EGUZKILORE
Número 23.
San Sebastián
Diciembre 2009
351 - 366

PRINCIPIO DE DISPONIBILIDAD Y PROTECCIÓN DE DATOS PERSONALES: A LA BÚSQUEDA DEL NECESARIO EQUILIBRIO EN EL ESPACIO JUDICIAL PENAL EUROPEO

José Francisco ETXEBERRIA GURIDI

Profesor Titular de Derecho Procesal
Universidad del País Vasco/Euskal Herriko Unibertsitatea

I. ALGUNAS DEFICIENCIAS EN LA COOPERACIÓN JUDICIAL EN MATERIA PENAL EN EL SENO DE LA UE

1.1. El carácter secundario de la tutela de los derechos y garantías en la cooperación judicial penal

Se ha achacado con relativa frecuencia que la cooperación judicial penal en la UE, o el progresivo desarrollo del espacio judicial penal europeo, se ha centrado fundamentalmente en términos de eficacia en la persecución de infracciones penales, aparcando en un segundo plano la protección de los derechos y las garantías que pueden verse afectados. Aunque existieran precedentes sobre la cuestión, es en el Consejo Europeo de Tampere cuando se proclama que el principio del reconocimiento mutuo de las resoluciones judiciales será la "piedra angular" de la cooperación judicial en la UE[1]. La primera concreción de este principio en el ámbito penal será la adopción de la Decisión Marco (DM) sobre la orden europea de detención y entrega, de 13 de junio de 2002.

---

1. En la comunicación de la Comisión al Consejo y Parlamento europeo [COM (2000) 495 final] se afirma que dicho principio "*significa que una vez adoptada una medida, como una resolución dictada por un juez en el ejercicio de sus facultades oficiales en un Estado miembro, en la medida en que tenga implicaciones extranacionales, será automáticamente aceptada en todos los demás Estados miembros, y surtirá allí los mismos efectos o, al menos, similares*".

A esta DM han sucedido otras muchas. Pero ha de reconocerse que el principio de reconocimiento mutuo de resoluciones judiciales en el ámbito penal no se aplica de forma automática o pura, sino que las autoridades de ejecución se reservan de ordinario el control del cumplimiento de ciertos requisitos o presupuestos[2]. La causa fundamental de que no se haya optado por la aplicación del principio de reconocimiento mutuo de resoluciones penales en su sentido amplio o puro no es otro que la coexistencia en el seno de la UE de una gran diversidad de sistemas penales, diversidad que se extiende a los órganos competentes para actuar a lo largo del proceso penal, a la estructura de los propios procesos penales, etc., pero también a los distintos niveles y contenidos de los derechos y garantías procesales. No descubrimos nada nuevo si afirmamos que en el ámbito de la justicia penal los derechos fundamentales del individuo resultan afectados con una particular intensidad, por lo que la mera proclama del principio de reconocimiento mutuo no es suficiente[3].

El principio de reconocimiento mutuo ha de contar con un sustrato sólido y este no es otro que la existencia de una mutua confianza respecto de los sistemas de justicia penal de los Estados miembros[4]. La mutua confianza se convierte, de este modo, no sólo en la clave de bóveda del reconocimiento mutuo, sino en su presupuesto previo[5]. Sin embargo, la confianza mutua entre los Estados miembros de la UE hay que generarla, no se construye sobre el vacío. Y si esa desconfianza está motivada por la diversidad de los sistemas de justicia penal, la situación no se modificará en tanto en cuanto no exista una armonización o aproximación mínima de las normas que regulan las estructuras procesales penales en aquéllos. Lo dicho vale especialmente para el nivel de reconocimiento y respeto de los derechos fundamentales del individuo que pueden resultar afectados[6]. En tal sentido, afirmaba el Abogado General, D. RUIZ-JARABO COLOMER en sus conclusiones a los asuntos *Hüseyn Gözütok* (C-187/01)

---

2. Por este motivo DELGADO MARTÍN, J. se refiere a la existencia de "grados en la aplicación del reconocimiento mutuo", esto es, cuanto mayor sea la cantidad de extremos a controlar en el Estado de ejecución, menor será el grado de aplicación del reconocimiento mutuo. La orden de detención europea y los procedimientos de entrega entre los Estados miembros de la Unión Europea, *"Derecho penal supranacional y cooperación jurídica internacional", Cuadernos de Derecho Judicial*, núm. XIII, 2003, p. 291.

3. Por este motivo, afirma MITSILEGAS, Valsamis que este principio característico del mercado interno no se puede trasladar sin más al ámbito de la justicia penal: The constitutional implications of mutual recognitions in criminal matters in the EU, *Common Market Law Review*, núm. 43, 2006, p. 1291.

4. En la Comunicación de la Comisión de 26 de julio de 2000 [COM (2000) 495 final] se afirma que "la confianza mutua es un elemento importante; no sólo confianza en la adecuación de las normas de los socios, sino también en que dichas normas se aplican correctamente".

5. WEYEMBERGH, Anne: *L'harmonisation des législations: condition de l'espace pénal européen et révelateur de ses tensions*, Bruxelles: Editions de l'Université de Bruxelles, 2004, pp. 144-145; GLESS, Sabine: "Free movement of evidence in Europe", en *El Derecho Procesal Penal en la Unión Europea*, (ARMENTA DEU, T./GASCÓN INCHAUSTI, F./CEDEÑO HERNÁN, M. coords.), Madrid: Colex, 2006, p. 130.

6. Entre las prioridades recogidas en el Plan de Acción relativo al Programa del Consejo Europeo de La Haya en materia de justicia civil y penal se destaca "garantizar un espacio europeo de justicia garantizando el acceso eficaz a la justicia para todos y la ejecución de sentencias. *La aproximación proseguirá, concretamente mediante la adopción de normas que garantizan un alto grado de protección de las personas, con objeto de crear una confianza mutua y de reforzar el reconocimiento recíproco que sigue siendo el elemento clave de la cooperación judicial*", Comunicación de la Comisión al Consejo y al Parlamento Europeo, de 10 de mayo de 2005, COM (2005) 184 final.

y *Klaus Brügge* (C-385/01), presentadas el 19 de septiembre de 2002, que la meta compartida de facilitar y acelerar la cooperación entre los Estados miembros "no puede ser alcanzada sin una recíproca confianza de los Estados miembros en sus sistemas de justicia penal y sin un reconocimiento mutuo de los respectivos pronunciamientos, adoptados en un verdadero '*mercado común de los derechos fundamentales*'".

