CNS 43/2020

Dictamen en relación a la consulta formulada por un ayuntamiento sobre la creación de una red supramunicipal para el intercambio de información policial

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito del delegado de protección de datos de un ayuntamiento en el que se pide que la Autoridad emita un dictamen sobre la creación de una red supramunicipal para el intercambio de información policial.

Analizada la petición, y visto el informe de la Asesoría Jurídica, se dictamina lo siguiente.

(...)

II

El Ayuntamiento expone en su consulta que es de su interés crear una red entre las corporaciones locales que utilizan el propio programa informático de gestión policial para compartir, entre cuerpos policiales, la información registrada en este programa a raíz de las actuaciones efectuadas por la policía local .

A continuación, detalla los siguientes aspectos de este sistema de información:

1. Al acceder al sistema deberá indicarse obligatoriamente el motivo de la consulta:

- **Requerimiento/apoyo judicial.**
- **Prevención y seguridad ciudadana.**

2. Para cada acceso se registrará la identificación del usuario, la fecha y la hora en la que se realiza el acceso, los datos consultados y el motivo de la consulta.

3. La información a consultar/intercambiar del sistema será la siguiente:

- **Personas físicas: nombre y apellidos; nº. DNI/NIE/Pasaporte o documento extranjero; sexo; fecha de nacimiento; lugar de nacimiento; nacionalidad; fecha de defunción (en su caso); sobrenombre; nombre del padre y la madre; domicilio/s; teléfono/s; correo/s electrónico/s; fecha creación/modificación del registro; módulo del programa de gestión con el que está relacionada la persona (novedad diaria, accidente de tráfico, atestado, citación judicial, etc.).**

- **Personas jurídicas: nombre comercial; CIF; actividad; domicilio/s; teléfono/s; correo/s electrónico/s; datos persona/s de contacto; fecha creación/modificación del registro; módulo del programa de gestión con el que está relacionada la entidad o empresa.**

- **Vehículos: matrícula; marca; modelo; bastidor; tipos de vehículo; seguro; datos de la persona propietaria; módulo del programa de gestión con el que está relacionado.**

- **Tenencia de animales: microchip; tipo microchip; nombre del animal; especie animal; raza; peligrosidad; fecha nacimiento; fecha de defunción (en su caso); datos de la persona propietaria.**

El Ayuntamiento manifiesta tener formalizado con la empresa propietaria del programa informático de gestión policial el correspondiente contrato de encargado del tratamiento. También que se está llevando a cabo un análisis de riesgos y que se prevé, en su caso, la realización de una evaluación de impacto.

A todo ello, plantea si el sistema de acceso, consulta e intercambio de información para las corporaciones locales que se adhirieran voluntariamente a este sistema de información policial, en los términos expuestos, cumple con la normativa vigente sobre protección de datos personales.

III

Para dar respuesta a la consulta efectuada, es necesario analizar, de entrada, cuál sería la normativa de protección de datos aplicable.

El 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 se refiere al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), no resulta aplicable a los tratamientos que se llevan a cabo en el ámbito policial y judicial penal, según se desprende del artículo 2.2.d) del RGPD, que dispone lo siguiente:

> **"2. El presente Reglamento no se aplica al tratamiento de datos personales:**
> **(...) d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."**

En este ámbito es necesario tener en consideración la Directiva (UE) 2016/680 del Parlamento y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en cuanto al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, búsqueda, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, ya la libre circulación de estos datos y por la que se deroga la Decisión marco 2008/977/J

Los estados miembros de la Unión Europea debían transponer la Directiva (UE) 2016/680 antes del 6 de mayo de 2018.

Dada la falta de transposición de esta Directiva por parte de España, en el caso que nos ocupa es necesario tener en cuenta las previsiones de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGGD), que en la disposición transitoria cuarta establece lo siguiente:

> **"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, ya la libre circulación de dichas datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, seguirán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva."**

Por tanto, en este caso hay que tener presente las previsiones de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y las disposiciones que la desarrollan.

IV

En la consulta se plantea la posible creación de un sistema supramunicipal de información policial que permita al cuerpo policial de las corporaciones locales que se adhieran voluntariamente consultar y, por tanto, intercambiar información de interés policial.

