Estrasburgo, 15 de febrero de 2018 T-PD(2018)01

COMITÉ CONSULTIVO DEL CONVENIO PARA LA PROTECCIÓN DE PERSONAS EN RELACIÓN AL TRATAMIENTO AUTOMATIZADO DE DATOS PERSONALES

Guía práctica sobre el uso de datos de carácter personal en el sector policial[1]

Dirección General de Derechos Humanos y Estado de Derecho

Introducción

[1] La presente guía tiene base en el esbozo de pautas preparado por David Allen (experto británico en la Policía), Evelien van Beek (experta holandesa en protección de datos) y John Borking (técnico y experto holandés en protección de datos)

La Recomendación (87)15, que regula el uso de datos personales en el sector policial, proporciona un conjunto general de principios a aplicar para asegurar el respeto del derecho a la vida privada y la protección de datos que se exponen en el artículo 8 del Convenio Europeo de Derechos Humanos en relación al Tratamiento Automatizado de Datos Personales («Convenio 108»).

La Recomendación (87)15 ha pasado por varias evaluaciones (en 1993, 1998 y 2002) que analizaron su aplicación y pertinencia. En 2010, el Comité Consultivo del Convenio 108 decidió llevar a cabo un estudio[2] en toda Europa sobre la utilización de datos personales por parte de la Policía. Dicha evaluación destacó que los principios de la Recomendación (87)15 continuaban proporcionando una base sólida para la elaboración de legislación acerca del tema a nivel nacional y que la preparación de una guía práctica sobre el uso de datos personales por parte de la Policía, con base en los principios de la Recomendación (87)15, proporcionaría orientación con respecto a lo que los principios implican a un nivel operativo.

Por tanto, se redactó la presente guía para destacar los aspectos más importantes que pueden surgir en el uso de datos personales en el sector policial y para resaltar los elementos clave a considerar en dicho contexto.

La presente no repite las disposiciones del Convenio 108 ni las de la Recomendación (87)15, sino que se concentra en la orientación práctica.

[2] Véase Informe «Twenty-five years down the line», de Joseph A. Cannataci

Los principios rectores expuestos en la Recomendación (87)15 y sus implicancias prácticas apuntan a asegurar que, en lo concerniente al uso policial de datos de carácter personal, se alcance un equilibrio entre los objetivos esenciales de interés general público y el respeto por los derechos de las personas a la privacidad y la protección de datos.

Cabe destacarse que la guía pretende proporcionar orientación para situaciones prácticas que la Policía puede enfrentar en su operativa diaria y reconoce que la recopilación y el uso lícitos de datos personales para la aplicación de la ley son cruciales para los intereses de la seguridad nacional y la prevención del delito o el mantenimiento del orden público. Mediante ejemplos concretos, enfatiza que la prevención y supresión del delito, incluso a través de la recolección y el uso de datos de carácter personal para la aplicación de la ley, pueden llevarse a cabo de manera eficiente y de acuerdo con la ley.

Con el objeto de facilitar la lectura de la guía, al final del presente documento se proporciona un glosario de los términos utilizados.

Consideraciones generales

La recopilación y el uso de datos personales con finalidades policiales constituyen una injerencia en el derecho a la vida privada y la protección de datos propuestos en el artículo 8 del Convenio Europeo de Derechos Humanos y el Convenio 108 y, por tanto, deben basarse en el Derecho (claro, previsible y asequible), perseguir una finalidad legítima y limitarse a lo necesario y proporcionado para conseguir dicha finalidad legítima.

Todo tratamiento de datos debe cumplir con los principios de necesidad, proporcionalidad y limitación de la finalidad. Esto implica que, para la Policía, el tratamiento de datos de carácter personal debe basarse en finalidades predefinidas, claras y legítimas, expresadas en la ley. Debe ser necesario y proporcionado a dichas finalidades legítimas y no debe llevarse a cabo de manera incompatible con ellas. El tratamiento de datos debe realizarse de manera lícita, imparcial y transparente. Además, los datos personales en posesión de la Policía deben ser adecuados, pertinentes y no deben ser excesivos en relación con la finalidad para la cual se hubieren obtenido. Por último, deben ser precisos y estar actualizados, para garantizar la mejor calidad de datos posible.

1. Alcance

Los principios que se explican en la presente guía atañen al tratamiento de datos de carácter personal para las siguientes finalidades policiales: prevención, investigación y enjuiciamiento de infracciones penales y la ejecución de sanciones penales. Esto incluye el mantenimiento del orden público por parte de la Policía (en lo sucesivo, «finalidades policiales»). Cuando el texto se refiere a «Policía», puede interpretarse fuerzas de orden público en un sentido más amplio, a

saber: fiscalías u otros órganos públicos o privados autorizados por ley para tratar datos de carácter personal con las mismas finalidades.

2. Recopilación y uso de datos

La Policía, en su calidad de responsable del tratamiento de datos, responderá tanto del tratamiento de datos que lleva a cabo, como de sus operaciones de tratamiento de datos.

La recopilación de datos personales con finalidades policiales debe limitarse a lo necesario y proporcionado para la prevención de un peligro real o la prevención, investigación y el enjuiciamiento de una infracción penal específica. Toda excepción a dicha disposición debe estar sujeta a la legislación nacional específica.

Del punto 2.1 de la Recomendación, se desprende que, para la consecución de las dos principales tareas policiales (prevención de un peligro real y supresión de una infracción penal específica), debe existir una correlación evidente y directa entre el tratamiento de datos llevado a cabo por la Policía y una situación donde las personas ya cometieron un delito o es probable que lo hagan.

La Policía siempre debe seleccionar la base jurídica adecuada para tratar datos personales y debe hacerlo de manera lícita. Asimismo, debe llevar a cabo una evaluación concienzuda con el fin de asegurarse de que el tratamiento tiene base en una legislación apropiada y los procedimientos para el tratamiento de datos previstos en ella se respetan por completo.

En todos los estadios del tratamiento, la Policía debe aplicar los principios de protección pertinentes (sobre todo, los de necesidad, proporcionalidad y tratamiento de datos orientado a

la finalidad) y no debe continuar tratando datos innecesarios para dicha finalidad. En este contexto, los datos personales recopilados en una etapa temprana de la investigación, y que luego resultan no ser pertinentes en el decurso de ella, deben dejar de ser tratados (por ejemplo, si se confirma la inocencia de un sospechoso) y, por tanto, deben ser bloqueados o eliminados. Esto no procede si se permite la utilización posterior de los datos (Punto 3).

Para los fines de la presente guía, la utilización posterior de datos se considera una nueva operación de tratamiento de datos, que debe cumplir con los criterios y las condiciones antes mencionados. La utilización posterior de datos debe ser lícita y llevarse a cabo para una finalidad legítima, necesaria y proporcionada a dicha finalidad.

Antes y durante la recopilación de datos, siempre debe considerarse si los datos recopilados son necesarios para la investigación o una tarea policial, como se describe en el Punto 1. Debe notarse que, una vez recopilados los datos personales, debe existir una relación clara entre la persona cuyos datos se están tratando y la finalidad de dicho tratamiento, esto es, una investigación o tarea policial específica. Dicha relación, así como el cumplimiento con los principios de protección de datos descripto en la presente guía, siempre deben ser demostrables. Luego de la fase de recopilación, y en diferentes etapas de la investigación, resulta necesario llevar a cabo un análisis concienzudo con la finalidad de evaluar cuáles datos deben retenerse y cuáles eliminarse.

De acuerdo con el principio de responsabilidad demostrada, la Policía, al igual que a otros responsables del tratamiento de datos, es responsable del tratamiento de datos que lleva a cabo. Ello implica que debe poder demostrar en todo momento que las actividades de

tratamiento cumplen con la normativa de protección de datos. Asimismo, requiere que la Policía implemente de manera activa medidas para salvaguardar y promover la protección de datos en todas sus actividades.

Antes de recopilar datos personales, los investigadores deben preguntarse: « ¿Por qué es necesario recopilar los datos? ¿Qué es exactamente lo que se pretende lograr?».

Ejemplo:

Para datos personales tales como la facturación del servicio telefónico: solo se deberían procurar los números requeridos para los períodos que se investigan y solo para aquellas personas sospechosas de estar conectadas con el delito.

Se puede recopilar una lista de números telefónicos relacionados con el delito sospechado si existen indicios de que tales datos cumplen con la finalidad de la investigación. No se puede conservar o tratar luego de que el análisis demuestre que los datos no son estrictamente necesarios para la finalidad de la investigación.