Esta es la posición que sostiene Anne WEYEMBERGH quien entiende que la armonización no es simplemente un elemento que favorezca el reconocimiento mutuo, sino que es la condición misma de dicho reconocimiento. Es más, apunta que el reconocimiento mutuo de decisiones judiciales penales no parece "deseable" desde el punto de vista de la protección de los derechos y libertades fundamentales si no es acompañado de una profundización de los trabajos de armonización. El principio de reconocimiento puede suponer una puesta en peligro de los derechos fundamentales si se suprimen las ocasiones de verificar si las garantías procesales mínimas que imponen el CEDH y la Carta de Derechos Fundamentales de la UE han sido efectivamente respetados[7].

En la Comunicación de la Comisión, de 19 de mayo de 2005, se sostiene que las dificultades puestas de manifiesto con las primeas aplicaciones del principio de reconocimiento mutuo podrían solucionarse en parte con la aprobación, en la Unión, de medidas legislativas de armonización. Uno de los ejes en torno al cual se han de articular aquéllas consiste en garantizar que las resoluciones judiciales objeto de reconocimiento mutuo respondan a "normas exigentes en términos de garantías de los derechos de las personas"[8]. Resulta loable que la propia Comisión se refiera a "normas exigentes" para la tutela de los derechos de las personas, pues no pocos autores han puesto de manifiesto el temor a que la armonización legislativa se produzca a un nivel bajo o inferior[9].

---

7. "La reconnaissance mutuelle des décisions judiciaires en matière pénale entre les Etats membres de l'Union européenne: mise en perspective", en *La reconnaissance mutuelle des décisions judiciaires pénales dans l'Union européenne* (DE KERCHOVE, Gilles/WEYEMBERGH, Anne ed.), Bruxelles: Editions de l'Université de Bruxelles, 2001, pp. 57-58. Esta misma autora afirma en otro lugar que "sin aproximación, no hay confianza mutua; sin confianza mutua, no hay reconocimiento mutuo efectivo y tampoco espacio penal europeo", *L'harmonisation des législations...*, cit., p. 147. También GÓMEZ-JARA DÍEZ, C: "Orden de detención europea y Constitución Europea: reflexiones sobre su fundamento en el principio de reconocimiento mutuo", *La Ley*, núm. 6069, 2004, p. 6. Podría sostenerse que la aproximación normativa no es necesariamente presupuesto del reconocimiento mutuo, sino que ambos pueden interactuar aprovechándose mutuamente, actuando, como una especie de "círculo virtuoso": PISANI, Mario. "Il 'processo penale europeo': problemi e prospettive", *Rivista di Diritto Processuale*, núm. 3, 2004, p. 676.

8. COM (2005) 195 final. Los ámbitos sobre los que ha de pivotar la armonización pertenecen en mayor medida al Derecho procesal penal: mejorar las garantías en los procesos penales; reforzar la presunción de inocencia; elaborar normas mínimas en materia de recogida de pruebas; regular las resoluciones dictadas en rebeldía y garantizar la transparencia de la elección del órgano jurisdiccional competente.

9. En tal sentido WEYEMBERGH, Anne afirma "Lejos de tender hacia un alineamiento por lo alto en este plano, el reconocimiento mutuo instiga más bien a contentarse con el más pequeño común denominador y entraña de esta manera una nivelación por lo bajo de los derechos y garantías procesales que disfrutan las personas afectadas por el proceso penal", *L'harmonisation des législations...*, cit., pp. 151-152; la misma autora en La reconnaissance mutuelle des décisions..., cit., pp. 60-61. También BRANTS, Ch.: "Procedural safeguards in the European Union: too little, too late?", en *European Evidence Warrant* (VERVAELE, J.A.E. ed.), Antwerpen/Oxford: Intersentia, 2005, p. 104 y 118. SCHÜNEMANN, Bern hace referencia igualmente al riesgo de que en todo el territorio de la UE se aplique el ordenamiento penal y procesal penal más punitivo de un Estado miembro, "¿Peligros para el Estado de Derecho a través de la europeización de la administración de justicia penal", en *El Derecho Procesal Penal en la Unión Europea*, cit., p. 25.

Para acreditar las dificultades que plantea la cooperación judicial penal en la UE resulta suficiente con la lectura de la Comunicación de la Comisión, de 3 de julio de 2007, relativa al "Informe sobre ejecución del Programa de La Haya en 2006". En la misma se afirma que el nivel de realización del Programa sobre la materia es "insuficiente" y, en general, en este ámbito "se ha progresado lentamente". Algunos aspectos, incluso, por ejemplo la aplicación de la DM sobre ejecución de resoluciones de embargo preventivo y de aseguramiento de pruebas, "es decepcionante"[10]. Igualmente pesimista es el balance de la Comisión en su Comunicación de 28 de junio de 2006 sobre "Ejecución del Programa de La Haya: el camino a seguir". Se afirma en la misma que "las discusiones en el Consejo han mostrado que recientemente está resultando muy difícil avanzar en la UE en áreas tales como el reconocimiento mutuo en asuntos penales y la cooperación policial" o que "no se ha logrado ningún avance en los últimos tres años con respecto a las normas mínimas básicas sobre derechos procesales aplicables en la UE"[11].

Por todo ello, y como conclusión a este primer apartado, procede aplaudir la aprobación de la DM 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Esta DM, que comentaremos, supone un primer paso en el necesario desarrollo de la dimensión de protección de las libertades y derechos en el seno de la cooperación judicial penal en la UE. Decimos que un primer paso, pues, como tendremos ocasión de comprobar, dicha DM tiene un alcance muy limitado.

1.2. El fundamento normativo: el Título VI del TUE y las interferencias

El derecho a la protección de los datos de carácter personal tiene en España un fundamento constitucional. Su art. 18.4 dispone que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[12]. En el plano internacional, podemos hacer mención igualmente al art. 8 CEDH, esto es, del derecho a la vida privada, uno de cuyos contenidos es precisamente el derecho a la protección de los datos de carácter personal[13]. No menos importante, por su repercusión en la posterior regulación de la materia por los Estados firmantes, es el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en adelante Convenio 108).

En el marco del acervo comunitario podemos mencionar en primer término la Directiva 95/46/CE, 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

10. COM (2007) 373 final.

11. COM (2006) 331 final. Se refiere indudablemente a la Propuesta de DM relativa a determinados derechos procesales en los procesos penales celebrados en la UE [COM (2004) 328 final].

