MANUAL

Guía para prevenir la elaboración ilícita de perfiles en la actualidad y en el futuro

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

En internet existe abundante información sobre la Agencia de los Derechos Fundamentales de la Unión Europea. Se puede acceder a dicha información a través del sitio web de la FRA en fra.europa.eu

Fotos (portada y página interior, de izquierda a derecha): © stock.adobe.com-Savvapanf Photo.

Más información sobre la Unión Europea en internet (http://europa.eu).

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2019

Print:	ISBN 978-92-9474-751-8	doi:10.2811/938618	TK-06-18-031-ES-C
PDF:	ISBN 978-92-9474-750-1	doi:10.2811/510128	TK-06-18-031-ES-N

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Guía para prevenir la elaboración ilícita de perfiles en la actualidad y en el futuro

Índice

Figuras y cuadros

Acrónimos y abreviaturas

CEDH	Convenio Europeo de Derechos Humanos
EIPD	Evaluación de impacto relativa a la protección de datos
ENISA	Agencia de Seguridad de las Redes y de la Información de la Unión Europea
EU-MIDIS	Encuesta de la Unión Europea sobre las minorías y la discriminación
FRA	Agencia de los Derechos Fundamentales de la Unión Europea
Frontex	Agencia Europea de la Guardia de Fronteras y Costas
GT29	Grupo de Trabajo del Artículo 29
NTP	Nacional de un tercer país
OACDH/ACNUDH	Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos
ONU	Organización de las Naciones Unidas
OSCE	Organización para la Seguridad y la Cooperación en Europa
PEC	Plan de estudios común
RGPD	Reglamento General de Protección de Datos
SEIAV	Sistema Europeo de Información y Autorización de Viajes
SEPD	Supervisor Europeo de Protección de Datos
SES	Sistema de Entradas y Salidas
SIS II	Sistema de Información de Schengen de segunda generación
TEDH	Tribunal Europeo de Derechos Humanos
TI	Tecnología de la información
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea
UNHRC	Comisión de Derechos Humanos de las Naciones Unidas
VIS	Sistema de Información de Visados

Introducción

A impulso de los avances tecnológicos, la elaboración de perfiles ha experimentado un creciente auge en contextos muy diversos, como el del *marketing*, el empleo, la sanidad, las finanzas, el control policial y fronterizo y la seguridad. El uso de herramientas de elaboración de perfiles con el fin de facilitar el trabajo de los agentes de policía y los guardias de frontera ha suscitado creciente atención en los Estados miembros de la Unión Europea durante los últimos años. Los agentes de policía y los guardias de fronteras utilizan de manera habitual y legítima perfiles con fines de prevención, investigación y enjuiciamiento de delitos penales, así como de prevención y detección de la inmigración irregular. Ahora bien, la elaboración ilícita de perfiles puede socavar la confianza en las autoridades, en particular las autoridades policiales, y estigmatizar a determinadas comunidades. Esto, a su vez, puede agravar las tensiones entre dichas comunidades y las autoridades policiales debido a la utilización de perfiles que pueden considerarse discriminatorios.

La presente guía explica en qué consiste la elaboración de perfiles, los marcos jurídicos que la regulan, y por qué practicarla de manera lícita no solo es necesario para respetar los derechos fundamentales, sino también crucial para la eficacia de la actuación policial y la gestión de fronteras. Además, la guía contiene orientaciones prácticas sobre cómo evitar la utilización ilícita de perfiles en las operaciones policiales y en la gestión de fronteras. Los principios y prácticas recogidos en la presente guía se sustentan en ejemplos, casos prácticos y jurisprudencia de la UE y de otros países.

¿Por qué es necesaria esta guía?

La elaboración de perfiles suscita una serie de inquietudes en relación con los derechos fundamentales ([1]). La utilización de perfiles comporta en la práctica el riesgo de violar principios jurídicos ya consolidados, como la igualdad y la no discriminación, así como los derechos de respeto a la intimidad y la protección de los datos personales. Además, su eficacia en la lucha contra las actividades ilegales ha suscitado dudas, así como las posibles consecuencias negativas sobre las relaciones entre las autoridades (incluida la policía y la guardia de fronteras) y las comunidades a las que sirven.

En respuesta a estas inquietudes, la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) publicó en 2010 la guía *Por una actuación policial más eficaz — Guía para entender y evitar la elaboración de perfiles étnicos discriminatorios*. Enfocada hacia el uso de perfiles en el contexto policial, dicha guía se centraba en particular en el ejercicio de las facultades de identificación y de registro. Su objeto era facilitar a los mandos intermedios herramientas destinadas a evitar el uso de perfiles discriminatorios basados en motivos étnicos.

Desde entonces, los avances tecnológicos han modificado considerablemente la naturaleza de la elaboración de perfiles. En la actualidad, la elaboración de perfiles toma en gran medida como base los resultados del análisis informático de grandes conjuntos de datos. Desde el punto de vista jurídico, las normas en materia de protección de datos, reformadas y más estrictas, aplicadas en la UE desde mayo de 2018, fijan nuevos parámetros para la recogida, el análisis y el uso de los datos personales.

Esta guía actualizada tiene en cuenta los significativos cambios introducidos con el fin de articular y ampliar la guía de 2010 para reflejar las nuevas realidades jurídicas y prácticas. El criterio desde el que se aborda la elaboración ilícita de perfiles es más amplio, ya que incorpora:

- la elaboración de perfiles en el contexto de la gestión de fronteras,
- la elaboración de perfiles discriminatorios por motivos de todo tipo, como la nacionalidad, la edad y el género, además del origen étnico, y
- la elaboración de perfiles algorítmica o informatizada.

Esta versión de 2018 incorpora también nuevos ejemplos y estudios de caso que reflejan las evoluciones e innovaciones registradas en materia de elaboración de perfiles.

([1]) Véase FRA (2018e), pp. 85-87; FRA (2017c), pp. 88-89; y FRA (2016), pp. 83-85.

¿Quién debe utilizar la presente guía?

La guía tiene como destinatarios principales a los instructores responsables de la formación de agentes de policía y guardias de fronteras. También resultará útil para los mandos intermedios que deseen aplicar lícitamente las técnicas de elaboración de perfiles. Su finalidad es incrementar los conocimientos teóricos y prácticos en materia de elaboración de perfiles, e ilustrar en términos concretos cómo es posible efectuar perfiles respetando los derechos fundamentales.

En la presente guía se analiza el uso de los perfiles por parte de agentes de policía de primera línea —por ejemplo, en el marco de actuaciones de identificación y registro— así como en las inspecciones efectuadas por los guardias de frontera en los pasos fronterizos, en particular cuando se toma la decisión de remitir a una persona a una inspección de «segunda línea» más exhaustiva. Por lo que respecta a la gestión de fronteras, constituye una herramienta de formación a disposición de quienes imparten el plan de estudios común para la formación de la guardia de fronteras en virtud del artículo 36, apartado 5, del Reglamento sobre la Guardia Europea de Fronteras y Costas [Reglamento (UE) 2016/1624].

La guía también aborda la elaboración de perfiles basada en el análisis de conjuntos de datos a gran escala, en particular los regulados por el Derecho de la Unión Europea. La elaboración de perfiles en otras situaciones, como la efectuada en el sector privado con fines comerciales, trasciende el ámbito de aplicación de la presente guía. La FRA continúa investigando esta cuestión ([2]).

