Tratamiento de datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales

Estudio de la Directiva UE 2016/680 y breve repaso a las nuevas medidas de investigación tecnológicas de la Ley de enjuiciamiento criminal

PID_00250898

Sílvia Pereira Puigvert

Universitat Oberta de Catalunya

Índice

1. Introducción

Vivimos en una sociedad cada vez más informatizada y se ha convertido en algo recurrente hablar de documentos, formularios y aplicativos electrónicos, servicios de mensajería instantánea, registros y portales telemáticos, etc. Hay toneladas de datos registrados electrónicamente y se hace necesario (mejor dicho, imprescindible) ocuparnos del tratamiento y protección de estos datos. Como algún autor indica, la importancia de los datos ha propiciado un constante debate normativo sobre la privacidad, la libre circulación de estos y, sobre todo, las garantías de seguridad ante tratamientos ilícitos de datos (Canals, 2016).

Referencia bibliográfica

D. Canals Ametller (2016). «El acceso público a datos en un contexto de transparencia y de buena regulación». En: *Datos. Protección, Transparencia y Buena Regulación* (págs. 11 y sig.). Documenta Universitaria.

Una buena muestra de este debate normativo fue la publicación el 27 de abril de 2016, por un lado, del Reglamento (UE) 2016/679 del Parlamento y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[1] (conocido como Reglamento general de protección de datos; Rodríguez, 2016) y, por otro lado, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, y la Directiva 2016/681 del Parlamento y del Consejo, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (Bosch).

Referencia bibliográfica

J. L. Rodríguez Álvarez (2016). «Transparencia y protección de datos personales: criterios legales de conciliación». En: *Datos. Protección, Transparencia y Buena Regulación* (pág. 57). Documenta Universitaria.

Referencia bibliográfica

Para más información sobre el contenido de esta Directiva 2016/681, véase:

A. Bosch Moliné. «La directiva europea sobre la utilización de datos PNR para la lucha contra el terrorismo y la delincuencia grave». Materiales didácticos UOC.

(1)Este Reglamento introduce importantes cambios en relación con los derechos de las personas, las obligaciones de los responsables y de los encargados de los tratamientos, la configuración y las competencias de las autoridades de control y el régimen sancionador, pero en el ámbito de la protección de datos de carácter personal mantiene en esencia los mismos principios reguladores del régimen jurídico de los tratamientos que ya están acogidos en nuestra Ley orgánica de protección de datos.

La necesidad de elaborar estándares mínimos sobre la protección de datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales surge ya desde el Convenio 108 del Consejo de Europa (1981) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y cuyo objetivo era garantizar a cualquier individuo, sea cual fuera su nacionalidad o lugar de residencia, el respeto de sus derechos y libertades fundamentales, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicho individuo (art. 1) y de la Recomendación 87 del Consejo de Europa (1987), sobre el uso de datos personales en el sector policial. Esta Recomendación, que tenía por objeto los datos con fines policiales como los necesarios para prevenir un peli-

gro para la seguridad pública o para el enjuiciamiento de infracciones penales, contemplaba una serie de derechos (de acceso, de rectificación y cancelación) que no distan mucho de los recogidos en las posteriores normas europeas.

A la búsqueda de una tutela reforzada de los datos responde, en primer lugar, la Decisión Marco 2008/977/JAI (de 27 de noviembre de 2008) y, en segundo lugar, la actual y vigente Directiva 2016/680 (de 27 de abril de 2016). A partir de este momento, el esquema a través del cual se agruparán las distintas cuestiones a tratar en este módulo empieza con un somero resumen sobre la Decisión Marco relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Seguidamente, se acometerá el estudio de la Directiva sobre tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales. Y el módulo se cerrará con el análisis de los presupuestos de las nuevas diligencias de investigación tecnológicas recogidas en la Ley de enjuiciamiento criminal (en adelante, LECrim), ya que pueden plantear situaciones especialmente controvertidas o perplejidades en lo que a la protección de datos e injerencia en la privacidad de las personas se refiere.

Empezando con la Decisión Marco 2008/977/JAI, esta pretendía, como objetivo específico, proteger los derechos fundamentales y las libertades de las personas cuando se tratasen sus datos personales con fines de prevención, investigación, detección y enjuiciamiento de una infracción penal o de ejecución de una sanción penal. Tanto es así, que en su preámbulo destacan disposiciones acerca del intercambio de datos personales en el marco de la cooperación policial y judicial en materia penal (Considerando número 5) y a las condiciones en que debe permitirse a las autoridades competentes de los Estados miembros la transmisión a autoridades y particulares y puesta a su disposición de datos personales recibidos de otros Estados miembros (Considerando número 17). Según el Considerando número 11 de la Decisión Marco, era necesario especificar los objetivos de la protección de datos en el marco de las actuaciones policiales y judiciales y establecer normas sobre la legalidad del tratamiento de datos personales, con el fin de garantizar que toda información que pueda intercambiarse se ha tratado lícitamente y de conformidad con los principios fundamentales relacionados con la calidad de los datos. Al mismo tiempo, no deben verse comprometidas en modo alguno las actuaciones legítimas de las autoridades policiales, aduaneras, judiciales y demás autoridades competentes.