12. Acerca de los perfiles propios que presenta este derecho en relación al derecho a la intimidad, *vid.* las SSTC 254/1993, de 20 de julio, y 292/2000, de 30 de noviembre, entre otras.

13. *Vid*. al respecto, por ejemplo, la sentencia del TEDH de 4 de diciembre de 2008, asunto *S. y Marper c. Reino Unido.*

de estos datos. Esta Directiva persigue que los Estados miembros garanticen la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales (art. 1.1)[14]. El problema reside, en cuanto ahora nos interesa, en su ámbito de aplicación, pues queda fuera del mismo, conforme al art. 3.2, el tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, excluyendo expresamente, por consiguiente, las actividades comprendidas en el Título VI TUE (cooperación judicial y policial en materia penal). La protección de los datos personales en materia de cooperación judicial penal se mantiene, pues, en el ámbito intergubernamental y sujeto a los instrumentos normativos propios del mismo (fundamentalmente las DM), esto es, en lo que se denomina el "Tercer Pilar" del Tratado[15].

Otro tanto ocurre con la Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. De forma casi idéntica a la del caso anterior, el art. 1.3 excluye de su ámbito de aplicación las actividades no comprendidas en el ámbito del Derecho comunitario, con mención expresa de las actividades del Título VI TUE y "en cualquier caso" de las actividades del Estado "en materia penal"[16].

La anterior Directiva es derogada y sustituida por la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Como se deduce del encabezamiento de la Directiva y se afirma expresamente en sus considerandos, la razón de la sustitución no es otra que adaptarse al desarrollo de los mercados y de las tecnologías para que el nivel de protección de los datos personales y de la intimidad ofrecido a los usuarios de los "servicios de comunicaciones electrónicas" sea el mismo, "con independencia de las tecnologías utilizadas", esto es, que sea extensible a las "nuevas tecnologías digitales" (4) y (5). Siendo este el principal motivo de la reforma, no es de extrañar que esta Directiva contenga en su art. 1.3 idéntica exclusión de su ámbito de aplicación a la contenida en la anterior Directiva, es decir, la cooperación judicial penal (Título VI TUE) y expresamente las actividades del Estado en materia penal[17].

---

14. En el Considerando (10) se insiste en el mencionado objeto de la Directiva con cita expresa del art. 8 CEDH y de los principios generales del Derecho comunitario, sin que la aproximación de las legislaciones nacionales pueda "conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad".

15. En concreto, el art. 13.1 de la Directiva prevé que los Estados miembros podrán adoptar "medidas legales" para limitar el alcance de ciertos derechos cuando la limitación constituya una medida necesaria para la salvaguardia de la prevención, la investigación, la detección y la represión de infracciones penales (letra d).

16. También en este caso, el art. 14.1 prevé que los Estados miembros podrán adoptar "medidas legales" para limitar el alcance de ciertos derechos cuando la limitación constituya una medida necesaria para la salvaguardia de la prevención, la investigación, la detección y la represión de infracciones penales.

17. El art. 15.1 contiene una referencia muy similar a la recogida en la nota anterior (17) aunque añade que la medida además de necesaria en una sociedad democrática ha de ser proporcionada y apropiada y, además, en relación con la conservación de datos señala expresamente que "los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado".

Todas las Directivas hasta ahora mencionadas tienen por objeto asegurar una adecuada protección de los datos de carácter personal, pero excluyen de su ámbito de aplicación las actividades relacionadas con la persecución de hechos punibles. Por este motivo llama la atención y, como se verá ha sido objeto de polémica, la aprobación de la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Llama la atención pues, al margen de su encabezamiento, el objeto de la presente Directiva que no es otro que resolver, precisamente, el problema que se plantea como consecuencia de la diversidad con que las legislaciones de los Estados miembros están abordando las excepciones a los derechos y garantías reconocidos con carácter general cuando se trata de una medida necesaria para la prevención, investigación, detección y enjuiciamiento de delitos.

En efecto, esta última Directiva reconoce en sus considerandos que varios Estados miembros han adoptado legislación que prevé la conservación de datos por los prestadores de servicios para la prevención, investigación, detección y enjuiciamiento de delitos y que "estas disposiciones de las normativas nacionales varían considerablemente" (5)[18]. Por si hubiera alguna duda acerca de los verdaderos motivos de su aprobación, el art. 1.1 de la Directiva dispone que la misma "se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro".

En principio hay que valorar muy positivamente el sentido de la Directiva, pues concreta con cierta precisión una serie de cuestiones que, al menos, sirven para satisfacer la exigencia de "calidad" de la previsión legal por la que se producen injerencias en los derechos de los individuos (en el sentido exigido por el TEDH en relación con el art. 8 CEDH). Así, se concreta la categoría de datos que deben conservarse, que en ningún caso puede comprender el contenido de las comunicaciones, se fijan unos períodos mínimos y máximos de conservación, se prevé la existencia de autoridades independientes de control, etc.

Ahora bien, de una lectura de los considerandos citados y, sobre todo, del art. 1.1 nos surge la duda de si no se ha producido una interferencia con las actividades propias del Título VI TUE, esto es, con al ámbito propio de la cooperación judicial y policial en materia penal. Las dudas no son infundadas si nos atenemos al recurso interpuesto por la República de Irlanda solicitando, precisamente, la anulación de la Directiva 2006/24/CE (pretensión que apoya la República Eslovaca).

En sus alegaciones, la República de Irlanda afirma que la elección del art. 95 CE como base jurídica de la Directiva 2006/24/CE constituye un error fundamental, pues el único objetivo o, al menos el objetivo principal o predominante de dicha Directiva es

18. También señala que las diferencias legales y técnicas entre disposiciones nacionales crean obstáculos en el mercado interior de las comunicaciones (considerando 6), pero menciona a continuación una serie de documentos de distintos órganos de la UE donde se subraya que la conservación de estos datos constituye una "herramienta valiosa" especialmente en el ámbito de la criminalidad organizada y el terrorismo (7) y (8).

facilitar la investigación, detección y enjuiciamiento de infracciones penales, con inclusión del terrorismo. Por lo tanto, la única base jurídica que puede proporcionar fundamento jurídico válido a las medidas que se recogen en dicha Directiva se encuentra en el Título VI (cooperación en materia penal)[19]. En su opinión, las medidas fundadas en el art. 95 CE deben tener por "centro de gravedad" la aproximación de las legislaciones nacionales con objeto de mejorar el funcionamiento del mercado interior y este objetivo tendría en la Directiva 2006/24 carácter meramente secundario[20].

