialmente en lo referente al deber de información, al ejercicio de los derechos por parte de los afectados, y a la necesidad de recabar el consentimiento para la cesión de los datos a las Fuerzas y Cuerpos de Seguridad en caso de que el tratamiento fuese previsto para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales[14].

En su informe, la Agencia concluyó que la reforma prevista podría vulnerar el principio de proporcionalidad, dado que la cantidad de datos solicitados resultaba excesiva para la persecución de las redes de inmigración ilegal, así como que la recogida de datos con independencia del país de nacionalidad y de origen no garantizaba, en último término, una adecuada vigilancia y control de las redes de inmigración ilegal, de las que se saben que proceden de países determinados. Finalmente, el proyecto presentado y aprobado estableció que los datos a recabar se limitarían al número de personas extranjeras que no hicieran uso de su billete de vuelta, y del vuelo de origen. Con esta información, ya en casos concretos, y ante la evidencia

[14] En los términos del artículo 22.2 de la LOPD.

de un elevado número de personas procedentes de determinados orígenes que permanecieran en territorio español sin hacer uso de su billete de vuelta, se procedería a informar a las autoridades policiales. Esta información se realizaría previo requerimiento concreto y estaría limitada a los datos correspondientes a personas determinadas[15].

Finalmente, resulta interesante ilustrar con otro ejemplo la aplicación del principio de finalidad en el uso de los datos. La AEPD ha recibido en ocasiones consultas respecto de la compatibilidad del acceso generalizado de las Fuerzas de Seguridad al padrón municipal con la legislación de protección de datos personales. El criterio de la Agencia Española de Protección de datos ha sido en estos casos que la cesión quedará limitada al nombre y domicilio de la persona y exclusivamente para las finalidades previstas para el propio Padrón Municipal, es decir, la prueba de la residencia en el municipio y del domicilio habitual en el mismo.

Asimismo, también existen normas a nivel interno con las que la Dirección General de la Policía ha querido completar las disposiciones reguladoras de los datos personales en su ámbito de actividad. La Resolución de 30 de junio de 1995, de la Dirección General de la Policía, por la que se dictan instrucciones sobre determinados aspectos de los ficheros policiales de datos de carácter personal es un ejemplo de ello. Su importancia es enorme, entre otras cosa porque, en cierta medida, aclara los principios contenidos en la propia legislación general de protección de datos[16].

Dentro del contenido de la Resolución, resultan especialmente relevantes los apartados referidos a la delimitación de los tipos de ficheros policiales, la cancelación de los datos y la adopción de medidas de seguridad.

En cuanto al primero de los aspectos mencionados, la Resolución acuerda la delimitación de tres niveles de fiabilidad, de modo que los ficheros de

---

[15] Nuevo Artículo 66 Ley 4/2000 de 11 de enero sobre derechos y libertades de los extranjeros en España y su integración social. «2. *Toda compañía, empresa de transporte o transportista estará obligada a enviar a las autoridades españolas encargadas del control de la entrada la información comprensiva del número de billetes de vuelta no utilizados por los pasajeros que previamente habían transportado a España(..). Cuando así lo determinen las autoridades españolas, la información comprenderá, además, (..) el nombre y apellidos de cada pasajero, su fecha de nacimiento, nacionalidad, número de pasaporte o del documento de viaje que acredite su identidad*».

[16] En este sentido su importancia sería similar a la de los códigos éticos adoptados por las policías de otros Estados (como por ejemplo Reino Unido), pero con el efecto de su carácter obligatorio, de modo que la Resolución constituye una auténtica «norma» obligatoria para los integrantes de los cuerpos policiales y no una mera expresión de principios, circunstancia típica de un código ético o de conducta.

investigación policial se clasificaran en alguna de las siguientes categorías: De alta fiabilidad; De relativa fiabilidad; y De baja fiabilidad. Esta clasificación es especialmente importante a la hora de valorar la exactitud de los datos y, por tanto, las posibles limitaciones a la utilización de los mismos.

Al propio tiempo, la Resolución dispone que deban adoptarse las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos mediante la limitación del acceso únicamente a personal autorizado.

En lo referente a la conservación y cancelación de los datos, la Resolución distingue tres grandes categorías de actuaciones de investigación por parte de los servicios policiales, ya se trate de la represión de amenazas graves e inminentes, otros peligros reales para la seguridad pública, o la represión de otras infracciones penales. Para todos estos supuestos la Resolución ordena observar una serie de criterios con vistas a la cancelación automática de los datos personales, con lo que se refuerza el cumplimiento estricto del principio de conservación.