Es muy recomendable establecer una clara distinción en cómo la Policía trata datos de carácter personal relacionados con diferentes categorías de personas, por ejemplo: sospechosos, personas condenadas por delitos, víctimas y terceras partes, tales como testigos. Ello también debería guardar relación con la finalidad específica para la que los datos se recopilaron.

De acuerdo con el principio de limitación de la finalidad, los datos personales recopilados para finalidades policiales deben usarse solamente para dichas finalidades y no para ninguna otra que sea incompatible con la finalidad original que se declaró al momento de la recopilación. Además, deben ser necesarios y proporcionados a las finalidades policiales, a menos que se prevea en la ley.

Durante todas las etapas del tratamiento de datos y la utilización posterior mencionada en las Consideraciones Generales, la Policía debe asegurarse de que los datos sean precisos, estén actualizados, sean adecuados, pertinentes y no sean excesivos con relación a las finalidades para los que son tratados.

Ejemplo:
Los datos policiales recopilados para una investigación donde la afiliación política es irrelevante no pueden usarse para determinar la afiliación política de la persona en cuestión, a menos que esté previsto en la ley.

3. Utilización posterior de datos

Con excepción del tratamiento para el que los datos fueron recopilados originalmente, todo tratamiento posterior de datos para finalidades policiales debe cumplir con los requisitos legales para el tratamiento de datos de carácter personal: debe estar previsto por ley, debe tender a un fin legítimo y debe ser necesario y proporcionado a dicho fin.

Sin perjuicio del tratamiento de datos computarizado y/o automatizado y el gran volumen de datos personales a menudo almacenado en diferentes entornos de tratamiento, los datos personales recopilados y retenidos para finalidades policiales no deben mantenerse y tratarse para finalidades inespecíficas o generales o de manera que no cumpla con el principio de limitación de la finalidad.

Además, debe notarse que la utilización posterior de datos personales con relación a personas vulnerables, tales como víctimas, menores o quienes gocen de protección internacional, deben someterse a un análisis jurídico y cuidado adicional con especial atención a la aplicación de los principios de necesidad y proporcionalidad.

En casos como los de trata de personas, narcotráfico o explotación sexual, o donde los datos de las víctimas también pueden utilizarse posteriormente cuando se las considera sospechosas, o cuando la protección de víctimas de un crimen más severo puede superar al interés de perseguir crímenes menos severos, resulta recomendable que la Policía aumente el intercambio de información sobre el tema dentro de organismos policiales internacionales o regionales. Si se cumple con todos los requisitos legales, como se dispone en el Punto 2, no debería obstaculizar la utilización de datos de dichas personas para la finalidad policial, pero deben respetarse las normas de confidencialidad en dichos intercambios.

Ejemplo:

Los datos recopilados de un titular de datos para finalidades fiscales solo pueden ser tratados por la Policía para mantener el orden público si la ley lo permite, si son utilizados con un fin legítimo y de manera necesaria y proporcionada al fin que se persigue.

En una investigación concreta de lavado de activos, el uso de datos provenientes de las declaraciones fiscales de una persona puede considerarse para establecer o negar la existencia de un vínculo entre la persona y las operaciones de lavado de activos.

4. Tratamiento de categorías especiales de datos (datos sensibles)

Las categorías especiales de datos, tales como datos genéticos, datos personales en relación con delitos, procesos y condenas penales y medidas de seguridad relacionadas con ellos, datos biométricos que identifiquen únicamente a una persona, datos personales para la información que revelan en relación con origen étnico o racial, preferencias políticas, afiliación sindical, convicciones religiosas o de otro tipo, informaciones referentes a la salud o a la vida sexual, solo pueden tratarse si está previsto en la ley y se toman los recaudos necesarios para lidiar con el riesgo posible de discriminación o efecto legal adverso que afecten de manera significativa a

los titulares de los datos. Los recaudos pueden ser de naturaleza técnica, por ejemplo, medidas de seguridad adicionales y de naturaleza organizativa. Dichos recaudos deben ajustarse a cada operación de tratamiento de datos, teniendo en cuenta sus especificidades, y es muy recomendable utilizar múltiples niveles de protección para dichas categorías de datos (por ejemplo, ficheros separados, tiempos de retención de datos más cortos, etc.). Resulta crítico evitar el acceso no autorizado o no buscado a dichas categorías de datos, incluso con medidas de seguridad adicionales.

Es necesario realizar un balance cuidadoso que considere la finalidad de la investigación, el contexto y la naturaleza de los datos, para determinar si la Policía puede tratar datos sensibles y con qué alcance. Por ejemplo, cuando la Policía trata datos biométricos, resulta recomendable diferenciar si es con finalidad identificatoria (donde, por ejemplo, dos huellas dactilares podrían ser suficientes) o con finalidad de investigación delictiva (donde podrían necesitarse más huellas).

El uso de Evaluaciones de Impacto en Protección de Datos (EIPD), que suele llevarse a cabo cuando es probable que un tratamiento depare un alto riesgo para los derechos y las libertades de las personas, también puede ser recomendable para ayudar a asegurar que se brinden las garantías necesarias. El responsable del tratamiento de datos debe evaluar y demostrar si la finalidad que se persigue puede conseguirse de manera que tenga un menor impacto en el derecho a la privacidad y la protección de datos y si el tratamiento de categorías especiales de datos no representa un riesgo de discriminación para el titular de los datos.

Además, debe recordarse que la recopilación y el tratamiento de datos sensibles en el contexto de la elaboración de perfiles está prohibido [Principio 3.11 de la Recomendación (2010)13[3]], excepto si dichos datos son necesarios y proporcionados a las finalidades lícitas específicas de tratamiento, y si el Derecho nacional proporciona las salvaguardas necesarias. En este contexto, además de las medidas antes detalladas, pueden recomendarse el uso de tecnologías de protección del derecho a la privacidad (PET, por sus siglas en inglés) y verificaciones más frecuentes en lo que respecta a la legitimidad del tratamiento. Por ejemplo, esto podría redundar en la adopción de medidas para contrarrestar la presunción de que las personas pertenecen a una organización delictiva a raíz del lugar donde viven, del lugar en que opera la organización o por el hecho de que comparten el mismo origen étnico.

Ejemplo:

No se permite apuntar a grupos o personas solo con base en sus convicciones religiosas.

Sin embargo, en una investigación de un grupo de personas posiblemente involucradas en actividades terroristas que se atribuyen a un grupo religioso en particular, podría resultar de importancia tratar datos específicos acerca de los seguidores de ese grupo religioso específico (en relación con el lugar de culto, los predicadores religiosos, las costumbres, las enseñanzas, los miembros y la estructura de la comunidad religiosa, etcétera, que fueran pertinentes a la investigación).

5. Proporcionar información a los titulares de los datos

Una de las obligaciones más importantes del responsable del tratamiento es proporcionar información acerca del tratamiento de los datos a los titulares de los datos. Dicha obligación es doble: requiere que el responsable del tratamiento proporcione información general al público

[3] Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados Miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la elaboración de perfiles (https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00)

acerca del tratamiento de datos que lleva a cabo y que proporcione información específica a los titulares de los datos si no hay restricciones o derogaciones con respecto al tratamiento de datos, como se describe en el Punto 7.

La información que se brinde al público en general debe generar conciencia, informarlo acerca de sus derechos y proporcionar una guía clara sobre el ejercicio de sus derechos. La información proporcionada debe ser efectiva y fácilmente asequible. Asimismo, debe incluir detalles acerca de las condiciones en las que proceden excepciones con respecto a los derechos de los titulares de los datos y cómo pueden apelar ante la autoridad de protección de datos o el Poder Judicial.

Los sitios web y otros medios de comunicación fácilmente asequibles desempeñan un papel importante en informar al público. Se recomienda tener plantillas de notas en dichos sitios web u otros medios con la finalidad de ayudar a los titulares de los datos a ejercitar sus derechos. Incumbe al responsable del tratamiento proporcionar información que destaque de manera adecuada la protección de datos y los derechos de los titulares de datos.

Con objeto de dar cumplimiento a la segunda obligación de proporcionar a los titulares de los datos información específica acerca de los datos tratados, la Policía ha de informar a dichos titulares acerca del tratamiento planeado antes de llevarlo a cabo o, si no es posible por motivos objetivos, luego de hacerlo. Dicha comunicación comprenderá información acerca del tratamiento de datos, la recopilación de los datos de personas e información detallada sobre sus derechos. La obligación de proporcionar información específica implica que, en principio, a los titulares de los datos se proporcionarán datos tales como nombre, datos de contacto del

responsable del tratamiento, el encargado del tratamiento de datos, los destinatarios de los datos, el conjunto de datos a tratar, la finalidad del tratamiento de datos, las bases legales para éste e información acerca de sus derechos.