Por lo demás, la consabida Decisión Marco tenía un ámbito de aplicación que se limitaba al tratamiento de los datos personales transmitidos o puestos a disposición entre Estados miembros. El contenido de esta Decisión ha venido marcado por luces y sombras. Y es que su trascendencia dependía, en buena medida, de si los Estados miembros, en la transposición de esta norma, deci-

días acatar sus preceptos de forma voluntaria para su ordenamiento interno o si se limitaban a transponerla para el ámbito de intercambio de información entre Estados miembros[2].

(2)«Protección de datos personales e investigación criminal» extraído de la página web del Poder Judicial.

Antes de abordar el estudio de la Directiva que deroga esta Decisión Marco, merece la pena hacer una breve referencia a la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos (LOPD) y, en particular, a su artículo 22, que se refiere a los ficheros de las Fuerzas y Cuerpos de Seguridad y a la distinción entre datos recogidos para fines administrativos y para fines policiales. Lo cierto es que se echa en falta en esta ley una mayor especificación de lo que son los fines administrativos y los fines policiales (art. 22 LOPD)[3]. Otras reglas de interés contenidas en la LOPD serían los artículos 2.2 c) (el régimen de protección de datos que se establece en esta ley orgánica no será de aplicación, entre otros, a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada) y 2.3 e) (se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta ley orgánica los tratamientos de datos personales procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad).

(3)Art. 22 LOPD: Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

En la medida en que existe un texto de anteproyecto de nueva Ley orgánica de protección de datos (de 23 de junio de 2017) es necesario destacarlo, especialmente, el artículo 20 que regula el tratamiento de los datos de naturaleza penal. El tratamiento de estos datos relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solamente podrá llevarse a cabo cuando se halle amparado en una norma de derecho de la Unión, en esta ley orgánica o en otras normas de rango legal. Y se encomendará al Ministerio de Justicia la gestión de los sistemas de información en que se recoja la totalidad de los datos relativos a condenas e infracciones penales,

así como a procedimientos y medidas cautelares y de seguridad conexas[4]. Y el artículo 15 del mismo anteproyecto dispone que el tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante el uso de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, vigilancia y disciplina del tráfico se regirá por su legislación específica y con carácter supletorio por el Reglamento general de protección de datos.

(4)Hay que tener presente de este anteproyecto la Disposición transitoria quinta, que presenta el siguiente tenor literal: los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley orgánica 15/1999, de 13 de diciembre, y sus disposiciones de desarrollo en tanto no entre en vigor la norma que trasponga al derecho español lo dispuesto en la citada directiva.

Y tras este marco introductorio, nuestra atención se repartirá entre la nueva Directiva sobre protección de datos para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales y las nuevas medidas de investigación tecnológicas de la LECrim.

2. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos

2.1. La colección de considerandos, ámbito material y de aplicación y objetivos

La Directiva (UE) 2016/680, cuya transposición debe ser a más tardar el 6 de mayo de 2018[5], se abre con un total de 107 considerandos que recogen, principalmente, reflexiones acerca de los objetivos de la Unión Europea, el respeto a los derechos fundamentales y principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea y los nuevos retos que se plantean en el ámbito de la protección de los datos personales por el avance de las nuevas tecnologías, que es imparable. Resulta ineludible aquí destacar el contenido concreto del Considerando número 80, que reza como sigue: aunque la presente Directiva también se aplica a las actividades de los órganos jurisdiccionales nacionales y otras autoridades judiciales, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los órganos jurisdiccionales actúen en ejercicio de su función jurisdiccional, con el fin de garantizar la independencia de los jueces en el desempeño de sus funciones.

(5)Artículo 63.1 de la Directiva: Los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones. Aplicarán dichas disposiciones a partir del 6 de mayo de 2018. Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia. Y el artículo 63.2 establece que no obstante lo dispuesto en el apartado 1, los Estados miembros podrán disponer que excepcionalmente y cuando suponga un esfuerzo desproporcionado, los sistemas de tratamiento automatizado establecidos con anterioridad al 6 de mayo de 2016 sean conformes con el artículo 25, apartado 1, antes del 6 de mayo de 2023. Más ampliación de plazo en el artículo 63.3: no obstante lo dispuesto en los apartados 1 y 2 del presente artículo, en circunstancias excepcionales, un Estado miembro podrá adaptar al artículo 25, apartado 1, un sistema de tratamiento automatizado a que se refiere el apartado 2 del presente artículo dentro de un plazo determinado después del período previsto en el apartado 2 del presente artículo, si de no hacer así surgieran serias dificultades para el funcionamiento de ese sistema de tratamiento automatizado concreto. Notificará a la Comisión los motivos de esas serias dificultades así como los del período específico dentro del cual adaptará ese sistema de tratamiento automatizado concreto a lo dispuesto en el artículo 25, apartado 1. En cualquier caso, el período determinado no podrá ser posterior al 6 de mayo de 2026.

Centrándonos en su ámbito material y de aplicación, resulta conveniente destacar que la Directiva establece las normas específicas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública (art. 1). Por lo que respecta a su ámbito de aplicación, la norma se extiende a las personas físicas, independientemente de su nacionalidad o lugar de residencia, en lo que se refiere al tratamiento de sus datos personales. Pero se excluyen de su ámbito de aplicación las actividades relacionadas con la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional.