En este sistema, por la información de que se dispone, se incorporará la información de la que dispone cada policía local como consecuencia del ejercicio de sus funciones (tanto a raíz de servicios planificados, como requerimiento de los ciudadanos), la cual incluye datos personales y que el cuerpo policial gestiona a través de un programa informático llamado DRAG, creado por una empresa privada.

Más allá de esto, en la consulta no queda claro el papel de los distintos agentes implicados en este sistema de información. En cualquier caso, ya falta de información más precisa sobre el modelo que se quiere adoptar, la finalidad pretendida podría alcanzarse a través de varios modelos organizativos alternativos.

De acuerdo con el artículo 3.d) de la LOPD, se entiende por "responsable del fichero o tratamiento" la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

En la consulta se apunta que el Ayuntamiento "tiene interés en crear una red entre las corporaciones locales que utilizan el propio programa DRAG", manifestación de la que podría desprenderse que esta corporación local asume la posición de responsable del sistema de información y , por tanto, de responsable del tratamiento.

Tampoco se podría descartar que nos encontráramos ante un supuesto de corresponsabilidad, esto es que las diferentes corporaciones locales que disponen de este programa informático de gestión de información policial (DRAG) acuerden y participen conjuntamente en la creación del nuevo sistema de información policial, por tanto, en la definición de los fines y medios del tratamiento.

Si bien el término de corresponsables del tratamiento no se encuentra definido expresamente en la LOPD, sí se refiere el artículo 5.1.q) del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), al definir el responsable del tratamiento como la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.".

En cualquier caso, esta figura sí se encuentra recogida en la Directiva 2016/680, que debe ser objeto de transposición al ordenamiento jurídico español.

El artículo 21 de la Directiva dispone que:

> **"1. Los Estados miembros dispondrán de que, cuando dos o más responsables del tratamiento determinen conjuntamente los objetivos y los medios de tratamiento, sean considerados corresponsables del tratamiento. Determinarán, de modo transparente y de mutuo acuerdo, cuáles serán sus responsabilidades respectivas en el cumplimiento de la presente Directiva, en particular por lo que se refiere al ejercicio de los derechos del interesado ya sus respectivas obligaciones en el suministro de la**

> **información contemplada en el artículo 13, salvo y en la medida en que las responsabilidades respectivas de los responsables se rijan por el Derecho de la Unión o del Estado miembro a que estén sujetos los responsables del tratamiento. El citado acuerdo designará el punto de contacto para los interesados. Los Estados miembros podrán designar cuál de los corresponsables puede actuar como punto único de contacto para el interesado por lo que respecta al ejercicio de sus derechos. 2. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los Estados miembros podrán disponer que el interesado pueda ejercer los derechos que le reconocen las disposiciones adoptadas conforme a la presente Directiva respecto a cada uno de los responsables y frente a ello."**

Por tanto, de tratarse el presente caso de un supuesto de corresponsabilidad, sería conveniente tener en cuenta lo que se establece en este precepto, sin perjuicio de lo que pueda establecerse en la futura norma de transposición.

Sea como fuere, advertir que la responsabilidad en estos casos abarcaría sólo a la información policial incorporada al nuevo sistema de información, no así a la información de la que dispone cada corporación local en los respectivos sistemas de información de gestión policial. En este caso, cada policía local sería responsable del tratamiento de la información generada por sus actuaciones, sin perjuicio de que, una vez incorporada al nuevo sistema, pase a formar parte de la responsabilidad del Ayuntamiento consultante (o, en su caso , del conjunto de entes locales participantes (caso de corresponsables)).

En cuanto a la empresa creadora del programa informático de gestión policial DRAG, en la consulta se señala que se cuenta con el correspondiente contrato de encargo del tratamiento, el cual comprende "cláusulas contractuales con los contenidos generales del régimen jurídico de encargo y los contenidos específicos de este tipo de encargo del tratamiento".

Por tanto, dicha empresa ostentaría en el presente caso la condición de encargada del tratamiento (artículo 3.g) LOPD), entendida como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

Más allá de que este contrato de encargo del tratamiento deba adecuarse a las previsiones del artículo 12 de la LOPD, mientras no entre en vigor la norma que transponga al derecho español la Directiva 2016/680, se recomienda tener también cuenta lo establecido en el artículo 22 de esta Directiva.