La información debe proporcionarse a menos que proceda una restricción o derogación, como se describe en el Punto 7, teniendo en cuenta la especificidad de los archivos policiales, tales como archivos de inteligencia criminal o archivos que contengan otros tipos de datos sensibles. Para evitar que se perjudique el desempeño de las funciones policiales, incluida la fiscalía, o a los derechos de las personas, incluso si se aplicaron restricciones o derogaciones al derecho a la información, debe proporcionarse información a los titulares de los datos tan pronto como cese de poner en peligro la finalidad con la que dichos datos se utilizaron.

A menudo, los titulares de datos, debido a restricciones o derogaciones en su derecho a la información, no pueden recibir información completa acerca del tratamiento que la Policía realiza con sus datos. Ello no debe afectar la posibilidad de ejercer el derecho al acceso.

Ejemplo:

A efectos de la investigación de un delincuente sexual de alto riesgo, el tratamiento de datos y la retención de datos a largo plazo pueden justificarse sin informar a las personas bajo vigilancia si esto podría perjudicar una investigación en curso o planificada.

Sin embargo, una vez que se haya logrado la finalidad del monitoreo encubierto y no se aplique ninguna otra restricción o derogación, se debe informar al titular de los datos sobre el hecho de que él o ella estuvo sujeto a tal medida.

6. Derechos de los titulares de los datos

Acceder a los datos personales propios es un derecho fundamental para sus titulares, ya que les permite estar al tanto del tratamiento de datos en relación con ellos. Además, también puede

constituir un prerrequisito para permitir el ejercicio de otros derechos, tales como el derecho de rectificación y el de supresión.

En caso de que se recopilen los datos de una persona durante una investigación u otra tarea de la Policía, como se describe en el Punto 1, tan pronto como las circunstancias lo permitan de manera segura, en principio, la Policía debe garantizar el acceso al titular de los datos si tal solicitud existiera. La comunicación debe contener la misma información que se describe en el Punto 5, a menos que el titular de los datos desee algo diferente.

Bajo las estrictas condiciones descriptas en el Punto 7, la ley puede disponer que el derecho al acceso sea limitado o excluido si proporcionar tal información perjudica la investigación u otra tarea policial importante, los intereses de Estado (tales como la seguridad pública, la seguridad nacional, etc.) o la protección de los derechos y las libertades de otros. Sin embargo, la retención de información acerca del tratamiento de datos por parte de la Policía solo debe usarse con moderación y cuando puede justificarse con claridad.

La Policía debe apuntar a responder incluso preguntas generales que surjan de los titulares de datos acerca de las actividades de tratamiento en relación con sus datos personales, pero puede utilizar formularios estandarizados para facilitar la comunicación.

Ejemplo:
Si un titular de datos pregunta a la Policía sobre los datos que trata acerca de él, la Policía, si no se aplica una excepción y luego de verificar la identidad del titular de los datos, debe proporcionar una respuesta detallada con referencias legales que contengan la lista de archivos policiales donde se encuentran los datos del titular de los datos, pero debe hacerlo en un lenguaje sencillo, evitando expresiones poco comunes o especializadas.

En principio, el derecho al acceso debe ser gratuito.

Se puede cobrar una tasa administrativa razonable por la solicitud si la ley nacional lo permite y la solicitud es manifiestamente infundada o excesiva. La Policía también puede negarse a responder a tales solicitudes manifiestamente infundadas o excesivas, en particular, si su carácter repetitivo justifica la denegación.

Con la finalidad de asegurar un justo ejercicio del derecho de acceso, la comunicación «en un formulario inteligible» rige tanto para el contenido como para la forma de una comunicación digital estandarizada. Sin embargo, resulta aconsejable dirigirse a la legislación nacional para asegurar la coherencia y evitar que los sospechosos se valgan de este método para averiguar si existe una investigación en curso sobre ellos.

Con respecto al acceso directo, el titular de los datos puede solicitar el acceso al responsable de los archivos. El responsable del tratamiento de datos evaluará la solicitud y toda posible restricción o derogación que solo se pueda usar si es necesaria para el desempeño de una tarea policial específica, como se describió en el Punto 1, o si es necesaria para la protección del titular de los datos o los derechos o las libertades de otros, y responder directamente al titular de los datos. En caso de una restricción, información parcial o derogación, aun se proporcionará la información acerca del uso de dichas medidas, junto con la motivación subyacente, así como la información concerniente a la reparación.

Ejemplo:
La solicitud de acceso puede ser rechazada si hay una investigación en curso sobre la persona, y el acceso del interesado a los datos podría comprometer dicha investigación.

Si se usara la restricción o la derogación, de acuerdo con la ley o práctica nacionales, la respuesta debe tomar en cuenta toda circunstancia a la que la restricción o derogación sea aplicable.

Como regla, lo ideal sería que la ley nacional proporcionara acceso directo. Si el derecho al acceso previsto es indirecto, los titulares de datos pueden dirigir su solicitud a la autoridad de control, que, luego de haber sido debidamente instruida, llevará a cabo la solicitud en su nombre y realizará verificaciones acerca de la disponibilidad y legitimidad del tratamiento de los datos personales del titular de los datos. Luego, la autoridad de control contestará al titular de los datos (proporcionando los datos que sea posible revelar, con sujeción a cualesquiera restricciones o derogaciones legalmente permitidas). En caso de restricción o derogación, debe llevarse a cabo la misma comunicación que para el caso de acceso directo.

El responsable del tratamiento debe considerar la solicitud y contestar al titular de los datos dentro de un plazo razonable, de acuerdo con las disposiciones de la ley nacional.

Debe haber arreglos establecidos para confirmar la identidad del titular de los datos antes de otorgar acceso a cualquier dato, así como para obtener información acerca de las actividades de tratamiento a las que la solicitud se refiere. Lo mismo es válido si el titular de los datos delega la autoridad a otra persona para que ejerza sus derechos.

Para los titulares de los datos, es un derecho esencial poder corregir datos incorrectos acerca de ellos o disponer que se eliminen datos cuyo tratamiento es excesivo, irrelevante o ilegal. Si el titular de los datos descubre datos incorrectos o irrelevantes, debe contar con el derecho a impugnarlos y asegurarse de que sean corregidos o eliminados.

En algunos casos, puede resultar apropiado agregar información suplementaria o correctiva al archivo. Resulta importante resaltar que este derecho solo puede ejercerse con el debido respeto a los derechos de otras personas.

Si la información a corregir o eliminar ya fue comunicada a otro lugar, las autoridades pertinentes deben ser informadas de los cambios a realizar.

Todos los cambios sugeridos deben ser respaldados con pruebas. Si los titulares de los datos pueden probar, mediante el uso de la documentación oficial, que los datos tratados por la Policía con respecto a ellos son incorrectos, el responsable del tratamiento no tendrá el derecho a decidir si corregirlos o no.

Como se mencionó en el Punto 7, puede que la Policía necesite no dar información u otorgar el derecho de acceso, de eliminación y de corrección que pueda poner en peligro una investigación y, por tanto, debería ser excluida mientras dure la investigación. Como se mencionó en el Punto 7, la legislación nacional puede imponer restricciones o derogaciones similares.

Las restricciones o derogaciones a los derechos de los titulares de datos solo deben aplicarse en tanto sean necesarias y se deben interpretar en sentido estricto[4]. Toda solicitud del titular de los datos debe evaluarse con cuidado caso a caso. Toda resolución de denegar una solicitud por parte del titular de los datos debe ser proporcionada por escrito (lo que incluye medios electrónicos). Dicha respuesta debe brindar una justificación clara de la toma de la resolución que pueda ser verificada por una autoridad independiente o un tribunal. Es posible que la

[4] Caso TEDH: parágrafo 42 de *Klass y otros contra Alemania* (Solicitud número 5029/71).

comunicación de los motivos para la denegación represente un riesgo para las fuerzas del orden público, el titular de los datos o para los derechos y libertades de otros. Si es el caso, y de ser necesario, debería documentarse y proporcionarse a la autoridad independiente o tribunal para su verificación.