La Directiva pretende asegurar que los datos de las víctimas, testigos y sospechosos de la comisión de delitos se encuentren debidamente protegidos en el marco de una investigación criminal. También se busca facilitar la cooperación transfronteriza de la policía y los fiscales para combatir más eficazmente el crimen y el terrorismo. Los Estados miembros deberán proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de sus datos personales, y garantizar que el intercambio de datos personales por parte de las autoridades competentes en el interior de la Unión no quede restringido ni prohibido por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Entre dichas autoridades competentes se deben incluir autoridades públicas tales como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad, y también cualquier otro organismo o entidad en que el derecho del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas.

2.2. Precisiones terminológicas

Tanto la Decisión Marco anterior como esta Directiva recogen la conceptualización de términos de interés. Así las cosas, se recoge un glosario con los términos de la Directiva que se consideran más relevantes para la temática examinada, sin perjuicio de que algunos de estos conceptos ya han sido objeto de análisis en otras asignaturas[6]:

(6)El resto de términos pueden consultarse en el artículo 3 de la Directiva. Se recomienda su lectura.

1) Datos personales: toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

2) Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

3) Autoridad competente: toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, o cualquier otro órgano o entidad a quien el derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública.

4) Responsable del tratamiento: la autoridad competente que sola o conjuntamente con otras determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el derecho de la Unión o del Estado miembro, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el derecho de la Unión o del Estado miembro.

5) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

6) Destinatario: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo al que se le comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades

públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el derecho de la Unión o del Estado miembro; el tratamiento de tales datos por las citadas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

7) Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o acceso no autorizados a datos personales transmitidos, conservados o tratados de otra forma.

8) Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de la persona física de que se trate.

9) Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, con imágenes faciales o datos dactiloscópicos.

10) Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

2.3. Principios relativos al tratamiento de datos personales

Si dirigimos nuestra mirada a los principios relativos al tratamiento de datos personales y en virtud del artículo 4 de la Directiva, estos datos serán tratados de manera lícita y leal; recogidos con fines determinados, explícitos y legítimos; adecuados, pertinentes y proporcionales con los fines para los que son tratados; exactos; conservados de forma que se permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados, y analizados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas. Si lo comparamos con el artículo 5 del Reglamento general de protección de datos, no se aprecian mayores diferencias; se destaca la expresión «minimización de datos» para referirse a que los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Junto con estos principios del artículo 4 de la Directiva, existen otras consideraciones, como la distinción entre datos personales basados en hechos y datos personales basados en apreciaciones personales (art. 7 del mismo texto).

Por otro lado, el artículo 10 de la Directiva contiene el tratamiento de categorías especiales de datos personales. El objeto de este artículo es regular el tratamiento de datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física. En estos supuestos, solamente se permitirá su revelación cuando: a) lo autorice el derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

2.4. Derechos del interesado

2.4.1. Derecho de información que debe ponerse a disposición del interesado y derecho de acceso

Es preciso abordar, a continuación, la regulación de cada uno de los aspectos de los artículos 13, 14 y 15 de la Directiva.

En primer lugar, los Estados miembros dispondrán que el responsable del tratamiento de los datos ponga a disposición del interesado como mínimo la siguiente información:

a) la identidad y los datos de contacto del responsable del tratamiento;

b) en su caso, los datos de contacto del delegado de protección de datos;

c) los fines del tratamiento a que se destinen los datos personales;

d) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma, y

e) la existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o su supresión, o la limitación de su tratamiento. Toda esta información deberá cumplir con la exigencia idiomática, es decir, deberá estar en una lengua comprensible además de tener un contenido mínimo general.

En casos concretos, se podrán facilitar informaciones adicionales tales como:

a) la base jurídica del tratamiento;

b) el plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo;

c) cuando corresponda, las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales, y

d) cuando sea necesario, más información, en particular cuando los datos personales se hayan recogido sin conocimiento del interesado.

Por su parte, el Reglamento general de protección de datos, en sus artículos 13 y 14, también contempla la información que debe ponerse a disposición del interesado o que se le debe proporcionar con un tenor literal muy parecido al de la Directiva, quizás el Reglamento diferencia más explícitamente entre que los datos personales se hayan obtenido o no se hayan obtenido del interesado. Del mismo modo que la Directiva, el Reglamento, en virtud del principio de transparencia, dispone que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y sin dificultades de comprensión, empleando para ello un lenguaje sencillo y, además, esta información podría facilitarse en formato electrónico, por ejemplo, a través de un sitio web. El texto reglamentario también hace hincapié en que no será necesario imponer la obligación de proporcionar información cuando el interesado ya la posea, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado como cuando el tratamiento se realice con fines de archivo en interés público, de investigación científica o histórica o fines estadísticos.

Volviendo a la Directiva, esta norma prevé que los Estados miembros podrán adoptar medidas legislativas por las que se retrase, limite u omita la puesta a disposición del interesado de la información (relacionada anteriormente) siempre y cuando dicha medida sea necesaria y proporcional para evitar que se obstaculicen indagaciones o investigaciones judiciales, para proteger la seguridad pública o los derechos y libertades de otros individuos.

En segundo lugar, y siguiendo el razonamiento teórico del siguiente precepto (14), se establece que los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en caso de que se confirme el tratamiento, acceso a dichos datos personales y la siguiente información:

a) los fines y la base jurídica del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales;

d) cuando sea posible, el plazo contemplado durante el cual se conservarán los datos personales o, de no ser posible, los criterios utilizados para determinar dicho plazo;

e) la existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado;

f) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma, y

g) la comunicación de los datos personales objeto de tratamiento.