Cómo utilizar esta guía

La presente guía recoge los principios y prácticas esenciales que regulan la elaboración de perfiles en el contexto de la actuación policial y la gestión de fronteras. Es posible leerla en su integridad o utilizarla como material de apoyo para las actividades formativas.

La guía se divide en tres capítulos. El capítulo 1 explica el concepto de elaboración de perfiles, clarifica cuándo se trata de una actividad ilícita y describe las posibles consecuencias negativas que puede acarrear para las personas físicas, las comunidades y para el ejercicio de las competencias en materia de actuación policial y gestión de fronteras. El capítulo 2 detalla los principios y prácticas que deben orientar la actuación de los agentes de policía y los guardias de fronteras que elaboren perfiles lícitamente. Por último, el capítulo 3 se centra en la elaboración de perfiles por medios

([2]) Véase el proyecto de la FRA sobre inteligencia artificial, macrodatos y derechos fundamentales.

algorítmicos. Dado que la práctica en este ámbito está menos desarrollada, esta sección recoge un menor número de ejemplos concretos. En su lugar, presenta los principales riesgos que comporta para los derechos fundamentales la elaboración de perfiles por medios informáticos, y expone los principales requisitos legales contemplados en el Reglamento General de Protección de Datos (RGPD) y en la Directiva sobre la policía.

Una serie de elementos visuales ponen de relieve los diferentes aspectos de la guía. Los mensajes principales se resumen en puntos clave y se destacan en recuadros de color amarillo. Los recuadros de color azul claro ponen de relieve aspectos esenciales del marco jurídico y los de color verde presentan ejemplos prácticos. Otros recuadros resaltan aspectos importantes para el análisis, casos prácticos y ejemplos tomados de la jurisprudencia. Pese a que se han intentado diversificar los estudios de casos, el número de ejemplos que tienen por origen el Reino Unido es desproporcionadamente elevado. Ello se debe a que en el Reino Unido la elaboración ilícita de perfiles es una cuestión abordada desde la década de 1980, mientras que en otros Estados miembros solo se le ha dado reconocimiento más recientemente. Es decir, que el Reino Unido ha desarrollado políticas y prácticas más amplias y duraderas en este ámbito, de las que es posible extraer ejemplos.

¿Cómo se ha elaborado esta guía?

La FRA organizó una reunión con expertos procedentes de diversos ámbitos con el fin de analizar una versión preliminar de la guía y colaborar en la elaboración del producto final.

A este respecto, la FRA desea expresar su agradecimiento a los expertos de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACDH), la Agencia Europea de la Guardia de Fronteras y Costas (Frontex), la Oficina de Instituciones Democráticas y Derechos Humanos (OIDDH) de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Amnistía Internacional, la Red Europea contra el Racismo (ENAR), el Centro Internacional para el Desarrollo de Políticas Migratorias (CIDPM), el FIZ Karlsruhe, Leibniz Institut für Informationsinfrastruktur GmbH, European Digital Rights, Open Society Initiative for Europe y representantes del Defensor del Pueblo de Francia, de los cuerpos policiales de los Países Bajos, Dinamarca y Austria y de la Guardia de Fronteras de Polonia por sus valiosas aportaciones durante la elaboración de esta guía.

Resumen de los puntos principales

1. La elaboración de perfiles nunca puede basarse únicamente en características protegidas

- La elaboración de perfiles implica **clasificar a las personas** en función de sus características.
- Para recoger y tratar **datos personales**, las autoridades policiales y las autoridades responsables de la gestión de fronteras deben asegurarse de que la recogida y el tratamiento de datos cuentan con una base jurídica, con un fin legítimo y válido y con que se cumplan los criterios de necesidad y proporcionalidad.
- **Características protegidas** como la raza, el origen étnico, el género o la religión pueden figurar entre los factores que dichas autoridades tengan en cuenta a la hora de ejercer sus competencias, pero **no pueden ser la única ni la principal razón para singularizar a una persona concreta**. (Para más información sobre las «características protegidas», véase el apartado 1.2.1).
- La elaboración de perfiles basados única o principalmente en una o varias características protegidas equivale a discriminación directa y, por lo tanto, constituye una actividad **ilícita** que **viola los derechos y libertades individuales.**

2. Todo encuentro con personas físicas debe ser respetuoso, profesional e informativo

- Un **encuentro cualitativamente satisfactorio** no descarta de por sí la introducción de sesgos en la elaboración de perfiles, pero redunda en una mayor probabilidad de que el encuentro se desarrolle por los cauces y se atenúe la sensación negativa que puede deparar el hecho de ser identificado por un agente de policía o un guardia de fronteras. En el ámbito de la gestión de fronteras, la conducta profesional y respetuosa está expresamente recogida como una obligación legal.
- **Una conducta profesional y respetuosa** depara por lo general en el interesado una mayor satisfacción con el encuentro.
- **Explicar las razones por las que se procede a una identificación** contribuye a generar entre los ciudadanos mayor confianza en las operaciones desarrolladas por la policía y la guardia de fronteras y mitiga la impresión de que la elaboración de perfiles pueda estar sesgada.
- No obstante, el respeto y la cortesía **nunca justifican la realización ilícita de inspecciones fronterizas o actuaciones de identificación y registro**.

3. La elaboración de perfiles debe estar justificada por motivos objetivos y razonables

- Para que se identifique y se someta lícitamente a una persona a una inspección fronteriza de segunda línea, deben **existir motivos de sospecha razonables y objetivos**.
- Las características personales pueden utilizarse como factores legítimos para la elaboración de perfiles. No obstante, para evitar discriminaciones, ***también*** **deben existir motivos de sospecha razonables** basados en información diferente de la relativa a las características protegidas.
- Las actuaciones policiales y la gestión fronteriza basadas en **información de inteligencia específica y actualizada** tienden a ser más **objetivas**.
- Es esencial que la decisión de identificar a una persona o someterla a una inspección fronteriza de segunda línea **no se base exclusivamente en la *impresión*** que pueda deparar en el agente, ya que con ello se corre el riesgo de que esta impresión esté basada en sesgos, estereotipos o prejuicios.

4. La elaboración ilícita de perfiles tiene efectos negativos sobre la labor policial y la gestión de fronteras

- **Las prácticas ilícitas de elaboración de perfiles debilitan la confianza en la policía y en la guardia de fronteras**. Pueden deteriorar la relación entre los policías o guardias de fronteras y los miembros de minorías u otras comunidades que pudieran sentirse señaladas. Esta sensación de injusticia puede llevar a que algunas personas y grupos pierdan la confianza en la policía y en otras autoridades, y a que por este motivo disminuyan las denuncias de delitos a la policía y la cooperación con las autoridades. A su vez, las autoridades pueden ver a ciertos grupos bajo sospecha, lo que a su vez puede incrementar las prácticas ilícitas de elaboración de perfiles.
- **La elaboración ilícita de perfiles socava la eficacia en el uso de los perfiles**, ya que la proporción de personas que son identificadas, bien por la policía o bien en la frontera, no se corresponde necesariamente con las tasas de delitos registrados entre diferentes grupos.
- Cuando los agentes de policía o de gestión de fronteras actúan de manera desproporcionada contra un grupo minoritario, se corre el riesgo de que se produzca una **profecía autocumplida**, y aumente el número de detecciones o de inspecciones en la frontera.