Las pretensiones de Irlanda no son atendidas por el TJCE. En su sentencia de 10 de febrero de 2009 desestima el recurso de anulación al considerar que la base jurídica de la Directiva impugnada es correcta. Considera el Tribunal que la elección de la base jurídica de un acto comunitario debe basarse en elementos objetivos susceptibles de control jurisdiccional, entre los que figuran, en especial, la finalidad y el contenido del acto. El art. 95 CE habilita al Consejo a adoptar las medidas relativas a la aproximación de las disposiciones normativas de los Estados miembros que tengan por objeto el establecimiento y el funcionamiento del mercado interior, en especial cuando existan disparidades entre las regulaciones nacionales que puedan obstaculizar el ejercicio de las libertades fundamentales o crear distorsiones de la competencia afectando directamente al funcionamiento del mercado interior, como es el caso analizado[21]. Además, argumenta el TJCE que conforme al art. 47 TUE ninguna disposición del Tratado CE se verá afectada por una disposición del TUE y, consecuentemente, puesto que la modificación de la Directiva 2002/58/CE, que llevó a cabo la Directiva 2006/24/CE, es competencia de la Comunidad, esta última Directiva no podía basarse en una disposición del TUE sin vulnerar el art. 47 del mismo. Conforme al criterio del contenido material de las disposiciones de la Directiva 2006/24, entiende el TJCE que las mismas se limitan en esencia a las actividades de los prestadores de servicios y no regulan el acceso a los datos ni la explotación de éstos por las autoridades policiales o judiciales de los Estados miembros. Estas últimas cuestiones sí estarían en el ámbito de aplicación del Título VI TUE[22].

---

19. En el trasfondo del recurso se encuentra una iniciativa de Francia, Irlanda, Suecia y Reino Unido presentada al Consejo con vistas a la adopción de una Decisión Marco con el mismo objetivo que la Directiva (documento del Consejo 8958/04, de 28 de abril de 2004).

20. La República Eslovaca añade que la conservación de datos personales exigida por esta Directiva ocasiona una intromisión significativa en el derecho de los particulares al respeto de su vida privada, protegido por el art. 8 CEDH y resulta dudoso que una intromisión tan importante pueda justificarse por motivos económicos, como por un mejor funcionamiento del mercado interior.

21. En opinión del Tribunal de los autos se desprende que las obligaciones relativas a la conservación de los datos tienen implicaciones económicas sustanciales para los prestadores de servicios, en la medida en que pueden conllevar importantes inversiones y costes de explotación. Estas diferencias podían afectar directamente al funcionamiento del mercado interior.

22. Por este motivo no es trasladable, como pretendía Irlanda, el sentido de la sentencia TJCE de 30 de mayo de 2006 que anuló la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la CE y los EE.UU. de América sobre el tratamiento y transferencia de datos de pasajeros por las compañías aéreas al Departamento de Seguridad Nacional, Oficina de Aduanas y Protección de Fronteras de los EE.UU. y también la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa a la protección de datos personales incluidos en los registros de nombres de pasajeros que se transfieren al Servicio de Aduanas. En esta sentencia el TJCE entendió que las Decisiones no tenían por objeto un tratamiento de datos necesario para realizar la prestación de servicios por parte de las compañías aéreas, pero sí para proteger la seguridad pública y para fines represivos.

Nos ocuparemos básicamente de la normativa que en materia de protección de datos personales en el marco de la cooperación judicial en materia penal se ha adoptado bajo el paraguas del Título VI TUE. En algunos casos estos actos tienen este objetivo principal, como ocurre con la DM 2008/977/JAI, de 27 de noviembre de 2008. En otros, sin tener como objetivo principal la materia que nos ocupa, sí existe una importante repercusión en la misma, y son constantes las referencias hacia ella: Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza; la Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust[23].

Antes de concluir este apartado nos gustaría referirnos a la Carta de los Derechos Fundamentales de la UE[24], pues dedica expresamente el art. 8 a la "Protección de datos de carácter personal". Este precepto, tras proclamar en su apartado 1 el derecho de toda persona a la protección de los datos de carácter personal que le conciernen, expone en el apartado 2, de forma escueta pero indicadora, los principios inspiradores: "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 acceder a los datos recogidos que le conciernen y a obtener su rectificación". Por último, impone la existencia de una autoridad independiente que controle el respeto de estas normas. En la medida en que no se ratifique el Tratado de Lisboa (así lo dispone su art. 6.1), la Carta carece de efectos vinculantes, pero resulta frecuente encontrar una mención a la misma en la práctica totalidad de las DM adoptadas en el marco del Título VI TUE, así como criterio interpretativo en numerosas decisiones del TJCE[25].

II. EL DECAIMIENTO DE LAS GARANTÍAS SOBRE PROTECCIÓN DE DATOS PERSONALES EN EL MARCO DE LA INVESTIGACIÓN PENAL

Como tendremos ocasión de comprobar, el catálogo de principios inspiradores, garantías y derechos que las diferentes normativas sobre protección de datos recogen, experimenta importantes restricciones cuando se vincula el tratamiento de dichos datos personales con la prevención o la investigación y represión de la delincuencia. Este hecho no es objetable en sí mismo. Los derechos fundamentales no son en su mayoría absolutos, cabe justificar restricciones o limitaciones en los mismos en la medida en que así lo exija un superior interés digno igualmente de tutela constitucional, como es el caso de la persecución de hechos penales en aras de la justicia y para garantizar el respeto del ejercicio de los derechos por los restantes ciudadanos. Algo similar cabe predicar del derecho a la protección de los datos personales. Pero, en igual medida,

---

23. Acerca de las dificultades que presenta el proceso de toma de decisiones en el marco del Título VI TUE (cooperación judicial y policial en materia penal), es decir, el llamado método del "tercer pilar" *vid*. la Comunicación de la Comisión COM (2006) 331 final.