Las limitaciones del derecho de acceso están en consonancia con las del derecho de información (evitar que se obstaculicen las indagaciones o investigaciones judiciales, proteger la seguridad pública o los derechos y libertades de otras personas).

2.4.2. Derecho de rectificación o supresión de datos personales

Aquí es importante destacar que los Estados miembros reconocerán el derecho del interesado a obtener del responsable del tratamiento (sin dilación indebida) la rectificación de los datos personales que le conciernan cuando tales datos resulten inexactos. A su vez, los Estados miembros también podrán disponer que el interesado tenga derecho a que se completen los datos personales cuando estos resulten incompletos. El segundo apartado del artículo 16 dispone que los Estados miembros exigirán al responsable del tratamiento suprimir los datos personales (de nuevo, sin dilación indebida).

No se procederá a la supresión y se limitará el tratamiento de los datos personales cuando:

a) el interesado ponga en duda la exactitud de los datos personales y no pueda determinarse esta exactitud o inexactitud o

b) los datos personales hayan de conservarse a efectos probatorios.

Las limitaciones al derecho de rectificación o supresión siguen lo dicho con anterioridad, esto es, para evitar que se obstaculicen las indagaciones o investigaciones judiciales y por protección de la seguridad pública y los derechos o libertados de otros sujetos.

2.4.3. Derechos del interesado en las investigaciones y los procesos penales

Respecto de estos derechos, el artículo 18 de la Directiva presenta la redacción que sigue: los Estados miembros podrán disponer que el ejercicio de los derechos de información, de acceso y de rectificación o supresión se lleve a cabo de

conformidad con el derecho del Estado miembro cuando los datos personales figuren en una resolución judicial o en un expediente tramitado en el curso de un proceso penal.

2.5. Obligaciones del responsable del tratamiento

Capítulo aparte merecen estas obligaciones que se traducen en la aplicación de las medidas técnicas y organizativas (por ejemplo, políticas de protección de datos) oportunas para garantizar que el tratamiento se lleve a cabo acorde con la Directiva (art. 19). En una línea similar, los artículos 24 y siguientes del Reglamento general de protección de datos se ocupan de las obligaciones generales del responsable y encargado del tratamiento. Para demostrar la conformidad con las directrices de la norma, se mantendrán registros de las actividades de tratamiento bajo responsabilidad del responsable o encargado del tratamiento. Este último también deberá evaluar los riesgos inherentes al tratamiento y establecer remedios para prevenirlos. Además, cuando el tratamiento se lleva a cabo con el consentimiento del interesado, este responsable o encargado debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación (el interesado debe ser consciente del acto que está realizando).

Ved también

Para una mayor información, en este apartado nos remitimos a lo estudiado en la asignatura Requisitos legales para el tratamiento de la información personal I.

2.6. Otras disposiciones

Se prevén otras disposiciones como las que regulan el encargado del tratamiento; la seguridad de los datos personales (se recomienda la lectura de los artículos 29 a 31 de la Directiva); el delegado de protección de datos; los principios generales de las transferencias de datos personales a terceros países u organizaciones internacionales (necesarias para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales); las autoridades de control independientes como supervisoras del cumplimiento de lo estipulado por la Directiva; la cooperación y las funciones del Comité Europeo de Protección de Datos (que velará para la aplicación coherente de la Directiva en el conjunto de la Unión), y el derecho a presentar una reclamación (en caso de operación de tratamiento ilícito o de cualquier acto que vulnere las disposiciones nacionales adoptadas de conformidad con la Directiva) ante una autoridad de control y el derecho a percibir una indemnización por los daños y perjuicios sufridos. Asimismo, los Estados miembros reconocerán el derecho que asiste a todo interesado a la tutela judicial efectiva si considera que sus derechos e intereses legítimos se han visto lesionados como consecuencia de un tratamiento ilícito de sus datos. Además, hay que resaltar, aunque sea evidente, que podrán imponerse sanciones a toda persona, física o jurídica, que no cumpla con las exigencias de la Directiva. Los Estados miembros deberán asegurarse de que estas sanciones sean efectivas, proporcionales y disuasorias[7].

[7] «Comentario a la Directiva (UE) 2016/680, de 27 de abril, sobre protección de datos en el ámbito de las infracciones penales» publicado en *Diario La Ley* número 8.756, 6 de mayo de 2016.

3. Las medidas de investigación tecnológicas en el proceso penal

El propósito de este módulo didáctico es ir un poco más allá de la Directiva 2016/680 y analizar una serie de medidas de investigación tecnológicas reguladas en la LECrim y que pueden plantear perplejidades o situaciones controvertidas en lo que a protección de datos e injerencia en la privacidad de las personas se refiere.

La Ley orgánica 13/2015, de 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas y que modifica la LECrim, incorpora nuevas diligencias de investigación como resultado de la proliferación del número de delitos relacionados con el uso de las nuevas tecnologías. Procurando dar respuesta al hecho incontestable de vivir en un entorno virtual en el cual hay toneladas de información digital conservada de múltiples maneras: correos electrónicos, archivos de imagen y audio, programas de computación, etc., frente al que «las autoridades judiciales y policiales encargadas de las investigaciones criminales son sabedoras de esa riqueza informativa almacenada en las diminutas tarjetas o unidades de memoria de los equipos electrónicos» (Ortiz, 2015), resultaba imperativo aprobar lo que era una asignatura pendiente: establecer nuevas medidas de investigación tecnológicas y evitar que la regulación vigente quedara obsoleta y en desuso. Está fuera de toda duda que era necesaria una reforma de estas características porque, además, tal y como expresó el fiscal delegado de Criminalidad Informática, Sr. Víctor Pillado Quintas, en un seminario sobre «La reforma de la justicia penal de 2015», celebrado en la Facultad de Derecho de la Universidad de Girona el día 26 de marzo de 2015, hasta ahora si aparecía una medida de investigación tecnológica, el proceso natural es que primero se enteraba el delincuente, después la policía y, finalmente, el juzgado y la fiscalía, y eso no era nada garantista.