Una tercera posibilidad podría ser que nos encontráramos frente a un modelo organizativo descentralizado. En este caso, cada corporación local sería responsable del tratamiento de la información generada por sus actuaciones y que gestiona a través del programa informático DRAG, y el sistema de información propuesto sólo sería un mecanismo o medio para facilitar el envío de la información que en un determinado momento pueda requerir un cuerpo de policial local a otro cuerpo de policía local para el ejercicio de sus funciones.

En cualquier caso, la definición de cuál es el papel de las diferentes administraciones intervinientes, decisión que deben tomar las entidades implicadas, se convierte en un elemento esencial para determinar las obligaciones y las responsabilidades que pueden corresponder a cada una de las administraciones implicadas.

V

Dicho esto, tanto la creación de este sistema de información policial como los flujos informativos que se produzcan a partir de su puesta en funcionamiento deben situarse en el marco norma

aplicable a la actuación de la policía local, a fin de considerarlos legítimos desde el punto de vista de la protección de datos personales.

De acuerdo con la LOPD, la creación de ficheros policiales, así como el tratamiento y comunicación de sus datos, se encuentra restringida a las administraciones públicas que tienen atribuidas competencias en materia de seguridad pública (artículos 22), entre las cuales , las corporaciones locales.

En este sentido, la Ley orgánica 2/1986, de 13 de marzo, reguladora de las Fuerzas y Cuerpos de Seguridad del Estado (LOFCSE), dispone que:

> **"Artículo primero.**
> **1. La Seguridad Pública es competencia exclusiva del Estado. Su mantenimiento corresponde al Gobierno de la Nación.**
> **2. Las Comunidades Autónomas participarán en el mantenimiento de la Seguridad Pública en los términos que establezcan los respectivos Estatutos y en el marco de esta ley.**
> **3. Las Corporaciones Locales participarán en el mantenimiento de la seguridad pública en los términos establecidos en la Ley Reguladora de las Bases de Régimen Local y en el marco de esta ley.**
> **4. El mantenimiento de la Seguridad Pública se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad."**

La LOFCSE regula en términos generales a las policías locales (Título V) y las considera como un cuerpo de seguridad más junto a la policía estatal y autonómica (artículo 2). Asimismo, concreta unas funciones comunes para todas las Fuerzas y Cuerpos de Seguridad (artículo 11).

La Ley 16/1991, de 10 de julio, de las policías locales (LPL) incorpora a este conjunto de funciones en su texto legal.

Así, de acuerdo con el artículo 11 de la LPL, corresponde a las policías locales que dependen de los municipios de Cataluña, en su ámbito de actuación, las siguientes funciones:

> **"a) Proteger a las autoridades de las corporaciones locales y vigilar y custodiar los edificios, instalaciones y dependencias de estas corporaciones. b) Ordenar, señalizar y dirigir el tráfico en el casco urbano, de acuerdo con lo que establecen las normas de circulación. c) Instruir atestados por accidentes de circulación acaecidos dentro del núcleo urbano, en cuyo caso comunicarán las actuaciones llevadas a cabo a las fuerzas o cuerpos de seguridad competentes. d) Ejercer de policía administrativa, a fin de asegurar el cumplimiento de los reglamentos, ordenanzas, bandos, resoluciones y demás disposiciones y actos municipales, de acuerdo con la normativa vigente. e) Ejercer de policía judicial, de acuerdo con el artículo 12 y con la normativa vigente. f) Llevar a cabo diligencias de prevención y actuaciones destinadas a evitar la comisión de actos delictivos, en cuyo caso comunicarán las actuaciones llevadas a cabo a las fuerzas o cuerpos de seguridad competentes. g) Colaborar con las fuerzas o cuerpos de seguridad del Estado y con la Policía Autonómica en la protección de las manifestaciones y en el mantenimiento del orden en grandes concentraciones humanas cuando sean requeridas para ello. h) Cooperar en la resolución de los conflictos privados, cuando sean requeridas para ello. i) Vigilar los espacios públicos. j) Prestar auxilio en accidentes, catástrofes y calamidades públicas, participando, de acuerdo con lo dispuesto en las leyes, en la ejecución de los planes de protección civil.**

k) Velar por el cumplimiento de la normativa vigente en materia de medio ambiente y de protección del entorno. l) Llevar a cabo las actuaciones destinadas a garantizar la seguridad vial en el municipio. m) Cualquier otra función de policía y de seguridad que, de acuerdo con la legislación vigente, les sea encomendada."