24. DO C 303, de 14 de diciembre de 2007.

25. *Vid*. al respecto PALAZZO, Francesco: "Charte européenne des droits fondamentaux et droit pénal", *RSC*, núm. 1, 2008, p. 2; ALONSO GARCÍA, R.: "El triple marco de protección de los derechos fundamentales en la Unión Europea", *Cuadernos de Derecho Público*, núm. 13, 2001, pp. 19-26.

tampoco las restricciones a este derecho pueden ser absolutas y lo que queremos dejar aquí patente es que con frecuencia se olvidan nuestros legisladores de precisar en las normas procesales o en otras las condiciones, bajo qué presupuestos y con qué limitaciones resultan justificadas dichas restricciones.

Si nos atenemos, por ejemplo, a lo dispuesto en la LO 15/1999, de protección de datos de carácter personal, ya su art. 2.2.c) excluye del ámbito de aplicación de la misma los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. La única garantía prevista para estos casos es la comunicación de la existencia de estos ficheros a la Agencia de Protección de Datos. No es ésta la única salvedad al régimen general de tutela del derecho. El consentimiento del afectado para el tratamiento de datos al que alude el art. 6 no es necesario cuando se trata de satisfacer fines policiales, aunque limitado a "aquellos supuestos y categorías de datos que resulten necesarios" para, entre otros fines, "la represión de infracciones penales" (art. 22.2). La persecución de hechos penales es también motivo de inaplicación del derecho a ser informado (art. 24.1)[26] o de los derechos de acceso, rectificación y cancelación (art. 23.1). Tampoco la cesión o comunicación de los datos está sujeta a la regla general del consentimiento del interesado cuando la misma tenga como destinatario el Ministerio Fiscal o los Jueces o Tribunales en el ejercicio de las funciones que tienen atribuidas (art. 11.2.d).

Como puede comprobarse, las salvedades al régimen general en materia de protección de datos cuando están relacionadas con la represión de hechos criminales apenas hacen mención a los criterios a que han de subordinarse dichas restricciones. Las más de las veces se limitan a una escueta referencia a que las mismas sean "necesarias". Sabemos, sin embargo, que el TEDH ha sido muy exigente con el requisito de la previsión legal cuando se trata de la injerencia en el derecho a la vida privada del individuo (art. 8 CEDH), y sobre todo cuando la misma se produce subrepticia o secretamente[27]. Quizás la única excepción la constituyan los criterios indicativos acerca del plazo de conservación de datos en ficheros policiales. La LO 15/1999 dispone inicialmente que estos datos se cancelarán "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento", si bien, a continuación, añade algunos criterios algo más precisos, como la edad del afectado, 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 (art. 22.4).

Si la finalidad de la previsión legal consiste en evitar posibles actuaciones abusivas o arbitrarias de los poderes públicos cuando se trata de la restricción del derecho que

---

26. Este precepto se refería originariamente también a la persecución de infracciones administrativas, sin embargo, la STC 292/2000, de 30 de noviembre, proclama que sustraer por tal motivo al interesado de información relativa al fichero y sus datos constituía una grave restricción de los derechos a la intimidad y a la protección de datos (f.j. 18).

27. Son numerosos los pronunciamientos en tal sentido del TEDH cuando se ha referido a la interceptación de las comunicaciones telefónicas, pero también en materia de protección de datos personales (huellas dactilares, perfiles de ADN) como es el caso de la reciente sentencia del Tribunal en el caso S. y Marper *c.* Reino Unido, de 4 de diciembre de 2008. En el plano doctrinal destacamos a ROGALL, Klaus: *Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht*, Tübingen: J.C.B. Mohr, 1992.

nos ocupa, se echa en falta una mayor concreción del contenido del derecho pese a dichas restricciones. El Convenio 108 también admite excepciones y restricciones con motivo de la represión de infracciones penales (art. 9). Pero precisamente por ello, considerando estas restricciones, el Consejo de Ministros del Consejo de Europa adoptó un instrumento de complemento de dicho Convenio para estos supuestos. Nos referimos a la Recomendación Nº R (87) 15, de 17 de septiembre de 1987, que tiene por objeto regular la utilización de datos personales en el sector de la policía. En dicha Recomendación, además de una específica referencia al art. 8 CEDH, se afirma en su Preámbulo que, considerando las disposiciones del Convenio 108 "y en particular las derogaciones permitidas por el art. 9", se recomienda a los Estados miembros asegurar la publicidad de lo dispuesto en los mismos y en particular los derechos que su aplicación confiere al individuo. En todo caso, son numerosas las referencias que en la Recomendación se hacen a que se recojan en una "legislación nacional específica" las excepciones a los derechos que se recomiendan en la misma.

III. LA DM 2008/977/JAI, DE 27 DE NOVIEMBRE, Y OTROS INSTRUMENTOS EUROPEOS SOBRE PROTECCIÓN DE DATOS EN LA INVESTIGACIÓN PENAL

Nos ocuparemos en este apartado esencialmente de la mencionada DM, sin olvidar que existen otros instrumentos normativos adoptados, ya sea en el marco del Título VI TUE o no, en materia de investigación penal en el ámbito europeo, pues como tendremos ocasión de comprobar, el ámbito de aplicación de dicha DM contiene numerosas excepciones (Eurojust, Sistema de Información Schengen, Sistema de Información Aduanero, etc.).

3.1. El Programa de La Haya y el "principio de disponibilidad"

El punto de arranque de la DM 2008/977/JAI ha de buscarse en el Programa de La Haya refrendado por el Consejo Europeo celebrado en noviembre de 2004. Para ejecutar dicho Programa la Comisión presentó una Comunicación al Consejo detallando una serie de prioridades, diez, a desarrollar en plazo de cinco años[28]. En el apartado o prioridad primera, relativa a los "derechos fundamentales y ciudadanía", se afirma, entre otras consideraciones, que "se debe prestar especial atención a la protección de los datos personales, cuyo carácter de derecho fundamental con entidad propia, distinto del derecho a la intimidad, se reconoce en la Carta de derechos fundamentales y en la Constitución". En la prioridad sobre la lucha contra el terrorismo se subraya el carácter crucial de la cooperación entre las autoridades competentes de los Estados miembros, "especialmente a la hora de intercambiar información pertinente para la investigación de actividades terroristas".