Referencia bibliográfica

J. C. Ortiz Pradillo (2015). «Investigación policial sobre dispositivos electrónicos y control judicial en la reforma de la justicia penal». En: VV. AA. Legalidad y defensa. Garantías constitucionales del derecho y la justicia penal (pág. 288). Castillo de Luna: Ediciones Jurídicas.

Enlace recomendado

Se adjunta un enlace para poder visualizar la grabación de este seminario sobre «La reforma de la justicia penal de 2015» y en el que participaron tres conferenciantes (vídeo cedido por el Centro de Estudios Avanzados del Proceso y de la Justicia de la Universidad de Girona): https://youtu.be/QjIk1s32PDA

Hasta la reforma de 2015, ya existían como diligencias de investigación: la entrada y registro en lugar cerrado (arts. 545 a 572 LECrim), el registro de libros y papeles (arts. 573 a 578 LECrim), y la detención y apertura de la correspondencia escrita o telegráfica (arts. 579 a 588 LECrim). Suponiendo una reforma para el proceso penal, y con la mirada puesta en las nuevas tecnologías, surgen las medidas siguientes: la interceptación de las comunicaciones telefónicas y telemáticas (arts. 588 ter a) a 588 ter m) LECrim); la grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (arts. 588 quater a) a 588 quater e) LECrim); la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (arts. 588 quinquies a) a 588 quinquies c) LECrim); el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a) a 588 sexies c) LECrim), y los registros remotos sobre equipos informáticos (arts. 588 septies a) a 588 septies c) LECrim). Todo

ello precedido de unas disposiciones comunes (art. 588 bis a) LECrim) sobre los criterios de idoneidad (para delimitar el ámbito y duración de la medida), excepcionalidad y necesidad (solo podrá acordarse la medida cuando no estén a disposición de la investigación otras medidas menos gravosas e igualmente útiles para el fin perseguido, o cuando el descubrimiento del hecho delictivo, la determinación de su autor, la averiguación de su paradero o la localización de los efectos del delito se vea gravemente dificultada sin acudir a esta medida) y proporcionalidad (la medida se reputará proporcionada cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros).

Veamos en los próximos epígrafes en qué consisten cada una de estas medidas de investigación tecnológicas y sus presupuestos. Vaya por delante decir que estas medidas tienen una naturaleza excepcional.

3.1. La interceptación de comunicaciones telefónicas y telemáticas

Según el Diccionario de la Real Academia Española, *interceptar* es «apoderarse de algo antes de que llegue a su destino», «detener algo en su camino» o «interrumpir, obstruir una vía de comunicación». Esta interceptación de comunicaciones, regulada en los artículos 588 ter a) a 588 ter m) LECrim, solo podrá ser autorizada cuando la investigación tenga por objeto alguno de los delitos del artículo 579.1 de la LECrim (delitos dolosos castigados con pena con límite máximo de, como mínimo, tres años de prisión; delitos cometidos en el seno de un grupo criminal; delitos de terrorismo) o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

La intervención judicial podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación. El juez deberá motivar su resolución en forma de auto, que contendrá lo que se relaciona a continuación:

a) la identificación del número de abonado, del terminal o de la etiqueta técnica;

b) la identificación de la conexión objeto de la intervención; o

c) los datos necesarios para identificar el medio de telecomunicación de que se trate (art. 588 ter d)). Este mismo precepto sigue estableciendo que, para determinar la extensión de la medida, se valorará alguno de los siguientes aspectos:

a) el registro y la grabación del contenido de la comunicación, con referencia de la forma o tipo de comunicaciones a las que afecta;

b) el conocimiento de su origen o destino;

c) la localización geográfica del origen o destino de la comunicación, y

d) el conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación.

Esta nueva regulación ya empieza desde su inicio a presentar algunos puntos críticos o débiles. En este orden de cosas, el apartado 3 de este artículo 588 ter d) acomete la regulación para los casos de urgencia disponiendo que, cuando las indagaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o terroristas y existan razones justificadas que hagan imprescindible esta medida, podrá ordenarla el Ministerio Fiscal o, en su defecto, el secretario de Estado de Seguridad. La medida se comunicará inmediatamente al juez encargado en el plazo máximo de 24 horas, y este último dispondrá de 72 horas (desde que fue ordenada la medida) para confirmarla o revocarla.

Por otra parte, hay previsto un deber de colaboración por parte de los prestadores de servicios de telecomunicaciones y, en general, de todos los que contribuyan al establecimiento de comunicaciones. La Policía Judicial pondrá a disposición del juez competente la transcripción de los pasajes que considere relevantes y las grabaciones íntegras llevadas a cabo (art. 588 ter f)). La duración máxima inicial de la medida será de tres meses prorrogables por períodos sucesivos de igual duración hasta un plazo máximo de dieciocho meses. Los artículos 588 ter j a 588 ter m regulan la incorporación al proceso de datos electrónicos de tráfico o asociados, por lo que se hace recomendable su lectura.