Por tanto, las policías locales de los ayuntamientos (con la denominación de policía local, policía municipal, guardia urbana u otras tradicionales) quedan legitimadas para llevar a cabo los tratamientos de datos personales que requieran para el ejercicio de las funciones legalmente encomendadas.

Con respecto a la posibilidad de compartir este tipo de información, es preciso tener presente que la legislación aplicable prevé una obligación de colaboración entre las Fuerzas y Cuerpos de Seguridad del Estado para el ejercicio y desarrollo del conjunto de funciones que tienen atribuidas, que abarca también el deber de comunicar aquella información que pueda resultar relevante y necesaria a tal efecto.

Al respecto, el LOFCSE dispone que "los miembros de las Fuerzas y Cuerpos de Seguridad ajustarán su actuación al principio de cooperación recíproca y su coordinación se efectuará a través de los órganos que a tal efecto establece esta Ley" (artículo 3).

También que "los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos de Policía de las Comunidades Autónomas deberán prestarse mutuo auxilio e información recíproca en el ejercicio de sus funciones respectivas" (artículo 45 LOFCSE).

De acuerdo con la Ley 4/2003, de 7 de abril, de ordenación del sistema de seguridad pública de Cataluña, la policía de la Generalidad-mozos de escuadra y las policías de los ayuntamientos constituyen la policía de las instituciones propias de Cataluña (artículo 5).

Esta misma Ley 4/2003 regula los principios a los que deben atenerse las administraciones públicas con competencias sobre seguridad, entre los que destaca el de "información recíproca, especialmente cuando sea necesario para cumplir mejor las competencias de cada administración" (artículo 21.b)).

En este sentido, la Ley dispone que "las autoridades y los miembros del cuerpo de la policía de la Generalidad-mozos de escuadra y de los cuerpos de policía local de Cataluña están obligados a facilitarse mutuamente la información que sea relevante para el cumplimiento de las funciones respectivas, sin perjuicio de la reserva que proceda por razón de la materia y con pleno respeto de la legislación aplicable, en particular la relativa a la protección de datos personales" (artículo 23.1 Ley 4/2003).

También debe tenerse presente que la propia LOPD legitima las comunicaciones de datos personales que tengan lugar entre administraciones públicas cuando éstas tienen por finalidad el ejercicio de competencias idénticas o que versen sobre una misma materia.

En concreto, el artículo 21.1 de la LOPD establece que "los datos de carácter personal recogidos o elaborados por las administraciones públicas para el ejercicio de sus atribuciones no deben ser comunicados a otras administraciones públicas para el ejercicio de competencias distintas o de competencias cuando traten materias distintas, excepto cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos". El apartado 4 del mismo artículo establece que "en estos casos no es necesario el consentimiento del afectado".

En este sentido, el artículo 10.4.c) del RLOPD complementa la regulación legal señalando que no será necesario el consentimiento del interesado cuando la cesión entre administraciones

públicas se realice "para el ejercicio de competencias idénticas o que versen sobre las mismas materias".

Apuntar que, a efectos de facilitar el intercambio de información entre cuerpos policiales, la Ley 4/2003 prevé que el departamento titular de las competencias en materia de seguridad pública debe gestionar y mantener un sistema unificado de informaciones policiales, al que tienen acceso el cuerpo de los Mossos d'Esquadra y las policías locales de Cataluña, previendo la misma Ley que mediante convenio de adhesión bilateral se regulen las condiciones del acceso y la participación de cada cuerpo de policía local (artículo 24.2).

También que el cuerpo de Mossos d'Esquadra debe facilitar el acceso de las policías locales a otras bases de datos, en los supuestos de interés local que se determinen por reglamento (artículo 24.3 Ley 4/2003).