Debe informarse al titular de los datos de todas las opciones disponibles luego de una resolución de denegación, tales como una apelación ante la autoridad de control, un tribunal u otra autoridad administrativa independiente. Dependiendo de la legislación nacional, sobre todo, si existe un derecho de acceso directo o indirecto, la comunicación del resultado de la revisión o apelación puede variar. En caso de acceso directo, el titular de los datos debe al menos ser informado de que una verificación del archivo policial tuvo lugar. Como alternativa, el órgano de control puede solicitar a la Policía divulgar los datos contenidos en el archivo del titular de los datos. El tribunal puede tener el poder de imponer el acceso, la corrección o la eliminación de los datos del archivo, incluso en casos de solicitud de acceso referidos a él por parte de la Policía o la autoridad de control.

Si la Policía envía una carta de denegación, debe incluir el nombre, domicilio, sitio web, etcétera, de todos los foros posibles ante los cuales puede solicitar reparación.

El titular de los datos debe contar con acceso a un tribunal para presentar una apelación y hacer que revisen los motivos para la denegación si no está satisfecho con la respuesta por parte de la autoridad de control o la autoridad independiente. La autoridad de control debe contar con facultades suficientes para examinar el archivo policial respectivo y disponer la comunicación de la evaluación.

7. Excepciones a la aplicación de los principios de protección de datos

Las excepciones solo pueden usarse con finalidades específicas previstas en el artículo 8 del Convenio Europeo de Derechos Humanos y el Convenio 108, si están previstas por ley (la ley debe ser pública, abierta, transparente y lo suficientemente detallada) y si constituyen una medida necesaria y proporcionada en una sociedad democrática con la finalidad de la protección de la seguridad nacional, la defensa, la seguridad pública, los intereses económicos y financieros importantes, la imparcialidad y la independencia del Poder Judicial, la prevención, la investigación y el enjuiciamiento de infracciones penales y la ejecución de sanciones penales, así como otros objetivos esenciales de interés general público (que incluye finalidades en conexión con la consecución de los compromisos legales u obligaciones internacionales de un Estado, sobre todo, los derivados de resoluciones vinculantes de los órganos de las Naciones Unidas y finalidades humanitarias) o la protección de los derechos y las libertades fundamentales de otros.

Las excepciones que deben incorporarse a la legislación nacional no deben describirse de manera general, sino que deben servir a una finalidad bien definida. Las excepciones pueden aplicarse a los principios descriptos en los Puntos 2, 3, 4 y 5, así como a los derechos de los titulares de datos (Punto 6).

Ejemplo:
Si dar información a un titular de datos puede poner en peligro la seguridad de un testigo o un informante, dicho derecho puede ser limitado a la luz de tales circunstancias.

Si la Policía se vale de la excepción definida en la ley nacional en la que se establecen garantías específicas, debe usarla con propósitos legítimos y solo en tanto sea necesario y proporcionado a la consecución del propósito para el que la usa. El propósito de que la Policía utilice excepciones debe limitarse a casos en los que no utilizar dichas excepciones pondría en peligro el accionar policial descripto en el Punto 1 o pondría en peligro las acciones llevadas a cabo con las finalidades que figuran en la lista de excepciones que arriba se describe.

Ejemplo:
Si la información específica recabada prueba que se han llevado a cabo operaciones de lavado de activos para financiar operaciones terroristas, los datos recopilados sobre personas pueden conservarse durante un período más prolongado del que sería estrictamente necesario para las investigaciones policiales si lo aprueba el organismo que garantiza la supervisión externa.

8. Utilización de técnicas especiales de investigación

Con respecto a la utilización de técnicas especiales de investigación, se invita a la Policía a dirigirse a la Recomendación (2017)6 del Comité de Ministros a los Estados Miembros sobre las «técnicas de investigación especial» con relación a los delitos serios, incluidos los actos de terrorismo. En particular, los parágrafos 7 a 10 de la Recomendación pueden proporcionar una guía útil acerca de la aplicación lícita de dichas técnicas de investigación.

Esta área suele estar regulada en detalle en el Derecho penal procesal nacional. Sin embargo, al resolver acerca de su uso, pueden evaluarse algunas consideraciones de protección de datos con el fin de permitir a la Policía utilizar los medios menos intrusivos de tratamiento de datos

durante sus operaciones. Si se pueden usar métodos menos intrusivos para conseguir las finalidades deseadas, se debe favorecerlos. El uso de técnicas especiales de investigación puede considerarse proporcionado si el mismo resultado no puede lograrse mediante métodos menos intrusivos. Independientemente del método de investigación u otra operación llevada a cabo por la Policía, esta está obligada a desempeñarse dentro de los principios generales de la protección de datos descriptos en las Consideraciones Generales, a menos que la ley la exima expresamente.

Con desarrollos tecnológicos cada vez más sofisticados, la vigilancia electrónica se ha vuelto más fácil. Sin embargo, la utilización de dichas técnicas interfiere con la protección de derechos y libertades fundamentales, en particular, el derecho a la privacidad. Al decidir el método de investigación, debe equilibrarse la gran probabilidad de que se produzcan graves injerencias en el derecho a la privacidad con la seriedad del delito a prevenir o investigar y la relación costo-efectividad, el uso de recursos y la eficacia de las investigaciones.

Ejemplo: En una investigación, las pruebas de comunicación entre dos sospechosos se pueden reunir de varias maneras. Si, mediante el uso de interrogatorios, testimonios, la obtención de datos de llamadas, se puede lograr el mismo resultado sin poner en peligro la efectividad de la investigación, se prefieren tales métodos al uso de medidas de vigilancia más intrusivas, como las escuchas telefónicas.

9. La introducción de nuevas tecnologías de tratamiento de datos

Si es probable que el tratamiento de datos resulte en un alto riesgo para los derechos de la persona, el responsable del tratamiento debe llevar a cabo Evaluaciones de Impacto en

Protección de Datos (EIPD) para evaluar todos los riesgos de las acciones. Considerando que la introducción de nuevas tecnologías de tratamiento de datos conlleva per se tal riesgo, es probable que la introducción de una nueva tecnología así haga recomendable una EIPD. Se aconseja que la evaluación de riesgo no sea estática, sino que tome en cuenta el caso específico, que se repita a intervalos regulares, que esté referida a fases pertinentes de la actividad de tratamiento de datos y que tome en cuenta las consideraciones de responsabilidad.

También resulta de gran importancia que, en términos de seguridad de datos y de comunicaciones, se respeten los estándares más altos al introducir tales tecnologías.

Ejemplo:

Las nuevas técnicas de minería de datos pueden ofrecer amplias posibilidades para la identificación de posibles sospechosos y deben evaluarse cuidadosamente para que cumplan con la ley de protección de datos existente, junto con la evaluación de los riesgos que puede representar para los derechos de las personas y sugerencias para la adopción de garantías en materia de protección de datos, incluso con respecto a la seguridad de datos.

La autoridad de protección de datos cumple un papel importante en asesorar con respecto a cuáles riesgos están relacionados a la protección de datos y qué garantías deben proporcionarse para asegurar que todos los medios técnicos respeten la ley de protección de datos. No obstante, la Policía no tiene la obligación de referir todos los casos a la autoridad de control cuando introduce nuevas tecnologías. Puede hacerlo si la EIPD que llevó a cabo previamente demuestra un alto riesgo significativo y persistente para los derechos de la persona, a pesar de la adopción de garantías específicas.

La consulta entre la autoridad de control y el responsable del tratamiento debe proporcionar a aquella la oportunidad suficiente de dar su opinión fundada y evaluación de las actividades de tratamiento de datos del responsable del tratamiento, a la vez que no pone en juego sus funciones clave.

La autoridad de control debe ser provista de datos adecuados, en particular con respecto al tipo de archivo, el responsable del tratamiento, el encargado del tratamiento, la base jurídica y finalidad del tratamiento de datos, el tipo de datos que se procesa y quién accede a dichos datos, así como de información sobre la retención de datos, la normativa sobre el registro y el acceso a los datos, y otros aspectos técnicos pertinentes de la aplicación.

Ejemplo:

La información detallada que se recoge en los archivos de referencia nacional que contienen datos de huellas dactilares, tal como la finalidad, el responsable del tratamiento, etc. podría comunicarse o ponerse a disposición de la autoridad de protección de datos para su

Tras la consulta, el responsable del tratamiento de datos deberá considerar detenidamente la aplicación de las medidas y las garantías necesarias que hayan sido recomendadas por la autoridad de protección de datos.