3.2. La grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

Se podrá autorizar la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado en la vía pública o en otro espacio abierto, en su domicilio u otro lugar cerrado. La escucha y grabación de las conversaciones privadas se podrá completar con la obtención de imágenes cuando se exprese por resolución judicial (arts. 588 quater a) a 588 quater e) LECrim).

En cuanto a los presupuestos de adopción, solamente podrá autorizarse cuando se den los siguientes requisitos:

1) que los hechos que estén siendo investigados sean constitutivos de delitos dolosos castigados con pena de límite máximo de, como mínimo, tres años de prisión; delitos cometidos en el seno de una organización criminal, y delitos de terrorismo; y

2) que pueda racionalmente preverse que la utilización de dispositivos aportará datos esenciales y con efectos probatorios para la causa penal.

Si nos referimos al control de la medida, la Policía Judicial pondrá a disposición de la autoridad judicial competente el soporte original o copia electrónica auténtica de las grabaciones e imágenes, y se complementará con la transcripción de las conversaciones que se consideren especialmente relevantes para los intereses del proceso (art. 588 quater d)).

El artículo 588 quater e) regula el cese de la medida y la necesidad de nueva autorización judicial para la grabación de conversaciones o captación de imágenes que pudieran tener lugar en otros encuentros.

3.3. Los dispositivos técnicos de captación de la imagen, de seguimiento y de localización

La Policía Judicial podrá obtener y grabar imágenes de la persona investigada cuando se encuentre en un espacio público, si ello fuera necesario para facilitar su identificación, para localizar instrumentos del delito u obtener cualesquiera datos relevantes para el enjuiciamiento del ilícito penal. Igualmente, cuando concurran razones de necesidad, el juez podrá acordar la utilización de dispositivos de seguimiento y localización (art. 588 quinquies a) a art. 588 quinquies c)).

Cuando existan razones de urgencia que hagan temer que, de no colocarse inmediatamente el dispositivo técnico de seguimiento y localización (por ejemplo, el sistema de geolocalización de posicionamiento global o GPS), se frustrara la investigación, la Policía Judicial podrá proceder a su colocación e informando en el menor lapso de tiempo posible y, en cualquier caso, en el plazo máximo de 24 horas, a la autoridad competente para que confirme o revoque la medida aplicada.

La duración de la medida será de tres meses prorrogable hasta un máximo de dieciocho meses. Y la Policía Judicial será la encargada de custodiar el material original para evitar su utilización indebida.

No debe quedar en el tintero tampoco que estos dispositivos de seguimiento y localización pueden suponer un considerable ataque a los derechos fundamentales de la persona investigada. El uso de balizas aportará gran cantidad de información sobre una persona, pero también datos de carácter personal. El Tribunal Europeo de Derechos Humanos se ha pronunciado ampliamente sobre esta cuestión. A título indicativo, el conocido caso UZUN contra Alemania, de 2 de septiembre de 2010, en el que se pone de manifiesto que el uso de GPS y balizas policiales puede conllevar una intromisión en la intimidad de la persona investigada y, por consiguiente, una vulneración del artículo 8 del Convenio Europeo de Derechos Humanos. También pueden consultarse las Sentencias Koop contra Suiza, de 25 de marzo de 1998, Kruslin contra Francia y Huvig contra Francia, de 24 de abril de 1990 (Uriarte).

Referencia bibliográfica

L. M. Uriarte Valiente. «Nuevas técnicas de investigación restrictivas de derechos fundamentales». Extraído de la página web de la Fiscalía General del Estado, págs. 22 y sig.

Como lectura complementaria a los apartados 3.2 y 3.3, se recomienda la Sentencia del Tribunal Supremo 329/2016, de 20 de abril, que se pronuncia sobre el empleo de prismáticos por los agentes policiales para observar lo que ocurre en el interior de un domicilio. Se habla de la reforma de la LECrim (arts. 588 quater a) y quinquies a)) y se admite que, aunque la reforma no diga nada sobre el uso de prismáticos, se requerirá autorización judicial al igual que con los dispositivos electrónicos de grabación de imágenes o de las comunicaciones orales directas entre sujetos que están siendo investigados, dado que su injerencia en la intimidad domiciliaria tiene la misma intensidad.

3.4. El registro de dispositivos de almacenamiento masivo de información

Cuando, con ocasión de la práctica del registro domiciliario, sea previsible la incautación de ordenadores u otros dispositivos técnicos, el juez deberá motivar las razones que justifiquen el acceso de los agentes de policía a la información almacenada en estos dispositivos. También existe la posibilidad de acceder a la información de dispositivos incautados fuera del domicilio del investigado (arts. 588 sexies a) a 588 sexies c) LECrim).

La resolución del juez de instrucción autorizando el registro de dispositivos de almacenamiento masivo de información fijará los términos y el alcance del registro y la eventualidad de realizar copias de los datos informáticos. Asimismo, fijará las medidas de aseguramiento de los datos para hacer posible la práctica de una prueba pericial. Se evitará la incautación de los soportes físicos que contengan los datos si ello causa un grave perjuicio a su titular o propietario. Cuando quienes lleven a cabo el registro o dispongan de acceso al sistema de información tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial. Esta ampliación de registro deberá ser autorizada por el juez.