5. La elaboración ilícita de perfiles tiene consecuencias jurídicas y financieras, y los agentes deben rendir cuentas por ello

- Los agentes de policía y de gestión de fronteras deben **responsabilizarse** de que la elaboración de perfiles se atenga a la ley.
- **Recoger datos fiables, precisos y oportunos** es crucial para garantizar la rendición de cuentas.
- Unos **mecanismos de reclamación eficaces** pueden surtir un efecto disuasorio en relación con los abusos de poder y contribuir a asegurar y restablecer la confianza pública en las operaciones desarrolladas por las autoridades policiales y los guardias de fronteras.
- **Las reuniones de valoración con miembros de la ciudadanía** (para escuchar sus opiniones, analizar la elaboración de perfiles y conocer su valoración de las operaciones) brindan la oportunidad de extraer lecciones importantes y mejorar los procedimientos empleados en la elaboración de perfiles.

6. La elaboración algorítmica de perfiles debe respetar garantías específicas en materia de protección de datos

- En el desarrollo y uso de perfiles por medios algorítmicos, cabe la posibilidad de que se introduzca un **sesgo** en cada etapa del proceso. Para evitar esta y otras posibles violaciones de los derechos fundamentales, tanto **los expertos en TI como los agentes encargados de la interpretación de los datos deberán tener una comprensión clara de los derechos fundamentales**.
- Es crucial utilizar **datos fiables**. Introducir en un algoritmo datos que reflejen sesgos vigentes o procedentes de fuentes poco fiables redundará en resultados sesgados y no fiables.
- La elaboración algorítmica de perfiles debe ser **legítima, necesaria** y **proporcionada.**
- El tratamiento de datos debe tener **un fin específico.**
- Los interesados tienen **derecho a ser informados** mediante la notificación de información sobre los datos personales que se recojan y se conserven, sobre el tratamiento y su finalidad, y sobre sus derechos.
- Los datos deben ser **recogidos, tratados y conservados con seguridad.** Las autoridades deben documentar las actividades de tratamiento en un expediente (incluida información sobre el uso que se hace de los datos) y de los registros relacionados (incluida información sobre las personas que acceden a los datos).
- Es preciso **prevenir y detectar** el tratamiento ilícito de los datos: 1) mediante evaluaciones de impacto previas, y 2) mediante el uso de herramientas de privacidad integradas «desde el diseño» en el algoritmo.

Sitios web pertinentes

Unión Europea
Tribunal de Justicia de la Unión Europea (TJUE): http://www.curia.eu
Legislación de la UE: http://eur-lex.europa.eu/
Agencia de los Derechos Fundamentales de la Unión Europea (FRA): http://www.fra.europa.eu
Parlamento Europeo: http://www.europarl.europa.eu
Consejo de Europa
Comité de Ministros del Consejo de Europa: http://www.coe.int/cm
Tribunal Europeo de Derechos Humanos (TEDH): http://www.echr.coe.int
Organización de las Naciones Unidas
Oficina del Alto Comisionado para los Derechos Humanos (OACDH): http://www.ohchr.org
Lucha contra la discriminación
Comisión Europea contra el Racismo y la Intolerancia (ECRI): http://www.coe.int/ecri
Red europea de organismos nacionales para la igualdad (Equinet): http://www.equineteurope.org/
Organismos nacionales de igualdad: http://www.archive.equineteurope.org/-Equinet-Members-
Protección de datos
Supervisor Europeo de Protección de Datos (SEPD): https://edps.europa.eu/
Comité Europeo de Protección de Datos (CEPD): https://edpb.europa.eu
Autoridades nacionales de protección de datos: https://edpb.europa.eu/about-edpb/board/members_es
Organismos con funciones policiales
Red de autoridades independientes de reclamación contra cuerpos policiales (IPCAN): https://ipcan.org/
Agencia de la Unión Europea para la Formación Policial (CEPOL): https://www.cepol.europa.eu/
Agencia de la Unión Europea para la Cooperación Policial (Europol): https://www.europol.europa.eu/
Gestión de fronteras
Agencia Europea de la Guardia de Fronteras y Costas (Frontex): https://frontex.europa.eu/
Oficina Europea de Apoyo al Asilo (EASO): https://www.easo.europa.eu/
Bases de datos de gran escala
Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA): https://www.eulisa.europa.eu/

1 Punto de partida: ¿qué es la elaboración de perfiles?

En este capítulo se explica en qué consiste la elaboración de perfiles y cuáles son los principales derechos fundamentales que pueden verse afectados. En él se presenta la elaboración de perfiles en el contexto de las actividades policiales y de gestión de fronteras, en función de tres elementos esenciales:

- El concepto de elaboración de perfiles y su aplicación por parte de las autoridades policiales y responsables de la gestión de fronteras. En esta sección se presentan también algunos tipos de elaboración de perfiles.

- Los principales derechos fundamentales que deben respetarse cuando se aspira a elaborar perfiles de forma lícita, concretamente la no discriminación y los derechos de respeto a la vida privada y la protección de datos.

- Los posibles efectos negativos derivados del uso de perfiles, en particular las posibles consecuencias para las personas físicas y para las relaciones con las comunidades, así como la confianza en las autoridades policiales y las autoridades responsables de la gestión de fronteras.

1.1. Definición de elaboración de perfiles

La elaboración de perfiles implica **clasificar a las personas** de acuerdo con sus características personales. Dichas características pueden ser «invariables» (como la edad o la altura) o «variables» (como las prendas utilizadas, los hábitos, las preferencias y otros elementos del comportamiento). Para elaborar perfiles se utiliza la minería de datos, mediante la cual se clasifica a las personas **«en virtud de algunas de sus**

características observables a fin de deducir, con un cierto margen de error, otras que no son observables» ([3]).

Puntos clave

- La elaboración de perfiles implica **clasificar a las personas** de acuerdo con las características que se les suponen.
- La elaboración de perfiles tiene dos finalidades principales en el contexto de la actividad policial y la gestión de fronteras: **identificar a personas conocidas en virtud de cierta información de inteligencia relativa a una persona concreta**, y como **método predictivo,** identificar a personas «desconocidas» que puedan resultar de interés para las autoridades policiales y las autoridades responsables de la gestión de fronteras. En ambos casos, pueden existir sesgos conscientes o inconscientes que pueden resultar discriminatorios.
- Las actividades de elaboración de perfiles realizadas por agentes de policía y guardias de fronteras pueden estar influenciadas por sesgos que tengan origen en sus experiencias individuales o institucionales. Estos sesgos pueden alterar el proceso de evaluación en la elaboración de los perfiles, y afectar tanto a la legalidad como a la eficacia de la acción policial.
- Los estereotipos pueden reflejar cierta verdad estadística. Sin embargo, aun en estos casos **los datos seguirán siendo problemáticos** si como resultado se trata a una persona como parte de un grupo y no sobre la base de sus circunstancias particulares.
- En el desarrollo y aplicación de la elaboración algorítmica de perfiles, **se puede introducir un sesgo en cada fase del proceso**. Para evitar esta y otras posibles violaciones de los derechos fundamentales, los expertos en TI que diseñen los algoritmos y los agentes que recojan e interpreten los datos deberán tener un conocimiento claro de dichos derechos y de cómo aplicarlos en este contexto.