Y, en lo que se refiere al programa informático de aplicación del cuerpo de Mossos d'Esquadra, que mediante convenio se ha de prever que las policías locales puedan usarlo, así como el trabajo en redes integradas de información policial (artículo 24.4 ley 4/2003).

En la consulta se apunta que el sistema de información que se pretende crear "no interfiere en el tratamiento de la información entre policías por medio del SIP o de otros sistemas de información compartidos", esto es el sistema unificado de información policial a que se refieren las previsiones mencionadas de la Ley 4/2003.

Se trata, se sostiene en la consulta, de un sistema "complementario y en ningún caso se dejará de cargar o compartir la información necesaria u obligatoria en el SIP para poder llevar a cabo las funciones y tareas policiales reguladas por las leyes."

Hacer notar, en este punto, que la Ley 4/2003 dispone que "el Gobierno, por medio del departamento titular de las competencias en materia de seguridad pública, tiene la responsabilidad de hacer efectiva la coordinación de las policías locales, que implica la determinación de los medios y de los sistemas de relación que hacen posible la acción conjunta de estos cuerpos, mediante las autoridades competentes, de forma que se consiga la integración de las respectivas actuaciones particulares dentro del conjunto del sistema de seguridad que les es confiado" (artículo 25.1).

También la LPL dispone que "a efectos de esta Ley, se entiende por "coordinación" la determinación de los medios y de los sistemas de relación que hacen posible la acción conjunta de las policías locales, mediante las autoridades competentes, de modo que se consiga la integración de las respectivas actuaciones particulares dentro del conjunto del sistema de seguridad ciudadana que les es confiado" (artículo 14).

Al respecto, el artículo 15 de la LPL concreta que:

> "1. La coordinación de la actividad de las policías locales puede extenderse, en todo caso, a las siguientes funciones: a) Promover la homogeneización de los medios técnicos y la uniformidad de los demás elementos comunes.
>
> b) Establecer los instrumentos y medios que hagan posible un sistema de información recíproca. (...)."

Visto esto, si bien podría decirse que, desde la vertiente de la protección de datos, existiría suficiente cobertura legal para el intercambio, entre cuerpos de policía local, de esa información personal que pueda ser de interés para el ejercicio de las funciones que legalmente tienen atribuidas, la creación de un sistema de información como el que se propone en la consulta parece que requeriría de la

intervención del departamento competente en materia de seguridad pública de la Administración de la Generalidad.

En cualquier caso, hacer notar que, desde el punto de vista de la protección de datos personales, es necesario velar por que cualquiera de estas comunicaciones de información policial, aparte de contar con legitimación suficiente, se adecuen, entre otros , al principio de calidad de los datos (artículo 4 LOPD).

Este principio, en su vertiente de limitación de la finalidad y minimización de datos, exige que los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, no siendo posible su tratamiento posterior de forma incompatible con estos fines, y deben ser adecuadas, pertinentes y limitadas a lo necesario para alcanzar estos fines que justifiquen su tratamiento.

Hay que tener en consideración, por tanto, que los accesos o comunicaciones de datos que tengan lugar a raíz de la puesta en funcionamiento del presente sistema de información sólo podrán considerarse adecuados a la normativa de protección de datos en la medida en que se limiten a los datos personales que cada cuerpo de la policía local requiera para el ejercicio de las funciones que, de conformidad con la legislación aplicable, sean de su competencia, y siempre que estos datos sean necesarios, pertinentes y adecuados en cada caso.

Este mismo principio, en su vertiente de exactitud de los datos, también exige que los datos personales sean exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Por este motivo, es también necesario prever mecanismos que garanticen la calidad de la información personal incorporada en el sistema de información policial, de modo que los datos que se traten sean exactos y actualizados en todo momento, cuestión que podría verse dificultada si se produjera la coexistencia de sistemas de información paralelos con objetivos coincidentes, aunque sólo sea parcialmente.