Ejemplo:

Es muy posible que la introducción de un sistema de reconocimiento facial automático u otro sistema basado en el tratamiento automatizado de datos biométricos requiera de asesoría a fin de obtener una visión clara de los riesgos que podría entrañar para los derechos de las personas. Cuando sea necesario y así lo recomiende la autoridad de protección de datos tras ser consultada sobre esta cuestión, deberán establecerse salvaguardas específicas (relativas al tiempo de retención de los datos, las funciones de cotejo cruzado, el lugar en el que se almacenan los datos y cuestiones relativas al acceso a los datos, etc.) para dar cumplimiento a los principios y disposiciones en materia de

El uso de la tecnología del Internet de las cosas (IdC) en la labor policial

Los datos enviados y recibidos por la Policía durante el transcurso de sus actividades operacionales a través de internet son buenos ejemplos del cómo se usa actualmente el IdC. Debido a las posibles vulnerabilidades que pueden afectar la seguridad, para el uso del IdC se requieren medidas tales como la autenticación de los datos, el control de acceso para garantizar la seguridad de los datos y la resiliencia frente a ataques (cibernéticos).

Ejemplo:
A la luz de las posibles vulnerabilidades que pueden afectar su seguridad, los lentes inteligentes utilizados por la Policía no deben estar conectados directamente a una base de datos nacional de antecedentes judiciales y debe garantizarse un elevado nivel de seguridad de los datos recopilados.

La analítica de Big Data en la Policía

Los avances tecnológicos en el tratamiento y el análisis de conjuntos de datos de gran tamaño y complejidad que conducen a Big Data y a la analítica de Big Data presentan oportunidades y desafíos para la Policía, que recurren a fuentes digitales y a técnicas de elaboración de perfiles para realizar sus tareas.

Las tecnologías de Big Data permiten la recopilación y el análisis masivo de una gran cantidad de datos generados por las comunicaciones electrónicas y los dispositivos provistos de otro tipo de datos en masa. Esto podría interferir con el derecho a la privacidad y protección de datos.

La Recomendación CM/Rec(2010)13[5] del Consejo de Ministros de Europa relativa a la protección de las personas físicas en lo que respecta al tratamiento automatizado de datos de carácter personal en el contexto de la elaboración de perfiles y las Directrices sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales en un mundo de Big Data[6] también pueden ser de utilidad en el contexto de la analítica de Big Data para uso policial.

Las tecnologías y las técnicas de análisis de Big Data pueden ayudar a detectar la delincuencia, no obstante, existen riesgos considerables para este tipo de tratamiento de datos que deben ser tomados en cuenta:

- Las bases de datos procedentes de un dominio pueden utilizarse en otro dominio y con otra finalidad, lo que cambia el contexto y puede dar lugar a conclusiones erróneas y a la falta de fundamento jurídico válido, por consiguiente, conducir a un tratamiento ilícito de datos que puede conllevar graves consecuencias para las personas implicadas.

- La elaboración de perfiles puede llevar a formular conclusiones discriminatorias, lo que puede traducirse en el refuerzo de los estereotipos, la estigmatización y la discriminación.

- La creciente cantidad de datos personales almacenados en las bases de datos puede provocar graves vulnerabilidades y el consiguiente riesgo de violación de la seguridad de los datos si no se garantiza la seguridad de la información.

[5] Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de personas con respecto al procesamiento automático de datos de carácter personal en el contexto de la elaboración de perfiles

[6] Documento T-PD(2017)1 - Big Data Guidelines /Directrices en materia de Big Data/

Cuando el Big Data se basa en datos de carácter personal, los responsables del tratamiento de datos deben prestar mayor atención a los siguientes requisitos:

- Verificación de la exactitud, el contexto y la pertinencia de los datos.
- Su uso requiere un elevado nivel de responsabilidad demostrada.
- Su uso deberá combinarse con métodos de investigación que complementen las conclusiones extraídas del análisis de Big Data. Una decisión que afecte a una persona no se tomará únicamente en relación con el tratamiento automatizado de datos de carácter personal.
- Su utilización será necesaria y proporcionada para el cumplimiento de las tareas policiales descritas en el Punto 1, prestando especial atención a que los datos tratados sean adecuados, pertinentes y no excesivos en relación con la finalidad para la que se tratan.
- El análisis predictivo requiere de la intervención humana para evaluar la pertinencia del análisis y las conclusiones.
- Deberían tenerse en cuenta las directrices éticas elaboradas a nivel nacional o internacional.
- Como principio y sin perjuicio de las restricciones y excepciones mencionadas en el Punto 7, el responsable del tratamiento de datos debe garantizar la transparencia mediante la explicación de cómo se tratan los datos de conformidad con los principios de privacidad y protección de datos. Si los datos recopilados para una finalidad se utilizan para otra finalidad, el responsable del tratamiento de datos debe, en principio, informar al titular de los datos de este uso posterior.

- Incluso si se utilizan métodos complejos, debe demostrarse la legitimidad del tratamiento —incluida la utilización posterior de los datos— y el cumplimiento de las condiciones establecidas en el artículo 8 del CEDH y en el Convenio 108.

- Debe existir una política de seguridad de la información que se aplique a lo largo de todo el tratamiento.

- Los responsables del tratamiento de datos deben garantizar que el tratamiento de los datos de carácter personal sea justo cuando se utilice Big Data para tomar decisiones que afecten a las personas, y que existan medios administrativos y judiciales para que las personas puedan impugnar dichas decisiones. Esto implica que los titulares de los datos tengan conocimiento del fundamento del algoritmo utilizado y de las finalidades para las que se ha utilizado.

Se recomienda encarecidamente observar las consideraciones anteriores, especialmente las relacionadas con la intervención humana y la combinación de nuevos métodos analíticos con los tradicionales, cuando en el análisis de Big Data se procesan datos sensibles.

10. Almacenamiento de datos

Los datos personales se tratarán hasta que hayan cumplido la finalidad para la que fueron recopilados, tal como se señala en el Punto 2. Los datos almacenados deben ser adecuados, estar actualizados, ser necesarios, pertinentes y no excesivos en relación con la finalidad para la cual se hubieren obtenido.

Deben establecerse normas claras en relación con la gestión de las diferentes bases de datos, en especial en lo que respecta al análisis de las búsquedas que dan lugar a resultados múltiples.

El principio de necesidad debe aplicarse a lo largo de todo el ciclo de vida del tratamiento. El almacenamiento puede permitirse si el análisis demuestra que los datos personales son estrictamente necesarios para alcanzar las finalidades policiales descritas en el Punto 1.

Los motivos de retención y tratamiento deben revisarse periódicamente. El tratamiento de datos personales fuera del marco legal permitido para la retención constituye una grave violación del derecho a la protección de los datos de carácter personal. Si la ley en relación con un delito específico establece un período de retención de datos de cuatro años y si después de transcurridos los cuatro años desde la recopilación de los datos en cuestión la Policía trata los datos personales en relación con este delito basándose únicamente en este motivo, y no existe ningún otro motivo legal para tratar estos datos, la retención de tales datos se consideraría ilícita.

Los plazos generales de retención de datos suelen estar regulados en el derecho nacional o internacional. A fin de respetar la legislación y garantizar al mismo tiempo la eficacia y el éxito de una investigación, se recomienda encarecidamente a los organismos policiales que elaboren normas y/o recomendaciones internas que fijen el plazo de retención de datos de carácter personal o de una revisión periódica de la necesidad de almacenar tales datos.

Ejemplo:

En el supuesto de que la ley establezca un plazo de retención de datos de cuatro años, pero la persona objeto de una investigación sea absuelta de todos los cargos por el tribunal al cabo de dos años, sus datos serán suprimidos de la base de datos (si la persona no es reincidente o si no hay información sobre ella en la que cometa de nuevo la misma categoría de delito y si ha transcurrido el plazo para solicitar la reparación), siempre que hayan caducado todos los plazos para la revisión del caso. Asimismo, si, después de cuatro años, la investigación sigue en curso y sus datos siguen siendo pertinentes para ésta, la Policía debería poder retenerlos.

En este último caso, es importante formular la política de retención de datos de modo que los datos utilizados en materia penal permanezcan bajo la supervisión del responsable del tratamiento de datos hasta que el procedimiento judicial concluya completamente (lo que significa que se agotaron los recursos dentro de la vía judicial o transcurrió el plazo para ello).

La Policía debe proporcionar sistemas y mecanismos para garantizar que los datos almacenados sean exactos y que se mantenga su integridad.

Las obligaciones internacionales, que incluyen el suministro de datos a organismos internacionales como Europol, Eurojust e INTERPOL, los acuerdos bilaterales y la asistencia jurídica mutua entre los Estados miembros y terceros países, deben cumplirse a la hora de elaborar las políticas internas.