Las prácticas de elaboración de perfiles tienen por objeto:

- Generar conocimiento, mediante el análisis de los datos existentes para formular premisas en relación con una persona. Se utilizan experiencias anteriores y análisis estadísticos para establecer correlaciones entre determinadas características y determinados resultados o conductas.

- Facilitar los procesos decisorios, utilizando dichas correlaciones para tomar decisiones sobre las medidas que deban adoptarse.

([3]) Dinant J.-M., Lazaro C., Poullet Y., Lefever N. y Rouvroy A. (2008), p. 3.

Esto convierte la elaboración de perfiles en una herramienta poderosa a disposición de los policías y los guardias de fronteras. Sin embargo, entraña ciertos riesgos importantes:

- Al elaborar perfiles, se establecen correlaciones genéricas que pueden no ser correctas para todas las personas. Cualquiera puede ser «la excepción a la regla».

- Los perfiles pueden generar correlaciones incorrectas, tanto para ciertas personas como para grupos.

- Los perfiles pueden crear estereotipos nocivos y provocar discriminación.

- Algunos estereotipos pueden reflejar una verdad estadística. Sin embargo, incluso en estos casos, los estereotipos pueden ser problemáticos si resultan en que se trata a una persona como miembro de un grupo antes que como un individuo.

Ejemplos

Elaboración de perfiles potencialmente inexactos

La premisa de que «las mujeres viven más tiempo que los hombres» se sustenta en estudios objetivos; sin embargo, un hombre concreto puede vivir más tiempo que una mujer concreta. Por consiguiente, tomar decisiones relacionadas con las mujeres partiendo de esta premisa entraña el riesgo de equivocarse en un caso concreto, y solo sería un procedimiento correcto tomando como referencia el término medio.

Puede que haya personas que permitan que sus familiares o amigos utilicen su coche, lo que restará fiabilidad a un perfil de riesgo en la conducción basado en la propiedad del vehículo.

1.1.1. Elaboración de perfiles en el contexto de la acción policial y la gestión de fronteras

Los agentes de policía y los guardias de fronteras utilizan de manera habitual y legítima perfiles con fines de prevención, investigación y enjuiciamiento de delitos penales, así como de prevención y detección de la inmigración irregular.

La elaboración de perfiles es «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la ubicación o los movimientos de dicha persona física» ([4]). Los resultados de este tratamiento de datos se utilizan para orientar la acción policial y de gestión de las fronteras, como las actuaciones de identificación y registro, las detenciones, la denegación de acceso a ciertas zonas, o la realización de «inspecciones de segunda línea» en frontera de carácter más exhaustivo. La elaboración de perfiles tiene dos usos principales:

- Identificar a personas físicas en función de información de inteligencia específica. Se utiliza un perfil que recoge las características de determinados sospechosos, basadas en las pruebas recogidas acerca de un hecho concreto.

- Como método predictivo para identificar a personas «desconocidas» que puedan ser de interés para las autoridades policiales y de gestión de fronteras. Se basa en el análisis de los datos y en premisas basadas en la experiencia. Lo ideal es que los métodos predictivos estén enfocados en el comportamiento. Sin embargo, no suele ser esto (o no es esto exclusivamente) lo que ocurre en la práctica, ya que no se enfocan (o no solo) en el comportamiento sino en características físicas visibles, como la edad, el género o la etnia.

El cuadro 1 presenta una comparación de las principales características de estos dos tipos de perfiles en el contexto de la actuación policial.

([4]) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DO L 119 (Directiva sobre la policía), artículo 3, apartado 4.

Cuadro 1: Características de la actuación policial basada en información de inteligencia específica y en métodos predictivos

	Actuación policial basada en información concreta	Policía predictiva
Contexto	Se ha cometido un delito o se ha emitido una alerta relativa a una persona concreta	No se ha cometido ningún delito o no se ha emitido una alerta relativa a una persona concreta
Enfoque	Reactivo	Proactivo
Objetivo	Detener a los sospechosos	Predecir dónde y cuándo podrían cometerse delitos o quién podría intentar entrar en el país irregularmente
Datos utilizados	Información de inteligencia específica relacionada con el caso («perfil individual»)	Información de inteligencia genérica relacionada con varios casos
Tipo de proceso	Se combinan procesos basados en datos y procesos humanos	Principalmente basado en datos («análisis de riesgos»)

Fuente: FRA, 2018.

Ambos tipos de prácticas pueden ser ilícitas si los perfiles no se elaboran de acuerdo con garantías concretas, incluida una justificación objetiva y razonable. El capítulo 2 y el capítulo 3 contienen información práctica acerca de cómo velar por que la elaboración de perfiles sea lícita y conforme a los derechos humanos.

1.1.2. Definición de elaboración algorítmica de perfiles

Debido al rápido avance de la tecnología, los perfiles se elaboran cada vez más con arreglo a la información almacenada en bases de datos y sistemas informáticos (sistemas TI). Existen distintas técnicas para elaborar perfiles por medios algorítmicos basadas en correlaciones y patrones de datos. La elaboración algorítmica de perfiles permite a los agentes de policía y de gestión de fronteras actuar contra personas o grupos específicos que constituyen un riesgo cierto en virtud del análisis de los datos.

Esta práctica entraña importantes problemas para los derechos fundamentales, como posible discriminación y violaciones de los derechos de respeto a la vida privada y la protección de datos. En este apartado de la guía se explica cómo pueden los agentes de policía y de gestión de fronteras utilizar y tratar los datos respetando los derechos fundamentales en su trabajo cotidiano.

Tratamiento de datos personales: ¿qué dice la ley?

Las normas que regulan el tratamiento de datos personales para elaborar perfiles están recogidas en el marco jurídico de protección de datos de la UE. El artículo 4, apartado 4, del Reglamento General de Protección de Datos (RGPD) y el artículo 3, apartado 4, de la Directiva sobre la policía recogen la definición de «"elaboración de perfiles": toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física».

El artículo 22, apartado 1, del RGPD establece que solo se podrá aceptar la elaboración de perfiles cuando la decisión no se base únicamente en el tratamiento automatizado y no produzca efectos jurídicos en los interesados que les afecten significativamente.

La elaboración de perfiles sujeta al ámbito de aplicación de la Directiva sobre la policía (véase la sección 3.1 sobre elaboración algorítmica de perfiles y protección de datos) debe cumplir lo dispuesto en el artículo 11, apartado 3, de la Directiva sobre la policía, que establece que «[l]a elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales establecidas en el artículo 10 (*) quedará prohibida, de conformidad con el Derecho de la Unión».

(*) «Categorías especiales de datos personales» son «datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o la vida sexual o las orientaciones sexuales de una persona física». *Véase* la Directiva sobre la policía, artículo 10, apartado 1.

El método utilizado para generar perfiles con procesos algorítmicos es parecido a la técnica conocida como «**análisis conductual**», por la que se establecen relaciones entre determinadas características y patrones de conducta. La figura 1 indica cómo utilizar algoritmos para realizar predicciones.