En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida de registro de dispositivos, la Policía Judicial podrá llevar a cabo el examen directo de los datos del dispositivo incautado, notificándolo inmediatamente, y en todo caso dentro del plazo máximo de 24 horas, al juez competente que deberá revocar o confirmar la medida.

Podrá pedirse la colaboración de expertos en el funcionamiento del sistema informático o en las medidas adoptadas para preservar la integridad de los datos informáticos (art. 588 sexies c).

3.5. Los registros remotos sobre equipos informáticos

Otra novedad de gran calado es la contemplada en los artículos 588 septies a) a 588 septies c); se trata de la instalación de un software que permita, de forma remota o telemática, el examen a distancia y sin conocimiento de su titular del contenido de un ordenador, dispositivo electrónico, instrumento de almacenamiento, siempre y cuando se persiga alguno de los siguientes delitos: delitos cometidos en el seno de un grupo criminal, delitos de terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

Otro requisito es que la resolución judicial que autorice el registro remoto deberá especificar todos los instrumentos objeto de la medida, el sistema de acceder a ellos, los agentes encargados, las medidas de aseguramiento de los datos y la autorización para la realización y conservación de copias de los datos. Cuando los agentes policiales tengan razones para creer que los datos buscados están almacenados en otro sistema informático, se lo comunicarán al juez, el cual podrá autorizar una ampliación del registro remoto.

Como ya hemos visto en alguna de las otras medidas, existirá un deber de colaboración por parte de los prestadores de servicio y de los titulares o responsables del sistema informático o base de datos objeto del registro. Un deber de colaboración que también se extiende a facilitar la asistencia necesaria para que los datos e información recopilados puedan ser objeto de examen y visualización. Asimismo, se adoptarán las medidas oportunas para proteger los datos contenidos en el sistema informático.

La medida tendrá una duración máxima de un mes, prorrogable por períodos iguales hasta un máximo de tres meses (Bachmaier, 2017).

En definitiva, en todas estas medidas puede haber una injerencia en el derecho de la privacidad de las personas y una confrontación con el principio de proporcionalidad, pero estas reformas parten de la necesidad de luchar más eficazmente contra la delincuencia y ciberdelincuencia. Ahora bien, hay que actuar con cautela y hacer una ponderación de intereses que tenga en cuenta lo que se persigue con estas medidas y el respeto a los derechos fundamentales de las personas investigadas. Y no debemos perder de vista que estas nuevas medidas de investigación tecnológicas se adoptarán en delitos muy concretos o que lleven aparejada una pena privativa de libertad de, como mínimo, tres años (Bachmaier, 2017, págs. 1-36).

Lectura complementaria

Como lectura complementaria de los registros remotos, se recomienda:

L. Bachmaier Winter (2017). «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley orgánica 13/2015». *Boletín del Ministerio de Justicia* (núm. 2.195).

Lectura complementaria

Se recomienda, como lectura ampliada de todas estas medidas la última edición de: Montero Aroca; Gómez Colomer; Barona Vilar; Esparza Leibar; Etxeberría Guridi. *Manual de Derecho Jurisdiccional III, Proceso Penal*. Tirant Lo Blanch.

4. Obtención de perfiles genéticos de condenados con fines de inclusión en la base de datos policial de ADN

Relacionado con la Directiva 2016/680 y las medidas de investigación tecnológicas, encontramos la obtención de perfiles genéticos de condenados con fines de inclusión en la base de datos policial de ADN. Así que merece que se le dedique un pequeño apartado.

La política de la Unión Europea contra el terrorismo ha supuesto incrementar el número de sistemas de información y bases de datos accesibles para los entes policiales. Los Sistemas de Información de Shengen (SIS y SIS II), el Sistema de Información de Visados (VIS) y la base de datos europea de solicitantes de asilo (Eurodac) desempeñan en la actualidad un papel importante para fines policiales.

Lectura recomendada

Se recomienda, para un mayor conocimiento de esta cuestión, la lectura del artículo siguiente:

C. Blasi Casagran (2015). «Límites del derecho europeo de protección de datos en el control de fronteras de la UE». *Revista CIDOB* (núm. 111, págs. 127-151).

Entrando ya en el asunto concreto que da título a este epígrafe, «obtención de perfiles genéticos de condenados con fines de inclusión en la base de datos policial de ADN», el artículo 129 bis del Código penal, introducido por la Ley orgánica 1/2015 que modifica el Código penal, establece una disposición normativa importante: la toma de muestras biológicas de una persona y la realización del análisis de ADN e inscripción en la base de datos policial. Lo dicho tendrá lugar en el caso de que se trate de condenados por la comisión de un delito grave contra la vida, la integridad de las personas, la libertad, la libertad sexual, de terrorismo o cualquier otro delito grave que conlleve un riesgo grave para la vida, salud o integridad física de las personas y si de las circunstancias del hecho, valoración de su personalidad pueda determinarse que existe un peligro relevante de reiteración delictiva. Únicamente podrán llevarse a cabo los análisis necesarios para la consecución de los identificadores que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo.

Este artículo sigue con un trascendente párrafo segundo que reza como sigue: si el afectado se opusiera a la recogida de las muestras, podrá imponerse su ejecución forzosa mediante el recurso a las medidas coactivas, eso sí, las mínimas indispensables para su ejecución, que deberán ser en todo caso proporcionadas a las circunstancias del caso y respetuosas con su dignidad. Por lo tanto, la obtención de perfiles genéticos es una medida de investigación que se puede adoptar de manera coactiva.