En la medida de lo posible, los datos deben clasificarse en función del grado de exactitud y fiabilidad, a fin de ayudar a la Policía en sus actividades. Se recomienda utilizar códigos de tramitación para distinguir estas categorías. Un sistema de clasificación facilita la evaluación de la calidad de los datos y su fiabilidad. La clasificación de los datos también es importante cuando se han de comunicar a otros organismos policiales o Estados.

Ejemplo:

La información recopilada directamente de la declaración de una persona será evaluada de manera diferente a la información recopilada de un testimonio de oídas de una persona. Los datos basados en hechos, o datos «verificados», se evaluarán de forma diferente a los datos basados en opiniones o evaluaciones personales, o a los datos «sin verificar».

Los datos personales recopilados por la Policía con finalidades administrativas deben mantenerse (en la medida de lo posible: lógica y físicamente) separados de los datos recogidos con finalidades policiales. La Policía puede acceder a esos datos cuando sea necesario y esté permitido por la ley.

Algunos ejemplos de datos administrativos son las listas de datos sobre los titulares de licencias o los datos sobre recursos humanos y certificados de tenencia de armas de fuego.

11. La comunicación de datos en el sector policial

Debe hacerse una distinción entre la comunicación nacional de datos en el sector policial (Punto 11) o a otros organismos públicos (Punto 12) y las transferencias internacionales (Punto 14) de datos. Dentro de estas distintas operaciones se aplican diferentes requisitos, dependiendo de quién recibirá los datos, ya sea la Policía, otra entidad pública o una entidad privada.

La Policía solo puede comunicar datos personales dentro del sector policial si existe un interés legítimo para dicha comunicación en el marco de las competencias legales de estos organismos (por ejemplo, una investigación penal en curso o una operación policial compartida y leyes o acuerdos que permitan la comunicación).

Deben existir normas claras y transparentes sobre la forma en que la Policía concede el acceso a los datos que obran en su poder y los fundamentos.

La comunicación de datos personales de un organismo policial a otro debe ajustarse a las Consideraciones generales descritas anteriormente.

Ejemplo:
Una unidad de Policía puede compartir datos sobre un sospechoso que presuntamente cometió un fraude fiscal con otra unidad de Policía que investiga un caso de asesinato si hay indicios de que el sospechoso de este delito podría ser la misma persona o si hacerlo prestaría ayuda material a la investigación.

12. La comunicación de datos por parte de la Policía a otros organismos públicos

La comunicación de datos a terceros que no sean organismos policiales está permitida si así lo establece la ley y los datos son requeridos por el destinatario para el desempeño lícito de sus funciones. Los acuerdos de asistencia mutua previstos por la ley entre los organismos policiales y los públicos permiten a estos últimos tener acceso a los datos de la Policía que serían esenciales para desempeñar sus funciones o tareas (por ejemplo, en sus investigaciones u otras obligaciones legales de conformidad con la legislación nacional).

Deben seguirse normas específicas cuando los datos deban transmitirse a escala nacional fuera del sector policial, ya que existe el riesgo de que el tratamiento de datos de carácter personal, que se consideran datos sensibles, pueda tener efectos adversos para la persona.

También podrá permitirse la comunicación de datos a cualquier otra autoridad pública si está prevista por la ley, si redunda indudablemente en interés del titular de los datos o si la

comunicación es necesaria para evitar un riesgo grave e inminente para otras personas o para el orden público o la seguridad ciudadana.

Los datos comunicados solo podrán ser utilizados por el organismo receptor para las finalidades para las que fueron transferidos.

Ejemplo:
Un migrante solicita un permiso de residencia. Se podrán solicitar datos policiales para verificar si la persona alguna vez estuvo involucrada en una actividad delictiva. Redundaría en interés de la Oficina de inmigración y el solicitante que esta comunicación de datos tenga lugar.

13. La comunicación de datos por parte de la Policía a organismos privados

Es posible que haya ocasiones específicas en las que la Policía pueda comunicar datos a entidades privadas. Esta comunicación deberá ser conforme a derecho y solo podrá ser llevada a cabo por la autoridad que trata los datos. Dicha comunicación solo podrá realizarse a efectos de la investigación u otras tareas policiales importantes descritas en el Punto 1, en interés del titular de los datos, por razones humanitarias o si fuera necesario para prevenir un riesgo grave e inminente para el orden público o la seguridad pública y se garantiza un nivel de protección adecuado que tenga en cuenta el carácter sensible de los datos policiales. Por ejemplo, también puede haber casos en los que los datos policiales puedan comunicarse a organizaciones humanitarias de acuerdo al Derecho internacional, en interés del titular de los datos o por razones humanitarias.

Cuando la Policía tenga derecho a compartir datos con los medios de comunicación para hacer pública la información relativa a una investigación, se deberá prestar especial atención a la

evaluación para determinar si es necesario y si dicha publicidad está permitida en aras del interés público. Deben establecerse las garantías adecuadas para asegurar que se respeten los derechos de las personas implicadas en el caso.

Esta comunicación solo debe realizarse sobre una base casuística y en cada caso debe existir una base jurídica clara que establezca el procedimiento necesario (por ejemplo, la necesidad de una autorización específica) que debe seguirse para que se produzca dicha comunicación.

Ejemplo:
Cuando la Policía se comunica con el sector financiero en relación con delincuentes conocidos por fraude o robo, cuando se comunica con una aerolínea sobre documentos de viaje hurtados o extraviados o cuando la Policía divulga detalles de personas buscadas que se cree que representan un riesgo para el público en general.

14. Transferencias internacionales

Por regla general, toda transferencia de datos policiales a escala internacional debe limitarse a los organismos policiales, hacerse con arreglo a la ley y cumplir su finalidad. Esto implica también seguir los procedimientos internos establecidos por el Derecho procesal penal nacional, que pueden incluir la participación activa de organismos y servicios policiales más amplios, como el Ministerio del Interior, el Ministerio de Justicia, la fiscalía, los jueces de instrucción, etc. Para ello, pueden ser de utilidad los instrumentos jurídicos internacionales multilaterales, como el Convenio 108 y el Estatuto de la Interpol y su documentación de apoyo en relación con el tratamiento de datos, los marcos jurídicos regionales, como la legislación de la UE y de las instituciones de la UE (sobre Europol, Eurojust, Frontex, etc.) y los acuerdos ulteriores (acuerdos bilaterales operacionales), los tratados bilaterales y, en general, los

acuerdos internacionales de asistencia mutua, u otros acuerdos bilaterales o multilaterales concertados para una cooperación eficaz.

Cuando se compartan datos, se debe tener en cuenta si la autoridad receptora está desempeñando una función que le ha sido asignada en virtud de la legislación con finalidades policiales, y si es necesario compartir los datos para que pueda llevar a cabo su tarea específica.

La autoridad emisora debe cerciorarse de que existe un nivel adecuado de protección de datos en el Estado receptor y que el Estado receptor cumple con las normas pertinentes sobre las transferencias internacionales de datos personales. Esto incluye el establecimiento de garantías adecuadas en relación con la protección de datos en los casos en que no existan disposiciones legales nacionales o acuerdos internacionales pertinentes. Este medio de transferencia debe utilizarse como último recurso. La normativa internacional en materia de transferencias internacionales, como el «Reglamento de INTERPOL sobre el tratamiento de datos» y su «Estatuto de la Comisión de Control de los Ficheros de INTERPOL», el «Reglamento sobre el control de la información y el acceso a los ficheros de INTERPOL», las disposiciones del Convenio europeo de asistencia judicial en materia penal de 20 de abril de 1959, y el Convenio sobre la Ciberdelincuencia (STCE Nº 185), podrá tenerse en cuenta[7] para garantizar que toda transferencia de datos se justifique desde el punto de vista jurídico y cuente con las garantías adecuadas. En la solicitud deben indicarse claramente todos los elementos necesarios de la parte solicitante para que la parte receptora pueda tomar una decisión bien fundada sobre la

[7] Esto se entiende sin perjuicio del derecho del Comité Consultivo del Convenio 108 y de otras instancias que tengan tal facultad de evaluar y revisar, en su caso, el nivel de protección de datos garantizado por dichos acuerdos multilaterales.

solicitud. Se espera que estos detalles incluyan el motivo de la solicitud, así como el propósito de la transferencia de datos.

Es necesario garantizar que se tomen las medidas adecuadas para proteger la seguridad de la información.