Figura 1: Elaboración algorítmica de perfiles en el contexto de la acción policial y la gestión de fronteras

Fuente: *FRA, 2018 [adaptado de/basado en Perry, W. L.,* et al. *(2013), pp. 11–15, y Zarsky, T. Z. (2002–2003), pp. 6–18].*

Análisis de cómo se utilizan los algoritmos para facilitar la toma de decisiones

Con el incremento de la disponibilidad y el uso de datos, el proceso decisorio se ve cada vez más facilitado o reemplazado por métodos de modelización predictiva, lo que se conoce generalmente como «uso de algoritmos». Un algoritmo es una secuencia de comandos enviados a un ordenador para transformar los datos de partida en resultados. Muchos algoritmos se basan en métodos estadísticos, y utilizan técnicas que calculan las relaciones entre distintas variables. Por ejemplo, los datos sobre la cantidad de alcohol que consume un grupo de personas y la esperanza de vida dentro de ese grupo pueden utilizarse conjuntamente para calcular la influencia media del consumo de alcohol sobre la esperanza de vida.

El resultado de los algoritmos es siempre una probabilidad, lo que significa que existe un cierto grado de incertidumbre acerca de las relaciones o clasificaciones establecidas. Por ejemplo, los proveedores de correo electrónico utilizan algoritmos para determinar qué mensajes son correo no deseado y enviarlos a la carpeta correspondiente. Los algoritmos funcionan bien, pero no son perfectos. A veces no se detecta el correo no deseado y este acaba en la bandeja de entrada; esto es un falso negativo (es decir, no se identifica falsamente como correo no deseado). También puede darse el caso, aunque no es tan frecuente, de que un correo legítimo sea filtrado a la carpeta de correo no deseado; esto es un falso positivo.

Tener un conocimiento básico sobre cómo ayudan los algoritmos a tomar decisiones permite a los profesionales detectar posibles problemas y hacerse las preguntas adecuadas en relación con el uso de algoritmos, incluido su potencial de discriminación y violación de los derechos de respeto a la vida privada y la protección de datos.

Para más información, véase FRA (2018b).

La creación de algoritmos con fines predictivos es un proceso complejo que requiere la toma de múltiples decisiones por diversas personas implicadas en el proceso. En este sentido, no solo se refiere a las normas que sigue un ordenador, sino también al proceso de recogida, preparación y análisis de los datos. Se trata de un proceso humano que comprende varias fases, en las que desarrolladores y responsables deben tomar decisiones. El método estadístico es solo parte del proceso de elaboración de las normas finales utilizadas para formular predicciones, establecer clasificaciones o tomar decisiones ([5]). En cualquier caso, la forma de recoger y utilizar los datos puede ser discriminatoria.

Ejemplo

Para que sea eficaz y preciso, el software *de reconocimiento facial necesita alimentarse de grandes cantidades de imágenes y datos. Cuantos más datos reciba, más precisos serán sus resultados. Pero hasta la fecha, las imágenes utilizadas para adecuar los algoritmos han sido en gran medida de hombres blancos, con cifras comparativamente bajas de mujeres o personas de otro*

([5]) FRA (2018b), p. 4.

origen étnico. En consecuencia, los resultados generados por el software *son menos precisos y entrañan mayor probabilidad de inexactitud en relación con las personas pertenecientes a estos grupos. Cuando los policías o los guardias de fronteras los utilicen para elaborar perfiles y decidir, por ejemplo, si detienen a una persona, pueden producirse errores que perjudiquen seriamente los derechos y libertades de esa persona.*

Para más información, véase Center on Privacy and Technology at Georgetown Law (2016); y Buolamwini J., Gebru T. (2018).

En cada fase del proceso de elaboración algorítmica de perfiles, se puede introducir un sesgo. Para evitar sesgos discriminatorios y violaciones de los derechos a la protección de datos y a la intimidad, tanto las personas que diseñen los algoritmos como los agentes de policía y de gestión de fronteras que recojan e interpreten los datos deberán tener un conocimiento claro de los derechos fundamentales y su aplicación en este contexto.

Es crucial utilizar datos fiables. En la elaboración algorítmica de perfiles, debe evaluarse la calidad de los datos utilizados para comprobar que son fiables: a menor variabilidad, mayor fiabilidad. Si se utilizan datos que reflejen sesgos previos o que provengan de fuentes poco fiables para construir un algoritmo, se obtendrán resultados sesgados y poco fiables. También pueden producirse errores durante las predicciones realizadas a partir de los datos:

- Los falsos positivos se refieren a casos en que una persona es señalada e investigada a causa de una predicción errónea de que es constitutiva de riesgo.

- Los falsos negativos se refieren a personas que entrañan un verdadero riesgo en el contexto de las operaciones policiales y de gestión de fronteras, pero a las que el sistema no ha identificado como tales.

1.2. ¿Cuándo es ilícita la elaboración de perfiles?

Puntos clave

- Las características personales pueden utilizarse como factores legítimos para la elaboración de perfiles. Sin embargo, para evitar que se elaboren perfiles discriminatorios y, por tanto, ilícitos, también deben existir motivos de sospecha fundados basados en informaciones no relacionadas con los **motivos protegidos**.
  - Son motivos protegidos el sexo, la raza, el color, los orígenes étnicos o sociales, las características genéticas, la lengua, la religión o las convicciones, las opiniones políticas o de cualquier otra índole, la pertenencia a una minoría nacional, el patrimonio, el nacimiento, la discapacidad, la edad y la orientación sexual.
  - Los motivos protegidos pueden revelarse, deducirse o predecirse a partir de otros datos personales.
- Para recoger y tratar **datos personales**, las autoridades policiales y de gestión de fronteras deben asegurarse de tener una base jurídica, un fin legítimo y válido, y de que se cumplan los criterios de necesidad y proporcionalidad.
  - Se entiende por datos personales cualquier información que pueda utilizarse para identificar a una persona —directa o indirectamente—, en particular mediante un nombre, un número de identificación, datos de localización o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Si se utiliza de forma lícita, la elaboración de perfiles es una **técnica de investigación legítima**. Para que sea lícita, debe estar basada en **justificaciones objetivas y razonables** y respetar los derechos fundamentales, como el derecho a la no discriminación y a la protección de los datos personales. Se considerará que la elaboración de perfiles no tiene una justificación objetiva y razonable «si no persigue un objetivo legítimo o si no existe una relación razonable de proporcionalidad entre los medios empleados y el objetivo que se pretende alcanzar» ([6]).

La elaboración de perfiles puede afectar a muchos derechos fundamentales. Esta sección trata de los principales derechos fundamentales afectados por la elaboración de perfiles ilícita: el derecho a la no discriminación, y los derechos a la intimidad y a la protección de datos. Se considerará que la elaboración de perfiles es ilícita si:

- incluye actos de trato diferenciado injustificado basado en motivos protegidos (véase el apartado 1.2.1), o

([6]) Comisión Europea contra el Racismo y la Intolerancia (ECRI) (2007), apdo. 28.

- constituye una injerencia innecesaria en la vida privada de las personas físicas o no es conforme a las normas que regulan el tratamiento de datos personales (véase el apartado 1.2.2).

1.2.1. Prohibición de la discriminación

Prohibición de la discriminación: ¿qué dice la ley?

«**Se prohíbe toda discriminación**, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual» (*).