2. EL TRATAMIENTO DE LOS FICHEROS POLICIALES EN LA CONVENCIÓN DE PRÜM

La Convención de Prüm prevé, en esencia, la mejora de la cooperación policial mediante el intercambio de información o, más exactamente, haciendo disponible la información contenida en ficheros nacionales a las autoridades homólogas de los países signatarios. De esta afirmación se concluye claramente que todos los principios de protección de datos a los que se someten los ficheros policiales y que acabamos de comentar son de aplicación, y ello por cuanto que la información que se hace disponible ya se encuentra, por regla general, en ficheros nacionales.

Con vistas a analizar la correspondencia de las disposiciones de protección de datos del Convenio de Prüm con aquellas que acabo de describir, aplicables en España, entraré en el detalle de algunos de estos preceptos.

Así, respecto del principio de limitación de la finalidad, el Convenio-artículo 35- indica que los datos únicamente podrán ser utilizados para la finalidad que justificó su transmisión. La utilización para otros fines sólo sería posible en caso de que se encontrase habilitada por el Derecho del Estado transmitente. De ello podemos concluir que la utilización de los datos que fueran transmitidos desde las bases de datos españolas debería ajustarse a la finalidad que justificó la transmisión, y al uso para el que esos datos fueron inicialmente recabados.

Asimismo, respecto del tratamiento de los datos transmitidos, Prüm establece la limitación de las autoridades receptoras de la información a aquellas competentes para el desempeño de una función en el marco de los fines de investigación y prevención de delitos[17]. Dicha regla deberá entenderse aplicable en el derecho español a las Fuerzas y Cuerpos de Seguridad, los órganos jurisdiccionales y el Ministerio Fiscal, de conformidad con lo establecido en su normativa reguladora[18].

El ya mencionado principio de exactitud de los datos, también está presente en el Convenio de Prüm al exigir tanto la corrección o cancelación de los datos que se revelen erróneos como la «señalización» de los datos «cuya exactitud no pueda determinarse». Como ya hemos tenido ocasión de analizar, esta previsión está en consonancia con las regulaciones de los ficheros policiales comentadas que prevé el almacenamiento de la información en función de su grado de fiabilidad.

Las medidas de seguridad que deben aplicarse también son objeto de una particular atención en el Convenio al prever que la información se proteja frente a toda acción fortuita que pueda suponer su acceso, modificación, divulgación o destrucción no autorizada. El detalle y los mecanismos para la introducción de estas medidas se encuentran en el acuerdo de desarrollo del Convenio que fue firmado el pasado día 5 de diciembre en Bruselas.

Cabe destacar que esta obligación ya se cumple en España, como consecuencia de la aplicación del Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal[19], que impone la obligación de adoptar medidas de seguridad de nivel alto a los ficheros que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.

---

[17] Artículo 36: Los datos de carácter personal transmitidos únicamente podrán ser tratados por las autoridades y tribunales que sean competentes para el desempeño de una función en el marco de los fines previstos en el artículo 35. En particular, la ulterior comunicación de los datos transmitidos a otras instancias requerirá la autorización previa de la Parte Contratante transmitente y estará sujeta al derecho interno de la Parte Contratante receptora.

[18] Esta norma es fundamental, habida cuenta que el artículo 36 prevé que la cesión de datos a otras instancias debería contar con la autorización de la Parte transmitente, siendo preciso que las transmisiones de datos procedentes de tratamientos efectuados en España queden limitadas a supuestos similares a los admisibles en la Ley española o que se encuentren amparados por una norma con rango de Ley o un Convenio internacional, de conformidad con los artículos 11 y 34 de la Ley Orgánica 15/1999.

[19] Real Decreto 994/1999 de 11 de junio. Artículo 4.3 «*Los ficheros que contengan datos (…) recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto*».

Entre dichas medidas, aparte de las referidas a identificación y autenticación recogidas para el denominado nivel medio se encuentran las relativas al cifrado de la información[20].

Los derechos de los afectados- acceso, rectificación, cancelación e indemnización en caso de perjuicio- también son objeto de reconocimiento, e incluso se prevé la posibilidad de recurso ante el órgano de control independiente. Cabría, no obstante preguntarse el encaje del efectivo ejercicio de estos derechos dada la limitación a los mismos contenidas en la LOPD. A este respecto cabe destacar que una interpretación armonizada de la Ley Orgánica a la vista del Convenio podría permitir el ejercicio de estos derechos, en su caso, por vía de excepción a lo previsto en la propia Ley Orgánica.

La tramitación de las reclamaciones de los afectados, la verificación de la licitud del tratamiento, el ejercicio de poderes de supervisión y control y la colaboración con otras autoridades de la misma naturaleza corresponderá a la Agencia Española de Protección de Datos[21].