Debe garantizarse un nivel adecuado de protección de datos (por ejemplo, mediante garantías estandarizadas ad hoc o aprobadas, proporcionadas por instrumentos jurídicamente vinculantes y de cumplimiento exigible) si los datos han de transferirse a países u organizaciones que no participan en el Convenio 108.

Si la autoridad emisora aplica condiciones en relación con el uso de los datos en el Estado receptor, éstas deberán observarse. Los Estados emisor y receptor deben estar de acuerdo en el uso de los datos en todas las operaciones de tratamiento y la autoridad emisora debe obtener garantías del destinatario de que se respetan las condiciones acordadas.

Ejemplo:

Una transferencia posterior de datos solo debería permitirse si es necesaria para el desarrollo de las tareas policiales descritas en el Punto 1 y si el segundo destinatario es también un organismo policial que garantiza un nivel adecuado de protección de datos. La Policía, incluidos los servicios de la fiscalía y/o los jueces de instrucción que originalmente enviaron los datos, también deben dar su consentimiento para la transferencia posterior. Si la Policía del país X envía datos personales a la Policía del país Y, el país Y los podrá transferir únicamente si, por encima de todos los requisitos previstos por la ley (existe un fundamento jurídico válido y la transferencia se ajusta a la finalidad original), el país X consiente la transferencia. Si los datos se envían al país Z, que no es parte en el Convenio 108, el país Y debe asegurarse de que este país ofrece un nivel adecuado de protección de los datos personales, incluida la existencia de medios eficaces para el ejercicio de los derechos del titular de los datos.

La transferencia internacional de datos personales a un organismo público no policial es admisible únicamente por motivos excepcionales y en casos individuales si es necesaria para el desempeño de la tarea de la autoridad que realiza la transferencia y no se dispone de medios eficaces para transferir los datos a un organismo policial competente. Los principios de protección de datos establecidos en el Convenio 108 deben ser aplicados a todos los tipos de transferencias, especialmente los que requieran un nivel adecuado de protección que tome en cuenta el carácter sensible de los datos policiales.

Ejemplo:

Si las autoridades fiscales del país X solicitan a la Policía del país Y el paradero de una persona implicada en la evasión fiscal no delictiva porque tienen pruebas de que la persona está implicada en asuntos penales en el país X, la Policía, si la legislación nacional lo permite (por ejemplo, en virtud de un convenio bilateral para prevenir la evasión fiscal concertado entre ambos países) puede transferir los datos personales de la persona.

Por regla general, debe evitarse la transferencia internacional de datos personales entre la Policía y los organismos privados en jurisdicciones diferentes. Solo podrá realizarse en casos muy excepcionales, cuando sea estrictamente necesario para el cumplimiento de las tareas policiales descritas en el Punto 1, y por medios legales, siempre que se garantice un nivel de protección adecuado que tenga en cuenta el carácter sensible de los datos policiales. Otros factores que deben tenerse en cuenta para la transferencia son el carácter urgente de la situación, la naturaleza del delito, su carácter transfronterizo y el hecho de que la intervención policial pudiera comprometer el propósito de la investigación por razones objetivas. Hay que tener en cuenta otros hechos como la seguridad de los datos, las garantías recibidas en cuanto al uso de los datos y la legalidad de la transferencia de datos en el país receptor. En este

contexto, cabe señalar que, en tal caso, el responsable del tratamiento de datos tiene una doble obligación con respecto a la protección de los datos personales: una impuesta por el marco jurídico del país en el que reside el responsable del tratamiento de datos y otra relacionada con la transferencia de datos. La Policía local será notificada posteriormente. Siempre que sea posible, la Policía debe hacer uso de los instrumentos jurídicos internacionales existentes en relación con este tipo de transferencia de datos. Las transferencias internacionales también pueden producirse excepcionalmente cuando la Policía comunica datos personales para satisfacer los intereses específicos del titular de los datos o los intereses legítimos prevalecientes (como, por ejemplo, con finalidades humanitarias).

15. Condiciones para las comunicaciones

Dado que el responsable del tratamiento tiene la obligación general de garantizar un alto nivel de calidad de los datos, es aconsejable realizar una revisión adicional antes de compartir los datos con otras personas. Al compartir o transferir datos, siempre es aconsejable verificar la calidad de los datos, si son correctos, están actualizados, son pertinentes y están completos. En la medida de lo posible, en todas las comunicaciones de datos deberán indicarse las resoluciones judiciales, así como las decisiones de no enjuiciar. Es necesario establecer canales de comunicación seguros que garanticen la seguridad de los datos al más alto nivel posible. La calidad de los datos puede ser evaluada hasta el momento en que se lleva a cabo la comunicación.

Ejemplo:

Si se envían datos personales que contienen información incorrecta (personal o de otro tipo), éstos podrán afectar negativamente a la investigación, perjudicar a la persona en cuestión o a otras personas que estén implicadas, o que puedan verse implicadas como consecuencia de la transferencia de datos incorrectos. Como resultado, la Policía de los países de emisión y recepción podrá quedar expuesta a una reparación civil. Básicamente, si se detiene a una persona a causa de una comunicación errónea del nombre del sospechoso, ello vulnera gravemente diversos derechos humanos de la persona en cuestión y puede socavar cualquier investigación penal.

16. Garantías para la comunicación

Es de suma importancia que los principios de necesidad y de limitación de la finalidad sean aplicables a cualquier comunicación nacional o transferencia internacional de datos personales que se realice sin la participación de los organismos policiales.

Los datos compartidos no deben ser utilizados para finalidades distintas de aquellas que motivaron su obtención. Las excepciones a esto son cuando la autoridad emisora, de conformidad con las disposiciones legales, presta su consentimiento para el uso posterior de los datos, y es necesario y vital para que el destinatario realice su tarea.

Los datos también pueden comunicarse si, por razones humanitarias, son necesarios en el interés del titular del dato para evitar un riesgo grave e inminente para el orden público o la seguridad ciudadana.

Ejemplo:

Los datos personales enviados por la Policía del país X a la Policía del país Y en un caso de blanqueo de capitales no pueden ser utilizados por la Policía para elaborar el perfil de la persona en cuestión con respecto a sus creencias religiosas o actividades políticas (a menos que sean pertinentes para el delito cometido y la Policía del país X haya prestado su consentimiento para tal uso).

17. Interconexión de archivos y acceso en línea a los archivos

En circunstancias específicas, la Policía puede recopilar datos mediante la coordinación de su información con otros responsables y encargados del tratamiento de datos. Además, puede combinar datos personales almacenados en diferentes archivos o bases de datos que se mantienen con distintas finalidades, como los que poseen otros organismos públicos y/u organizaciones privadas. Esto puede ser en relación con una investigación penal en curso o para identificar tendencias temáticas con respecto a un determinado tipo de delito.

Para que estas acciones sean legítimas, deben estar autorizadas o sustentadas en una obligación jurídica de cumplir con el principio de limitación de la finalidad.

Si el organismo policial pertinente tiene acceso directo a los archivos de otros organismos policiales o no policiales, solo deberá acceder a los datos y utilizarlos si el ordenamiento jurídico nacional, que debe reflejar los principios fundamentales de protección de datos, lo permite.

Se debe contar con leyes y directrices claras, que se ajusten a los principios de protección de datos, para las referencias cruzadas de las bases de datos. Estas referencias cruzadas serán necesarias, vinculantes y proporcionadas.

Ejemplo:
Los datos conservados a efectos de ciudadanía solo pueden utilizarse en una investigación si la normativa nacional así lo permite y en la medida en que sea necesario para la finalidad de la investigación. Por ejemplo, el número de hijos que tiene un sospechoso puede no ser pertinente en una investigación y, por lo tanto, no debe ser tratado por la Policía.

18. Seguridad de los datos

La Policía debe adoptar medidas de seguridad adecuadas contra riesgos tales como el acceso accidental o no autorizado, la destrucción, la pérdida, la utilización, la modificación o la divulgación de datos personales. Al considerar la seguridad de los datos, la Policía también debe tener en cuenta factores como la localización de los datos, la certificación adecuada de los proveedores de servicios y la existencia de garantías en cuanto a la disponibilidad de los datos. También es aconsejable prestar atención a las consideraciones de seguridad de los datos al distribuir los derechos de acceso. El responsable del tratamiento debe notificar sin demora, como mínimo a la autoridad de control competente, de las violaciones de la seguridad de los datos que, según su evaluación, puedan interferir gravemente en los derechos y las libertades fundamentales de los titulares de los datos. Se debe informar sin dilaciones indebidas de la violación de la seguridad de los datos a los titulares de datos afectados, cuando ello suponga un riesgo para sus derechos y no comprometa la labor policial.