Artículo 21 de la Carta de los Derechos Fundamentales de la Unión Europea

«**El goce de los derechos reconocidos por la ley ha de ser asegurado sin discriminación alguna**, especialmente por razones de sexo, raza, color, lengua, religión, opiniones políticas o de otro carácter, origen nacional o social, pertenencia a una minoría nacional, fortuna, nacimiento o cualquier otra situación. Nadie podrá ser objeto de discriminación por parte de una autoridad pública, especialmente por los motivos mencionados en el párrafo 1».

Artículo 1 del Protocolo n.º 12 al Convenio para la Protección de los Derechos Humanos

(*) *Cabe señalar que, en la práctica, muchos Estados miembros han ampliado la protección contra la discriminación a motivos adicionales a los enumerados en la Carta y en el Convenio Europeo de Derechos Humanos (CEDH).*

Discriminación es «cuando [...] una persona es tratada de manera menos favorable de lo que sea, haya sido o vaya a ser tratada otra en una situación comparable» por razón de una característica personal percibida o real ([7]). Estas características se denominan «motivos protegidos» o «características protegidas» en la legislación contra la discriminación. Para más información sobre el derecho y la jurisprudencia

([7]) Directiva 2000/43/CE del Consejo, de 29 de junio de 2000, relativa a la aplicación del principio de igualdad de trato de las personas independientemente de su origen racial o étnico, DO L 180, artículo 2; y Directiva 2000/78/CE del Consejo, de 27 de noviembre de 2000, relativa al establecimiento de un marco general para la igualdad de trato en el empleo y la ocupación, DO L 303, artículo 2.

europeos en esta materia, véase la edición de 2018 del *Manual sobre el Derecho europeo en materia de no discriminación*, publicado conjuntamente por la FRA y por el Consejo de Europa ([8]).

Existen varios tipos de discriminación:

Discriminación directa es cuando una persona es tratada de manera menos favorable, *única o principalmente* por razón de un motivo protegido, como la raza, el género, la edad, la discapacidad o el origen étnico ([9]).

Ejemplo

En respuesta a una amenaza terrorista, se confiere a la policía la facultad de identificar y registrar a cualquier persona que se considere que puede estar involucrada en actividades terroristas. Se cree que la amenaza proviene de una organización terrorista activa en una determinada región del mundo, pero se carece de información de inteligencia más específica. Si un policía procede a la identificación de un hombre basándose única o principalmente en que su aspecto indique que puede ser originario de esa misma región del mundo, esto constituiría discriminación directa y sería ilícito.

Discriminación indirecta (también conocida como «discriminación de impacto desigual» en el contexto de la acción policial y la gestión de fronteras) es cuando una disposición, un criterio o una práctica *de carácter aparentemente neutro* colocaría a personas con determinadas características protegidas en una situación de particular desventaja en comparación con otras personas, a menos que tal disposición, criterio o práctica se justifiquen objetivamente por un fin legítimo y que los medios para alcanzar tal fin sean necesarios y proporcionados ([10]). La discriminación indirecta necesita en general estadísticas para valorar si una persona ha sido tratada, en la práctica, de manera menos favorable que otra por razón de su pertenencia a un grupo con determinadas características protegidas.

([8]) FRA y Consejo de Europa (2018).

([9]) Véase la nota anterior, p. 43.

([10]) Directiva 2000/78/CE del Consejo, de 27 de noviembre de 2000, relativa al establecimiento de un marco general para la igualdad de trato en el empleo y la ocupación, DO L 303 (Directiva de igualdad en el empleo), artículo 2; véase también FRA y Consejo de Europa (2018), p. 53.

Ejemplo

Para realizar controles rutinarios, las autoridades policiales deciden parar uno de cada diez coches en la ciudad X entre las 21.00 y la 1.00 horas; el 60 % de la población de la ciudad X que conduce durante estas horas es de ascendencia afrocaribeña, mientras que la población afrocaribeña de la ciudad y sus alrededores no supera el 30 %. Dado que es probable que este grupo se vea afectado más negativamente que otros, esto sería discriminación indirecta.

El análisis de la discriminación por un solo motivo no refleja adecuadamente las diversas manifestaciones del trato desigual. **Discriminación múltiple** es aquella que tiene lugar por varios motivos que operan por separado. Por ejemplo, puede que una persona sea discriminada no solo por su origen étnico, sino también por su edad y su género ([11]). La **discriminación interseccional** describe una situación en la que varios motivos operan simultáneamente e interactúan de manera que son inseparables y producen tipos concretos de discriminación (véase el recuadro Ejemplo).

Ejemplo

Un policía identifica y registra a un joven de ascendencia africana sin motivos razonables para sospechar que ha cometido un delito. No lo discrimina solo por su edad (no todos los jóvenes son identificados) o por su origen étnico (no todos los jóvenes de ascendencia africana son identificados), sino precisamente porque es al mismo tiempo joven y de ascendencia africana.

La discriminación también puede tener su origen en el tratamiento automatizado de datos personales y en el empleo de perfiles algorítmicos. La discriminación puede producirse durante el diseño y la ejecución de los algoritmos, debido a los sesgos que se incorporan en estos últimos —de forma consciente o no—, así como cuando se toman decisiones en virtud de la información obtenida.

El artículo 9, apartado 1, del RGPD establece específicamente que queda prohibido el tratamiento de categorías especiales de datos personales que revelen características personales, como el origen étnico o racial, las opiniones políticas, o las convicciones religiosas o filosóficas (véase la lista completa de motivos protegidos en la figura 7, apartado 2.2.4). Esta prohibición se puede levantar en casos concretos,

([11]) FRA y Consejo de Europa (2018), p. 59.

como la protección del interés público, siempre que la exención tenga base jurídica, sea proporcionada y necesaria, y establezca garantías adecuadas ([12]).

Del mismo modo, en el contexto de la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, el artículo 11, apartado 3, de la Directiva sobre la policía sobre el mecanismo de decisión individual automatizado prohíbe «[l]a elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales», incluidos los datos que revelen el origen étnico o racial y las convicciones religiosas, así como los datos genéticos y biométricos ([13]). Una vez más, se permiten excepciones a esta prohibición en algunos casos, pero deben ser necesarias, contar con garantías adecuadas, y tener una base jurídica o la finalidad de proteger los intereses vitales de una persona física ([14]).

Prohibición de elaborar perfiles discriminatorios: ¿qué dice la ley?

«**Queda prohibida la elaboración de perfiles que dé lugar a la discriminación** de personas físicas **por razones basadas en datos personales** que, por su naturaleza, son especialmente sensibles en relación con los derechos y las libertades fundamentales, con arreglo a las condiciones previstas en los artículos 21 y 52 de la Carta [de derechos fundamentales]».

Considerando 38 de la Directiva sobre la policía

«**La elaboración de perfiles que dé lugar a una discriminación** de las personas físicas basándose en las categorías especiales de datos personales establecidas en el artículo 10 (*) **quedará prohibida**, de conformidad con el Derecho de la Unión».

Artículo 11, apartado 3, de la Directiva sobre la policía

(*) Artículo 10 de la Directiva sobre la policía: «[...] datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos

([12]) Reglamento General de Protección de Datos (RGPD), artículo 9, apartado 2, letra g).