Pero es fundamentalmente en la prioridad séptima, titulada "Encontrar el equilibrio adecuado entre la protección de la vida privada y la seguridad al compartir

28. Que lleva por título "Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia" [COM (2005) 184 final]. El Programa de La Haya sitúa como alta prioridad en la agenda de la UE el "espacio de libertad, seguridad y justicia" y supone "el fin de un ciclo" (se refiere al Programa de Tampere) y "el principio de uno nuevo".

información", cuando se relacionan, por un lado, el principio de disponibilidad y, por otro lado, la necesaria protección de los datos de carácter personal. Esta prioridad subraya que el intercambio de información resulta esencial en la lucha eficaz contra el terrorismo y la delincuencia transfronteriza. Ahora bien, se añade, este intercambio de información no es admisible ilimitadamente, sino en el marco de un equilibrio adecuado entre seguridad y vida privada: "respetando plenamente los derechos fundamentales a la intimidad y a la protección de datos, así como el principio de disponibilidad de la información". En este contexto, se concreta lo que ha de entenderse por *principio de disponibilidad*: "las autoridades de un Estado miembro pondrán a disposición de las autoridades de otro Estado miembro la información que necesiten a efectos represivos, bajo ciertas condiciones"[29].

Con todo, podemos retrotraernos unos años para encontrar esta misma vinculación entre intercambio de información en la represión de hechos criminales y protección de datos personales. Nos referimos al Convenio sobre asistencia judicial en materia penal entre los Estados miembros de la UE, de 29 de mayo de 2000. Dicho Convenio dedica el Título IV, aunque con un solo artículo, a la protección de datos de carácter personal[30].

3.2. Ámbito de aplicación de la DM 2008/977/JAI

El objeto de la DM es realmente loable. "Para garantizar la protección de los datos personales sin comprometer el resultado de las investigaciones penales, es necesario definir los derechos del interesado". La citada proclama recogida en el considerando (28) constituye el eje sobre el que debería girar la DM. Tal como hemos anticipado anteriormente, ocurre que con frecuencia la normativa sobre protección de datos incorpora excepciones o limitaciones en el catálogo de derechos y garantías cuando entra en juego el interés público en la persecución de hechos penales. Pero a continuación poco más se añade acerca de la concreta situación del afectado y los mecanismos de reacción o defensa y los límites a las limitaciones o excepciones que se imponen sobre aquél. En la medida en que un derecho fundamental no es absoluto y admite restricciones justificadas, tampoco las restricciones pueden ser absolutas.

En tal sentido, el art. 1.1 DM afirma que el objetivo de la misma consiste en garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal.

---

29. En el mismo apartado se perfila esta finalidad al afirmar que la Comisión presentará propuestas, "entre ellas la posibilidad de consultar recíprocamente las bases de datos de los Estados miembros". En otro documento (Comunicación) presentada por la Comisión y titulado "Ejecución del Programa de La Haya: el camino a seguir" se dice que la Comisión "cree firmemente que, en paralelo al avance en el intercambio de información, es imprescindible avanzar en la protección de datos en el ámbito de la cooperación policial y judicial" con una legislación sobre la materia que "garantice un alto nivel de protección de los datos personales en todos los Estados miembros" [COM (2006) 331 final].

30. DO C 197, de 12 de julio de 2000. En el Informe Explicativo del mismo (DO C 379, de 29 de diciembre de 2000) se dice acerca de dicho Título IV que "es la primera vez que un convenio sobre cooperación judicial en materia penal incluye normas de protección sobre el intercambio de datos entre dos o varios Estados miembros".

En efecto, se reconocen en dicha DM una serie de garantías y derechos vinculados a la protección de datos personales (principios informadores, plazos de conservación de datos, derechos de información, acceso, rectificación, etc.). Sin embargo, pese al encabezamiento de la DM, su ámbito de aplicación no se extiende a todo el abanico de cooperación judicial y policial en materia penal. Aunque el objetivo de este primer precepto se extiende a la protección de datos en el marco del Título VI TUE, tenemos que acudir al antepenúltimo de los preceptos de la DM (art. 28) para aclarar cuál es su verdadero ámbito de aplicación. Conforme a dicho precepto, cuando algún acto adoptado en virtud del Título VI antes de la entrada en vigor de la presente DM y que regule el intercambio de datos personales entre Estados miembros o el acceso a sistemas de información, contempla disposiciones específicas sobre protección de datos, "éstas primarán" sobre las disposiciones de la presente DM.

La primera consecuencia a resaltar, por tanto, es la inexistencia de un régimen jurídico unificado en materia de protección de datos en el marco de la cooperación penal del Título VI. Hubiera sido deseable, de conformidad con lo previsto en el art. 1.1 DM ("garantizar un alto nivel de protección"), unificar el régimen de protección de datos optando, a ser posible, por el nivel más elevado de los distintos existentes[31]. El articulado de la DM no concreta qué actos adoptados en el marco del Título VI TUE quedan excluidos. El considerando (39) sí lo hace. Expresamente se dice en el mismo que la presente DM no afecta a las disposiciones sobre protección de datos que rigen el funcionamiento de Europol, Eurojust, el Sistema de Información de Schengen (SIS)[32] y el Sistema de Información Aduanero ni a las disposiciones contenidas en la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre transferencia automatizada de perfiles de ADN, datos dactiloscópicos y datos de registros nacionales de matriculación de vehículos. Pero el mencionado considerando condiciona la exclusión a que la regulación sobre protección de datos sea más detallada que la de la presente DM[33].

3.3. Algunas garantías sobre protección de datos

Con carácter previo al análisis de ciertas garantías recogidas en la DM que nos ocupa y en otros actos normativos, procede adelantar que, de conformidad con el art. 1.5, nada obsta a que los Estados miembros puedan establecer, para la protección de los datos personales recopilados o tratados a nivel nacional, garantías mayores a las establecidas en dicha DM. Como tendremos ocasión de comprobar, son numerosas las

---

31. Aunque se refiera al principio de reconocimiento mutuo, en concreto su aplicación en materia de obtención de pruebas, la Comisión se queja de que en el marco de la cooperación judicial penal se alcanzan, en ocasiones, acuerdos "sobre la base del mínimo común denominador", lo cual resulta insatisfactorio: Comunicación de la Comisión COM (2006) 331 final, de 28 de junio de 2006, "Ejecución del Programa de La Haya: el camino a seguir".

32. La DM cuando todavía era una propuesta no excluía de su ámbito de aplicación el SIS y se proponía que las disposiciones sobre protección de datos aplicables conforme a la regulación del SIS fueran sustituidas [COM (2005) 475 final].

33. Con el mismo tenor, el considerando (40), con referencia a otros actos adoptados en virtud del Título VI que dispongan sobre protección de datos, condiciona la exclusión del ámbito de aplicación de la DM a que las disposiciones contenidas en los primeros en relación al uso y transmisión de datos personales sean más estrictas que las previstas en la presente DM.

ocasiones en que la DM se remite al "Derecho nacional" para condicionar el ejercicio de determinados derechos o imponer limitaciones al tratamiento de datos personales.