La seguridad de la información es esencial para la protección de datos. Consiste en un conjunto de procedimientos para garantizar la integridad, disponibilidad y confidencialidad de todos los tipos de información dentro de la organización policial, con el objetivo de proporcionar seguridad a los datos y a la información, y limitar los efectos de los incidentes y las violaciones de seguridad de los datos a un nivel predeterminado.

El nivel de protección de una base de datos y/o de un sistema o red de información se determina mediante una evaluación de riesgos. Cuanto más sensibles sean los datos, mayor será la protección que se necesite.

Los mecanismos de autorización y autenticación son esenciales para proteger los datos, y la información sensible debe estar siempre cifrada. Se considera una buena práctica contar con un régimen de auditoría para comprobar regularmente que el nivel de seguridad es adecuado.

Se aconseja a las autoridades policiales que, cuando sea necesario, lleven a cabo las EIPD (véase el Punto 4) para evaluar los riesgos de vulneración del derecho a la privacidad de las personas en relación con la recolección, el uso y la divulgación de información. Esto ayudará a identificar los riesgos y a desarrollar soluciones para asegurar que las preocupaciones se aborden adecuadamente. Toda evaluación de impacto de este tipo debe abarcar los sistemas y procesos pertinentes de las operaciones de tratamiento, pero no los casos individuales.

Un oficial de protección de datos (DPO, por sus siglas en inglés) dentro de la Policía puede desempeñar un papel esencial en la realización de auditorías internas y en la evaluación de la legitimidad del tratamiento, lo que contribuye a un mayor nivel de protección de datos y de seguridad de los datos dentro de la organización. Además, el DPO puede facilitar el diálogo entre la organización y los titulares de datos, así como entre la organización y la autoridad de control, lo que puede contribuir a la transparencia general del órgano policial.

Puede ser recomendable un Sistema de Gestión de Identidades y Accesos (IAM, por sus siglas en inglés) para gestionar el acceso de los empleados y de terceros a la información. Se necesitará autenticación y autorización para acceder al sistema y establecer derechos de privilegio para determinar qué información se puede ver. El IAM puede considerarse un requisito útil para garantizar un acceso seguro y adecuado a los datos.

El responsable del tratamiento, tras una evaluación de los riesgos, debe aplicar las medidas adecuadas en relación con distintos elementos, a saber:

a. el control del acceso a los equipos,
b. el control de los soportes de datos,
c. el control del almacenamiento,
d. el control de usuario,
e. el control del acceso a los datos,
f. el control de la comunicación,
g. el control de la introducción de datos,
h. el control del transporte,
i. la recuperación e integridad del sistema,
j. fiabilidad e integridad.

La protección de la privacidad desde el diseño

El concepto de protección de la privacidad desde el diseño forma parte integrante de la seguridad de los datos. La protección y la seguridad de los datos pueden integrarse directamente en los sistemas y procesos informáticos, mediante el empleo de medidas técnicas y organizativas, para garantizar un alto nivel de protección y seguridad de los datos y, en particular, para reducir al mínimo la probabilidad de que se viole la seguridad de los datos. Este enfoque que se conoce como protección de la privacidad desde el diseño promueve el cumplimiento de las normas de privacidad y protección de datos desde el inicio. Puede lograrse a través del software y/o hardware. Requiere un análisis de amenazas, un enfoque basado en el ciclo de vida completo y pruebas rigurosas.

Los responsables del tratamiento de datos deben garantizar que la privacidad y la protección de los datos sean una consideración fundamental en las primeras fases de cualquier proyecto y, posteriormente, a lo largo de su ciclo de vida. En particular, a la hora de poner en marcha nuevos sistemas de TI para almacenar o acceder a datos personales, elaborar leyes, políticas o estrategias que afecten la privacidad y emprender una iniciativa de intercambio de información que utilice los datos para nuevas finalidades.

La protección de la privacidad desde el diseño requiere la aplicación de tecnologías de protección del derecho a la privacidad (PET) para permitir una mejor protección de los datos personales. Las PET evitan el tratamiento innecesario de datos personales, sin perder funcionalidad en el propio sistema informático.

Ejemplo:
Los escáneres de personas utilizados con finalidades policiales deben diseñarse de manera que respeten la intimidad de las personas que se inspeccionan y, al mismo tiempo, cumplan su propósito. Por lo tanto, la imagen del cuerpo en estas herramientas tiene que ser borrosa por defecto.

19. Control externo

Debe existir, al menos, una autoridad de control independiente responsable de garantizar y supervisar que el tratamiento de datos cumpla con la normativa internacional y nacional en el sector de las fuerzas del orden.

Algunos Estados pueden exigir más de una autoridad de control, mientras que otros preferirán tener una única autoridad de control, responsable de la totalidad de la supervisión de las operaciones de tratamiento de datos.

El órgano de control debe ser totalmente independiente, lo que significa que no pertenecerá al organismo policial ni estará dirigido por otro órgano del poder ejecutivo de una administración nacional. Debe disponer de recursos suficientes para llevar a cabo sus tareas y funciones y no recibirá instrucciones de nadie. La independencia personal de su máximo jerarca/presidente, incluida la independencia política, financiera, funcional y operativa, son factores decisivos a la hora de juzgar la independencia del órgano de control.

La normativa nacional debe conferirle poderes consultivos, de investigación y de ejecución que le permitan investigar las reclamaciones, disponer de medidas reglamentarias o poder imponer sanciones cuando sea necesario. Los instrumentos jurídicos y administrativos de que dispone deberán ser eficaces y sus decisiones deberán tener fuerza ejecutiva.

Las autoridades de control deben tener la capacidad de cooperar en cuestiones de carácter policial tanto bilateralmente como a través del Comité Consultivo del Convenio 108.

Ejemplo:

La autoridad de control debe ser independiente y debe disponer de todas las facultades necesarias para llevar a cabo su tarea. La autoridad de control creada en el seno de un ministerio o la propia Policía no cumple esta obligación.

Glosario/Definiciones

A los efectos de la presente Guía:

a. «datos personales» significa cualquier información relativa a una persona física identificada o identificable («titular de los datos»);

b. «datos sensibles» significa datos genéticos, datos personales relativos a delitos, procedimientos penales y condenas, y medidas de seguridad conexas, datos biométricos que permitan identificar a una persona de forma inequívoca, datos personales para la información que revelen en relación con el origen racial o étnico, las preferencias políticas, la afiliación sindical, las convicciones religiosas o de otro tipo, la salud e informaciones referentes a la salud o la vida sexual;

c. «datos genéticos» significa datos relacionados con características genéticas, heredadas o adquiridas durante el desarrollo prenatal, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente;

d. «datos biométricos» significa datos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona;

e. «tratamiento de datos» significa cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, como la recopilación, el

almacenamiento, la conservación, la modificación, la recuperación, la divulgación, la facilitación, la supresión, la destrucción o la realización de operaciones lógicas o aritméticas sobre dichos datos. Cuando no se utilice el tratamiento automatizado, se entenderá por tratamiento de datos una operación o conjunto de operaciones realizadas con datos personales dentro de un conjunto estructurado de dichos datos que sean accesibles o recuperables con arreglo a criterios específicos;

f. «responsable» significa la persona física o jurídica, la autoridad pública, el servicio, la oficina o cualquier otro organismo que, sola o en conjunto con otros, tenga poder de decisión en materia de tratamiento de datos;

g. «destinatario» significa persona física o jurídica, autoridad pública, servicio, oficina o cualquier otro organismo que recibiere comunicación de datos;

h. «encargado» significa la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

i. «Internet de las cosas» (IdC) significa la interconexión de dispositivos físicos, vehículos (también denominados «dispositivos conectados» y «dispositivos inteligentes»), edificios y otros elementos integrados con electrónica, software, sensores, accionadores y conectividad de red que permiten a estos objetos recoger e intercambiar datos;

j. «técnicas especiales de investigación» significa las técnicas aplicadas por las autoridades competentes en el contexto de las investigaciones penales a efectos de prevenir, detectar, investigar, enjuiciar y reprimir delitos graves, con la finalidad de recopilar información de forma que no se alerte a las personas afectadas;

k. «tecnologías de protección del derecho a la privacidad» (PET) significa una serie de diferentes tecnologías para proteger los datos personales en los sistemas informáticos. El aspecto más importante para el uso de las PET es determinar si se necesita información de carácter personal en la etapa de desarrollo o diseño de un nuevo sistema informático o cuando se actualiza uno existente.