([13]) Para más información, véase Grupo de Trabajo del Artículo 29 (2017b).

([14]) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DO L 119 (Directiva sobre la policía), artículo 10.

dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física [...]».

«En la realización de inspecciones fronterizas, la guardia de fronteras no discriminará a las personas por motivos de sexo, origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual».

Artículo 7, apartado 2, del Código de fronteras Schengen

La prohibición de la discriminación no implica que no se puedan utilizar características personales como factores legítimos para elaborar perfiles en el contexto de investigaciones criminales o inspecciones fronterizas (véase la sección 2.3). Sin embargo, deben existir motivos razonables de sospecha basados en otra información que no sean los motivos protegidos. Por ejemplo, puede que una persona encaje con la descripción concreta de un sospechoso, o que su aspecto no se corresponda con la información que contiene su documento de viaje ([15]).

Análisis de la discriminación por motivos de nacionalidad

El artículo 21 de la Carta de los Derechos Fundamentales de la Unión Europea **limita la prohibición de la discriminación por motivos de nacionalidad a los ciudadanos de la Unión**. La Directiva sobre igualdad racial no incluye la nacionalidad entre los motivos protegidos.

Sin embargo, los Estados miembros han ampliado la prohibición de la discriminación para que comprenda la nacionalidad de diversas maneras. Por ejemplo, reconocer que la nacionalidad se utiliza a veces como indicador de raza, origen étnico o religión. En algunos de estos casos «las diferencias de trato por motivos de nacionalidad [...] [serán] consideradas infracciones de la legislación que prohíbe la discriminación por estos motivos» (véase *European network of legal experts in gender equality and non-discrimination*, 2016, p. 99). En la práctica, suele ser difícil distinguir la discriminación por motivos de nacionalidad de la discriminación por motivos de etnia.

El hecho de que la nacionalidad no se mencione expresamente como posible motivo de discriminación en el artículo 21 de la Carta refleja principalmente

([15]) Reino Unido, House of Lords (2006), Lord Scott, Opinions of the Lords of appeal for judgment in *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.* [2006] UKHL 12, 8 de marzo de 2006, apdo. 67.

el diferente estatuto que corresponde a los ciudadanos de la UE (y otras personas que gozan del derecho de libre circulación en virtud del Derecho de la Unión) y a los nacionales de terceros países en virtud del Derecho de la Unión. Esto tiene especial importancia en los procedimientos en frontera, donde la nacionalidad es el factor decisivo para determinar si una persona debe ser sometida a una inspección exhaustiva, o debe estar en posesión de un visado para entrar al espacio Schengen o transitar por él.

Al mismo tiempo, someter sistemáticamente a todas las personas de una determinada nacionalidad a la inspección de segunda línea podría ser una práctica discriminatoria. La nacionalidad puede ser una parte legítima de los perfiles de riesgo para detectar migración irregular o presuntas víctimas de trata de seres humanos, pero no debe ser el único o principal factor de una inspección de segunda línea. Además, al igual que en otros contextos, el trato diferenciado en función de la nacionalidad es discriminatorio y, por tanto, ilícito cuando se utiliza como indicador para discriminar por razón de motivos protegidos estrechamente ligados a la nacionalidad, como la raza, la etnia o la religión.

En sus Principios y Directrices recomendados sobre los derechos humanos en las fronteras internacionales de 2014, la Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos incluye la nacionalidad entre los motivos protegidos que no deben utilizarse para elaborar perfiles de inmigrantes (principio 8).

Jurisprudencia

En *Rosalind Williams Lecraft contra España*, un policía paró a una mujer en el andén de una estación de tren de España y le pidió que le mostrase sus documentos de identificación. La mujer preguntó al policía por qué había sido ella la única persona identificada en el andén y la respuesta fue: «porque eres negra». En su sentencia, la Comisión de Derechos Humanos de Naciones Unidas subrayó que, con carácter general, es legítimo realizar verificaciones de identidad en pro de la seguridad pública y con el fin de prevenir la delincuencia y controlar la inmigración irregular. Sin embargo, determinó que «cuando las autoridades efectúan dichas verificaciones las meras características físicas o étnicas de las personas objeto de los mismos no deben ser tomadas en consideración como indicios de su posible situación ilegal en el país. Tampoco deben efectuarse de manera tal que

solo las personas con determinados rasgos físicos o étnicos sean señaladas. Lo contrario no solo afectaría negativamente la dignidad de las personas afectadas, sino que además contribuiría a la propagación de actitudes xenófobas entre la población en general y sería contradictorio con una política efectiva de lucha contra la discriminación racial».

En 2017, se presentó una denuncia parecida al TEDH, en relación con el trato dispensado a un nacional paquistaní durante y después de ser identificado por la policía en España. El órgano jurisdiccional deberá decidir si el demandante sufrió discriminación por motivos de origen étnico durante la verificación de su identidad, y si existió violación del artículo 8 (derecho a la vida privada y familiar) debido a que las autoridades españolas no adoptaron todas las medidas razonables para descubrir si el incidente tenía motivaciones racistas. El caso está visto para sentencia en el momento de redactarse la presente guía.

Para más información, véase UNHRC, Rosalind Williams Lecraft contra España, Com. n.º 1493/2006 y TEDH, Zeshan Muhammad contra España, n.º 34085/17, presentada el 6 de mayo de 2017. Véase también FRA y Consejo de Europa (2018).

En *B.S. contra España,* una trabajadora sexual de origen nigeriano, que era residente legal en España, alegó que la policía española la maltrató física y verbalmente por razón de su raza, género y profesión. Afirmó que, a diferencia de otras trabajadoras sexuales de origen europeo, ella fue sometida a controles policiales reiterados y fue víctima de insultos racistas y sexistas. The AIRE Centre y la European Social Research Unit de la Universidad de Barcelona solicitaron al TEDH el reconocimiento de la discriminación interseccional. El Tribunal resolvió que había existido violación del artículo 3 (prohibición de los tratos inhumanos o degradantes), pero además examinó si también se había dejado de investigar un posible vínculo de causalidad entre las actitudes racistas alegadas y los actos violentos de la policía. En relación con este asunto, el TEDH resolvió que había existido violación del artículo 14 (prohibición de la discriminación), porque los órganos jurisdiccionales nacionales no habían tenido en cuenta la vulnerabilidad específica de la demandante, inherente a su condición de mujer africana que ejercía la prostitución. Aunque se adoptó un enfoque interseccional, la sentencia no utilizó el término «interseccionalidad».

Para más información, véase TEDH, B.S. contra España, n.º 47159/08, 24 de julio de 2012.

Análisis de la carga de la prueba

En 2016, el Tribunal de Casación francés dictó por primera vez una resolución sobre la cuestión de las verificaciones de identidad discriminatorias. En sus *Decisiones de 9 de noviembre de 2016*, el Tribunal resolvió que la policía realizó verificaciones de identidad discriminatorias a tres de trece hombres de origen africano o árabe. Determinó que, en estos casos, el Estado era responsable y debía indemnizar a los tres demandantes. En otros ocho casos, el Tribunal resolvió que las verificaciones de identidad impugnadas eran legales, ya que se basaban en elementos objetivos y, por tanto, no discriminatorios. Los jueces no dictaron sentencia en los otros dos casos, sino que los devolvieron a instancias inferiores para que se juzgaran de nuevo.