Este artículo seguro que habrá recibido aplausos, pero también despertará algunas reticencias, sin ir más lejos, desde la perspectiva de la protección de datos. No debe perderse de vista que se trata de una base de datos para fines exclusivamente de investigación y de prevención de posibles conductas delictivas reincidentes y darle una atención mediática y una publicidad innecesaria sería un grave error (Solar, 2015).

Referencia bibliográfica

P. Solar Calvo (2015, 11 de noviembre). «El nuevo art. 129 bis CP». *Legal Today*.

Lecturas recomendadas

Se recomiendan dos lecturas para profundizar en este tema: la lectura del artículo de A. Líbano Beristain (2016). «Obtención (coactiva) de perfiles genéticos de condenados con fines de inclusión en la base de datos policial de ADN», en *Revista General de Derecho Procesal* (núm. 38, en línea); y el Acuerdo del Pleno No Jurisdiccional de la Sala Segunda del Tribunal Supremo de 24 de septiembre de 2014.

Actividades

Preguntas cortas:

1. ¿Cuáles son los principales hitos de la Directiva 2016/680?

2. Enumerad y explicad brevemente los derechos del interesado reconocidos por la Directiva 2016/680.

3. Enumerad y explicad brevemente las nuevas medidas de investigación tecnológicas de la LECrim.

Preguntas a desarrollar:

1. Cada vez más datos son considerados por el derecho; por eso se pregunta que especifiquéis la tipología/tipificación de estos datos (según su titularidad, procedencia, información que contienen). Os podéis servir de doctrina y jurisprudencia para la resolución de esta pregunta.

2. Haced un cuadro comparativo entre la Decisión Marco 2008/977/JAI y la Directiva 2016/680.

3. Buscad la Sentencia del Tribunal Supremo número 798/2013, de 5 de noviembre (Ponente, Berdugo Gómez de la Torre) y haced un informe de la misma (valorando los antecedentes de hecho y fundamentos jurídicos, especialmente lo que señala el Tribunal sobre el uso de radiotransmisores o balizas de seguimiento GPS).

4. Haced una valoración personal del artículo 129 bis del Código penal sobre la obtención coactiva de perfiles genéticos de condenados con fines de inclusión en la base de datos policial de ADN.

Bibliografía

AAVV. *Datos. Protección, Transparencia y Buena Regulación*. Documenta Universitaria, 2016.

AAVV. *Derecho Jurisdiccional III, Proceso Penal*. Tirant lo Blanch, última edición.

Armenta Deu, T. *Lecciones de Derecho Procesal Penal*. Marcial Pons.

Bachmaier Winter, L. (2017). «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley orgánica 13/2015». *Boletín del Ministerio de Justicia* (núm. 2.195).

Blasi Casagran, C. (2015). «Límites del derecho europeo de protección de datos en el control de fronteras de la UE». *Revista CIDOB* (núm. 111).

Bosch Moliné, A. «La directiva europea sobre la utilización de datos PNR para la lucha contra el terrorismo y la delincuencia grave». Materiales didácticos UOC.

Etxeberria Guridi, J. F. (2011). «Protección de datos personales y cooperación judicial penal: la Decisión Marco 2008/997/JAI, del Consejo de la UE». En: VV. AA. *Derecho y nuevas tecnologías* (vol. I).

González-Montes Sánchez, J. L. (2015). «Reflexiones sobre el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas». *Revista Electrónica de Ciencia Penal y Criminología*.

Líbano Beristain, A. (2016). «Obtención (coactiva) de perfiles genéticos de condenados con fines de inclusión en la base de datos policial de ADN». *Revista General de Derecho Procesal* (núm. 38).

Marchena Gómez, M.; González-Cuéllar Serrano, N. (2015). *La reforma de la Ley de enjuiciamiento criminal en 2015*. Castillo de Luna: Ediciones Jurídicas.

Ortiz Pradillo, J. C. (2015). «Investigación policial sobre dispositivos electrónicos y control judicial en la reforma de la justicia penal». En: VV. AA. *Legalidad y defensa. Garantías constitucionales del derecho y la justicia penal*. Castillo de Luna: Ediciones Jurídicas.

Rodríguez Lainz, J. L. (2014). «GPS y balizas policiales». *Diario La Ley* (núm. 8.416).

Solar Calvo, P. (2015, 11 de noviembre). «El nuevo art. 129 bis CP». *Legal Today.*

Uriarte Valiente, L. M. «Nuevas técnicas de investigación restrictivas de derechos fundamentales». Extraído de la página web de la Fiscalía General del Estado.

Legislación de referencia:

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L0680).

Decisión Marco 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 (disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:es:PDF).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE «Reglamento general de protección de datos» (disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679).

Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (disponible en: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=uriserv:OJ.L_.2016.119.01.0132.01.SPA).

Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Anteproyecto de Ley orgánica de protección de datos de carácter personal de 23 de junio de 2017.

Real decreto de 14 de septiembre de 1882, aprobatorio de la Ley de enjuiciamiento criminal.

Ley orgánica 13/2015, de 5 de octubre, de modificación de la Ley de enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Ley orgánica 10/1995, de 23 de noviembre, del Código penal.

Ley orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley orgánica 10/1995, de 23 de noviembre, del Código penal.