También con carácter general conviene resaltar que la DM resulta de aplicación al tratamiento automatizado como no automatizado, total o parcial, de datos personales que formen parte o esté previsto que vayan a formar parte de un fichero (art. 1.3). Resulta incuestionable que mediante esta previsión la DM ha pretendido que no queden excluidos del ámbito de tutela de la DM los datos personales por la naturaleza del tratamiento a que son sometidos o porque el tratamiento de los mismos no sea uniforme[34].

3.3.1. La previsión de autoridades de control independientes

Para asegurar la efectividad del régimen de protección de los datos personales, suele ser habitual que los instrumentos normativos sobre la materia, tanto a nivel nacional como supranacional, establezcan la constitución de autoridades independientes que velen por la correcta aplicación de dicho régimen[35]. La Recomendación Nº R (87) 15, sobre utilización de datos personales en el ámbito de la Policía, por ejemplo, dedica el primero de los principios a dicha cuestión y dispone que cada Estado miembro debe disponer de una autoridad de control independiente y ajena a la Policía, encargada de velar por el respeto de los principios enunciados en dicha Recomendación.

La DM que nos ocupa no constituye una excepción, y en su considerando (33) se afirma que la creación en los Estados miembros de autoridades de control que ejerzan sus funciones con plena independencia constituye un aspecto esencial de la protección de datos personales tratados en el marco de la cooperación policial y judicial entre dichos Estados. En consonancia con lo señalado, su art. 25.1 prevé que cada Estado miembro disponga de "una o más autoridades" independientes en el ejercicio de sus funciones que consistirán en "asesorar y vigilar la aplicación de las disposiciones que los Estados miembros hayan adoptado en aplicación de la presente DM". Estas funciones de asesoramiento y vigilancia pueden ser asumidas por las autoridades de control ya existentes en los Estados miembros en virtud de la Directiva 95/46/CE[36].

Las funciones que pueden atribuirse a estas autoridades independientes de control son amplias. Pueden tener funciones consultivas con carácter previo al tratamiento de

---

34. El Convenio 108, que se refiere al tratamiento automatizado de datos, prevé en su art. 3.2.c) que los Estados firmantes puedan en cualquier momento hacer saber que se aplicará también dicho Convenio a los ficheros de datos personales que no sean objeto de tratamiento automatizado. La Recomendación Nº R (87) 15, sobre utilización de datos personales en el ámbito de la policía, también limita su ámbito de aplicación a los datos personales tratados automatizadamente. Sin embargo, también se dispone que los Estados miembros pueden extender los principios contenidos en la misma a los datos personales que no sean objeto de tratamiento automatizado. Es más, se afirma que el tratamiento no automatizado no puede ser admitido cuanto tiene por finalidad eludir la aplicación de la citada Recomendación.

35. SERRANO PÉREZ, M.M.: *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid: Civitas, 2003, pp. 461 y ss.; REBOLLO DELGADO, L.: *Derechos fundamentales y protección de datos*, Madrid: Dykinson, 2004, pp. 166 y ss.

36. Así se recoge en el considerando (34). La existencia de autoridades de control está prevista en el art. 28 de la mencionada Directiva. En la LO 15/1999, los arts. 35 y ss. se refieren a la Agencia de Protección de Datos.

datos personales que formen parte de un nuevo sistema si estos datos son reveladores del origen racial o étnico, de opiniones políticas, de convicciones religiosas o filosóficas, de afiliación sindical, relativos a la salud o a la vida sexual; o cuando el tipo de tratamiento, en particular mediante tecnologías, mecanismos o procedimientos nuevos, entrañe otro tipo de riesgos específicos para los derechos fundamentales (art. 23). En cuanto a las funciones de control o vigilancia, se les puede atribuir poderes para ordenar el bloqueo, la supresión o la destrucción de datos, prohibir provisional o definitivamente un tratamiento, etc. (art. 25.2.b). También dispondrán de capacidad para actuar en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente DM o de poner dichas infracciones en conocimiento de la autoridad judicial (art. 25.2.c)[37]. Para poder hacer efectivas estas funciones, la autoridad de control dispondrá de poderes de investigación, como el derecho de acceder a los datos que sean objeto de tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control (art. 25.2.a).

De forma similar a la indicada, la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, sobre el Sistema de Información Schengen de segunda generación (SIS II), contiene un régimen de sometimiento al control de autoridades independientes, pero en un doble plano atendiendo a la particular arquitectura de dicho sistema. Por un lado, una autoridad independiente "nacional" de control se encargará de supervisar la legalidad del tratamiento de los datos personales del SIS II dentro de su territorio y a partir de él (art. 60.1) y, por otro lado, corresponderá al Supervisor Europeo de Protección de Datos controlar que las actividades de tratamiento de datos personales de la "Autoridad de Gestión" sean conformes a dicha Decisión (art. 61.1)[38]. También la Decisión 2002/187/JAI por la que se crea Eurojust prevé un sistema dual de control por autoridades independientes. Por un lado, Eurojust dispondrá de un responsable de protección de datos que será un miembro designado específicamente para esta tarea y que en el ejercicio de sus funciones no recibirá ninguna instrucción (art. 17). Por otro lado, se constituye una Autoridad Común de Control externo, es decir, compuesto por jueces o personas independientes que no pertenezcan a Eurojust (art. 23)[39]. Más parcas son las referencias contenidas en la Decisión 2008/615/JAI, sobre cooperación transfronteriza en la lucha contra el terrorismo y la delincuencia transfronteriza, a la intervención de autoridades de control independientes[40].

---

37. De conformidad con los art. 17 y 18 DM, los derechos de acceso, rectificación, supresión o bloqueo se pueden ejercitar directamente ante el responsable del tratamiento o por mediación de la autoridad de control. Si el responsable del tratamiento denegare el acceso, se ha de poner en conocimiento del interesado que "puede recurrir ante la autoridad nacional de control" o los juzgados o tribunales competentes (art. 17.3).

38. A la Autoridad de Gestión le compete la gestión operativa del Sistema Central (art. 15), cuya unidad de apoyo técnico se encuentra en Estrasburgo, aunque existe una copia de seguridad en una localidad austriaca.