VI

Por otra parte, en cuanto a la implementación del sistema de información, recuerda la necesidad de adoptar las medidas de carácter técnico y organizativo necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que están expuestos, tanto si proceden de la acción humana o del medio fí

Al respecto, recordar que el nuevo marco europeo regulador del derecho a la protección de datos personales (tanto la Directiva 2016/680 como el RGPD) configura un sistema de seguridad que se basa en determinar, a raíz de una previa valoración de los riesgos , qué medidas técnicas y organizativas deben aplicarse para garantizar los niveles de seguridad adecuados al rie

Este nuevo modelo se fundamenta en el principio de responsabilidad proactiva de modo que no sólo debe cumplirse la norma, sino que también debe poderse demostrarlo, y en la protección de los datos desde el diseño y por defecto, de tal forma que tanto en el momento de definir las diferentes operaciones de tratamiento, como a la hora de determinar y aplicar los medios que se utilizarán para tratar los datos personales, se tendrán en cuenta los principios, derechos y obligaciones que recoge la normativa de protección de datos personales que sea de aplicación a los tratamientos que se pretende llevar a cabo.

Por tanto, es necesario realizar este análisis de riesgos con carácter previo a la puesta en funcionamiento del sistema de información para determinar las medidas de seguridad técnicas y organizativas apropiadas para salvaguardar el derecho a la protección de datos de los posibles

afectados.

Apuntar, en relación con la determinación de estas medidas, que el esquema de medidas de seguridad previsto en el RLOPD, si bien en estos momentos sería de obligado cumplimiento, podría no ser suficiente una vez se transponga la Directiva 2016/680 . En algunos supuestos este esquema podrá seguir aplicándose, si del análisis de riesgos previo se concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado al caso concreto, pero en otros puede ser necesario completarlas con medidas adicionales fruto del análisis de riesgos.

En la consulta se hace referencia expresa a la implementación de un registro de accesos, de modo que, para cada acceso, se prevé registrar el nombre del usuario del sistema, el día y hora del acceso, las datos consultados y el motivo de la consulta.

Más allá de valorar positivamente la implementación de esta medida de seguridad, recuerda la necesidad de evaluar la adopción de otras medidas adicionales, como por ejemplo el establecimiento de mecanismos apropiados que permitan la correcta identificación y autenticación de los usuarios del sistema información a efectos de garantizar que no se producirán tratamientos no autorizados, entre otros.

Hay que tener presente, visto el artículo 29.2 de la Directiva 2016/680 (a la espera de la norma de transposición), que las medidas de seguridad a implementar en un caso como el que se examina deberían ir dirigidas a todo caso en:

> **a) denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento (control de acceso a los equipamientos); b) impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas (control de los soportes de datos); c) impedir que se introduzcan sin autorización datos personales conservados, o que éstos puedan inspeccionarse, modificarse o suprimirse sin autorización (control del almacenamiento); d) impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas mediante instalaciones de transmisión de datos (control de los usuarios); e) garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado sólo puedan tener acceso a las datos personales para las que han sido autorizadas (control del acceso a las datos); f) garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse oa cuya disposición pueden ponerse las datos personales mediante equipamientos de comunicación de datos (control de la transmisión); g) garantizar que pueda verificarse y constatarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado y en qué momento y por qué persona han sido introducidos (control de la introducción); h) impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, las datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte); e) garantizar que los sistemas instalados puedan restablecerse en caso de interrupción (restablecimiento); j) garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que las datos personales almacenados no se degraden por fallos de funcionamiento del sistema (integridad).”**

También, es necesario decir, sería necesaria la adopción y la implantación de medidas de formación del personal que debe tratar los datos personales en cuestión.

En todo caso, recuerda que estas medidas de seguridad deberían ajustarse al Esquema Nacional de Seguridad (artículo 1 Real Decreto 3/2010, de 8 de enero).

De acuerdo con las consideraciones hechas hasta ahora en relación con la consulta planteada, se hacen las siguientes,

Conclusiones

Es necesario definir las responsabilidades de los distintos agentes implicados en la implementación de este sistema de información para determinar las obligaciones y las responsabilidades de cada uno de ellos.

Existe habilitación para el intercambio de información entre los diferentes cuerpos policiales, siempre de acuerdo con la coordinación hecha por el Departamento competente en materia de policías locales, pero es necesario respetar el principio de calidad de los datos, el principio de exactitud y, previo análisis de riesgos, determinar las medidas de seguridad adecuadas para garantizar los derechos de las personas afectadas.

Barcelona, 30 de noviembre de 2020