No quiero finalizar sin hacer una breve consideración al tratamiento de datos genéticos previstos por el Convenio. Desde la Agencia Española de Protección de Datos partimos de la premisa de que cualquier dato de carácter genético deberá ser considerado como un dato que afecta a la salud de las personas, y sometido, por tanto, a disposiciones específicas. A todo ello se une el hecho de que, como ya hemos comentado, el ordenamiento español sólo permite el tratamiento de este tipo de datos cuando se trate de vestigios encontrados en el lugar del delito, así como aquellos otros obtenidos con el consentimiento del interesado o en virtud de resolución judicial que acuerde la obtención de muestras de un determinado sospechoso.

Además, los datos obtenidos en virtud de una resolución judicial únicamente podrían ser empleados en la resolución de la causa en cuyo marco fueron obtenidos, dado que, en caso contrario, implicaría la utilización de los datos para otras finalidades distintas. En definitiva, los datos recopila-

---

[20] Así, dispone el artículo 23 del Reglamento que «*La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte*», añadiendo el artículo 26 que «*La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros*».

[21] Competencia derivada, principalmente, del artículo 9.1 del Estatuto de la AEPD aprobado por el Real Decreto 428/1993 de 26 de marzo.

dos en el ámbito de una investigación concreta no podrán ser incluidos en una especie de banco de datos genéticos que pudieran emplearse para futuras investigaciones, sino que será exigible la existencia de una autorización concreta para un nuevo tratamiento o que el interesado prestase su consentimiento inequívoco a la conservación de sus datos genéticos. En este sentido, no sería suficiente considerar habilitada la creación de una base de datos de mayor amplitud por el hecho de que se contenga la previsión en el propio Convenio, ya que éste se remite a la legislación interna para establecer el ámbito y alcance del tratamiento.

Esta afirmación debe entenderse, no obstante, con las matizaciones que se deriven de la eventual aprobación del proyecto de Ley presentado por el Gobierno que prevé la creación de bases de datos policiales sobre identificadores obtenidos a partir del ADN.

3. CONCLUSIONES

Es evidente que la eficacia de la acción policial depende en gran medida de la información de la que dispongan las Fuerzas y Cuerpos de Seguridad. Y es también patente que la proliferación de acciones criminales cada vez más globalizadas sólo puede combatirse debidamente mediante el desarrollo de mecanismos de colaboración internacional entre fuerzas policiales. Pero debe tenerse siempre presente que los instrumentos de los que dispongan los cuerpos policiales en la lucha contra el crimen no pueden ser ilimitados ni utilizarse indebidamente. Los derechos de los ciudadanos y, entre ellos, a la protección de sus datos personales deben salvaguardarse en todo momento buscando, como hemos tenido ocasión de comprobar a través del análisis de nuestra regulación, un equilibrio proporcionado con el que se garantice, sin fisuras, que la sociedad democrática y de valores que intentamos proteger no se vea, en último término, afectada.

RESUMEN

Con este trabajo se pretende exponer la regulación de los ficheros que, conteniendo datos de carácter personal, se encuentran en manos de las Fuerzas y Cuerpos de Seguridad. La primera parte de la exposición se centra en la regulación que de los ficheros con fines policiales realiza la legislación internacional- Recomendación 87(15) del Consejo de Europa- y la normativa española- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal-. La delimitación de los criterios que debe seguir el tratamiento de los datos personales por las fuerzas de

orden público y las garantías que en dicho tratamiento deben adoptarse son las líneas claves desarrolladas en el artículo. En la segunda parte del mismo, se analizarán algunas de las implicaciones del Tratado de Prüm, convenio internacional que prevé la disponibilidad de información en manos de las fuerzas policiales de un Estado miembro a sus homólogos de otro Estado miembro, respecto del tratamiento de la información disponible y su adecuación a la normativa reguladora en la materia.

PALABRAS CLAVE: Protección de datos; ficheros policiales; fuerzas de seguridad; principio de proporcionalidad; finalidad; conservación de los datos; medidas de seguridad; derechos de acceso, rectificación y cancelación de los datos; ADN.

ABSTRACT

The aim of this article is to explain the legal regulation of the files with personal data processed by police forces. The first part of the article is focused on the regulation of the police files from an international and national perspective- Recommendation 87(15) of the Council of Europe and Spanish Organic Law 15/1999, on the protection of personal data-. This part of the text explains the criteria to be followed while processing personal data by Police forces as well as the safeguards to be adopted in that processing. In the second part, the analysis is focused on the implication of the Treaty of Prüm, International Convention aiming at to make available the information handled by Law enforcement authorities of a Member State to the competent authorities of other Member State, with respect to the processing of the information available and its adequacy to the legislation applicable to that field.

KEY WORDS: Prüm, police files; law enforcement authorities; proportionality principle purpose limitation; data storage; security measure; right of access, rectification and erasure.