39. A ambos les corresponde velar por la adecuación del tratamiento de los datos a lo previsto en la Decisión y tienen acceso a todos los datos, ficheros y locales de Eurojust.

40. El art. 31 prevé que los Estados garanticen en caso de lesión de los derechos a la protección de datos del interesado, la presentación de una queja ante un tribunal o ante una autoridad de control independiente.

3.3.2. Principios de licitud, proporcionalidad y finalidad

En consonancia con lo que viene siendo habitual en materia de protección de datos, las autoridades competentes solo podrán recoger datos personales con fines determinados, explícitos y legítimos en el marco de sus funciones y sólo podrán tratarlos para el mismo fin con el que se hayan recogido (art. 3.1). La recopilación de los datos ha de ser para fines determinados, sin mayor concreción. La DM hace referencia a una serie de fines genéricos: prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales (art. 1.2)[41]. En cuanto al posterior tratamiento, se admite como excepción que lo sea para fines distintos en la medida en que: a) el tratamiento no sea incompatible con los fines para los que se recogieron; b) las autoridades estén autorizadas para ello; y c) el tratamiento sea necesario y proporcionado a ese fin (art. 3.2). Los fines distintos de los originarios se especifican en el art. 11 cuando el tratamiento de los datos en estos casos se haga por las autoridades de otro Estado miembro[42]. De cumplirse las condiciones previstas en el art. 13 los datos transmitidos o puestos a disposición por un Estado miembro pueden ser transmitidos por otro Estado miembro a un tercer Estado u organismo internacional. Incluso cabe la posibilidad de transmisión a particulares si ello resulta esencial (art. 14)[43].

En el marco también de los principios se dispone que el tratamiento de los datos deberá ser lícito y adecuado, pertinente y no excesivo con respecto a los fines para los que se recojan (art. 3.1). Nos encontramos ante una manifestación clara del principio de proporcionalidad. No se mencionan, en cambio, criterios indicadores de la medida de la proporcionalidad, por ejemplo, la gravedad de las infracciones penales. Resultaría más adecuado, a nuestro juicio, si la DM se hubiera hecho eco de una serie de apreciaciones o criterios que sí se recogían en la Propuesta de DM [COM (2005) 475 final]. Por ejemplo, clasificar los datos según su grado de exactitud y fiabilidad [que los basados en hechos se distingan de los basados en apreciaciones u opiniones personales (art. 4.1)] o la obligación de distinguir claramente entre datos relativos a personas meramente sospechosas de participar en un delito; a personas ya condenadas; a personas de las que se sospeche fundadamente que cometerán un delito; a personas consideradas víctimas o testigos o personas que no pertenezcan a ninguna de las categorías mencionadas (art. 4.3)[44].

---

41. La Recomendación Nº R (87) 15 hace una mayor precisión en la medida en que condiciona la recopilación de datos a que sean necesarios para la prevención de "un peligro concreto" o para la represión de "una infracción penal determinada" (principio 2.1).

42. Prevención y represión de infracciones penales distintas, otros procedimientos judiciales y administrativos directamente relacionados, prevención de amenazas inmediatas y graves a la seguridad pública o cualquier otro fin con el consentimiento previo del Estado transmisor o del interesado.

43. Se refiere, por ejemplo, al cumplimiento de funciones legalmente asignadas. No concreta el articulado de la DM qué ha de entenderse por particulares, pero el considerando (18) dispone que por tales no han de entenderse los abogados o víctimas.

44. Similares criterios para diferenciar los datos se recogen en la Recomendación Nº R (87) 15 (principio 3) o en la Decisión 2002/187/JAI sobre Eurojust (art. 15). Este último precepto alcanza a concretar qué tipo de datos personales se pueden tratar en un caso (personas objeto de actuaciones penales) o en otro (testigos o víctimas).

3.3.3. Rectificación, supresión y bloqueo de los datos

La DM se ocupa de la rectificación, supresión y bloqueo de datos desde una doble perspectiva: como obligación impuesta a los responsables del tratamiento (art. 4) y como derechos que pueden ser ejercitados por el interesado (art. 18). La rectificación procede cuando los datos sean incorrectos, pero comprende también la actualización o complemento. La supresión o disociación procede cuando ya no sean necesarios para los fines para los que fueron recogidos o legalmente tratados con posterioridad. En lugar de suprimirse, los datos pueden ser bloqueados si existen razones justificadas para suponer que la supresión pueda perjudicar los intereses legítimos del interesado. Desde la perspectiva del interesado, los Estados miembros han de concretar si aquél puede invocar estos derechos directamente ante el responsable del tratamiento o por mediación de una autoridad de control independiente. Si se deniega la rectificación, supresión o bloqueo, se ha de comunicar por escrito la misma al interesado, así como las posibilidades de reclamación o recurso (art. 18.1).

Se deja, sin embargo, a la libre discrecionalidad de los Estados miembros fijar los plazos a efectos de la supresión de datos personales o de la comprobación periódica de la necesidad de su conservación (art. 5). Tampoco se acompaña el pronunciamiento de mayores precisiones que serían deseables, como las recogidas en el art. 22.4 LO 15/1999 o la Recomendación Nº R (87) 15 (principio 7): edad del afectado, carácter de los datos conservados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolución, el indulto, la prescripción de la responsabilidad, etc.

3.3.4. Derechos de acceso e información al interesado

Ambos derechos están interrelacionados. El interesado tiene derecho a ser informado de la recopilación o tratamiento de sus datos personales por las autoridades competentes. Sin embargo, se realiza una remisión al Derecho nacional (art. 16.1). Este derecho puede excepcionarse, pues conforme al apartado siguiente el Estado transmisor de los datos puede pedir a otro Estado miembro que se abstenga de informar al interesado. Se echan en falta, también aquí, mayores precisiones acerca de los casos en que se puede limitar el derecho a ser informado.

En cuanto al derecho de acceso, todo interesado que lo solicite tendrá derecho a obtener al menos la confirmación, por parte del responsable del tratamiento o de la autoridad nacional de control, de que se han transmitido o puesto a disposición datos que le conciernen, e información sobre los destinatarios a quienes se han remitido (art. 17.1). Pero también en este caso pueden los Estados miembros adoptar medidas legislativas para limitar el acceso en determinados casos, por ejemplo, si ello resulta necesario y proporcionado para evitar que se obstaculicen investigaciones o procedimiento jurídicos; o para evitar que se obstaculice la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales (art. 17.2).