El Tribunal también aclaró la cuestión de la carga de la prueba en estos casos. Las verificaciones de identidad no se documentan cuando no son conducentes a procedimientos judiciales o administrativos. El Tribunal explicó que los demandantes debían proporcionar a los órganos jurisdiccionales elementos de prueba de la presunta discriminación. La policía debía demostrar que no había existido trato diferenciado en la realización de las verificaciones de identidad o que el trato diferenciado estaba justificado por elementos objetivos.

Además, el Tribunal determinó que los jueces pueden tener en cuenta —como elementos probatorios— estudios y estadísticas que reflejen la frecuencia de las verificaciones de identidad realizadas, por motivos discriminatorios, en el mismo grupo de población que el demandante (es decir, minorías visibles, determinadas por características físicas asociadas a su origen étnico presunto o real). Sin embargo, estas pruebas por sí solas no bastan para demostrar la existencia de discriminación.

Por tanto, el Tribunal resolvió que una verificación de identidad basada en características físicas asociadas a un origen étnico presunto o real, sin justificación objetiva previa, es discriminatoria y representa una mala praxis grave que, en estos tres casos, acarreaba la responsabilidad del Estado.

Para más información, véase Francia, Tribunal de Casación (Cour de Cassation), Décision 1245, 9 de noviembre de 2016.

1.2.2. Derecho al respeto a la vida privada y a la protección de los datos personales

Con arreglo al ordenamiento jurídico de la UE, el respeto a la vida privada (artículo 7 de la Carta) y la protección de los datos personales (artículo 8 de la Carta) son derechos distintos, aunque estrechamente relacionados. El derecho a la vida privada (o derecho a la intimidad) es un derecho más general, que prohíbe *cualquier injerencia* en la vida privada de una persona física. El concepto de vida privada no incluye simplemente lo que una persona desea mantener confidencial, sino también los medios a través de los cuales expresa su personalidad, por ejemplo, al elegir con quién interactúa o cómo se viste. La protección de los datos personales se limita a la evaluación del carácter lícito del *tratamiento de datos personales* ([16]). Cuando no se hace referencia específica al Derecho de la Unión, ambos conceptos se utilizan de forma indistinta para los fines de esta guía. Estos derechos no son absolutos y pueden limitarse en circunstancias concretas (véase el artículo 8 del CEDH y el artículo 52 de la Carta).

Derechos a la intimidad y a la protección de los datos personales: ¿qué dice la ley?

«1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

Artículo 8 del Convenio Europeo de Derechos Humanos

«Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones».

Artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea

«1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento

([16]) FRA, SEPD y Consejo de Europa (2018).

legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación [...]».

Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea

«1. Todo interesado tendrá derecho a no ser objeto de una decisión **basada únicamente en el tratamiento automatizado**, incluida la elaboración de perfiles, que **produzca efectos jurídicos** en él **o le afecte significativamente de modo similar**.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato [...];

b) está autorizada por el Derecho [...] que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado».

Artículo 22, apartados 1 y 2 del Reglamento General de Protección de Datos

«Los Estados miembros dispondrán la prohibición de las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, salvo que estén autorizadas por el Derecho de la Unión o del Estado miembro al que esté sujeto el responsable del tratamiento y que establezca medidas adecuadas para salvaguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento».

Artículo 11, apartado 1, de la Directiva sobre la policía

El Derecho derivado de la Unión profundiza en los derechos a la intimidad y la protección de los datos personales. Dos instrumentos legislativos especifican cómo se pueden recoger y tratar los datos personales. El Reglamento 2016/679 o Reglamento General de Protección de Datos (RGPD) establece los principios generales y las garantías que se aplican al tratamiento de los datos personales. Más concretamente, la Directiva 2016/680, conocida como la «Directiva sobre la policía», establece las normas que se aplican al tratamiento de datos personales en el contexto de las operaciones policiales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales. El cuadro 2 recoge los principios más importantes y algunas diferencias esenciales entre ambos instrumentos. Las leyes que regulan la creación de las grandes bases de datos de la UE utilizadas para la

gestión de fronteras, como el Sistema de Información de Visados (VIS), el Sistema de Entradas y Salidas (SES) o el Sistema Europeo de Información y Autorización de Viajes (SEIAV) incorporan también su respectivo marco de protección de datos (véase la sección 3.2 sobre las bases de datos de gran escala).

Cuadro 2: Requisitos de protección de datos: diferencias entre la Directiva sobre la policía y el RGPD

Principio de protección de datos	RGPD	Directiva sobre la policía
Licitud, lealtad, transparencia	Los datos personales deben ser tratados de manera lícita, leal y **transparente**.	Los datos personales deben ser tratados de manera lícita y leal.
Limitación de fines	Los datos personales recogidos para un fin no deberán ser objeto de tratamiento adicional para un fin incompatible; **el tratamiento con fines científicos, históricos o estadísticos no será incompatible con los fines iniciales**.	Los datos personales recogidos para un fin no deberán ser objeto de tratamiento adicional para un fin incompatible; otros fines no serán incompatibles con el fin inicial si dicho tratamiento está autorizado por la ley y es necesario y proporcionado.
Minimización de los datos	Los datos personales recogidos serán adecuados, pertinentes y **limitados a lo que sea necesario** en relación con los fines para los que fueron recogidos.	Los datos personales recogidos serán adecuados, pertinentes y **no excesivos** en relación con los fines para los que sean tratados.
Limitación del plazo de conservación	Los datos personales deberán conservarse en un formato que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que se hayan recogido dichos datos; **los datos personales podrán conservarse durante períodos más largos con fines científicos, históricos o estadísticos.**	Los datos personales deberán conservarse en un formato que permita identificar al interesado durante un período no superior al necesario para los fines para los que se hayan recogido dichos datos.
Exactitud	Los datos personales recogidos deberán ser exactos y actualizados. Los datos personales incorrectos o inexactos deberán ser suprimidos o rectificados.	
Integridad y confidencialidad	Los datos personales deberán mantenerse protegidos contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.	

Fuente: FRA, 2018.

Ejemplos

Un guardia de fronteras envía la lista de pasajeros de un avión a personas no autorizadas. Una vez compartidos, estos datos personales pueden utilizarse para fines distintos o particulares. Esta es una clara violación de los principios de protección de datos.

Un policía sale de la oficina con una lista de datos personales relacionados con sospechosos de su ordenador. Dado que esta acción menoscaba el principio de seguridad de los datos personales, constituye una violación de los principios de protección de datos.

Jurisprudencia

Las sentencias de los órganos jurisdiccionales indican cómo se aplican estos principios en la práctica.

Limitación de fines

En *Heinz Huber contra Bundesrepublik Deutschland,* el TJUE evaluó la legitimidad del Registro Central de Extranjeros (*Auslanderzentralregister, AZR*), que contiene ciertos datos personales relativos a nacionales extranjeros —tanto ciudadanos de la UE como de países terceros— que han residido en Alemania durante más de tres meses. El TJUE concluyó que los datos recogidos para un fin concreto no pueden utilizarse para un fin distinto. El Tribunal determinó que el AZR es un instrumento legítimo para aplicar las normas de residencia, y que la diferencia de trato entre los nacionales extranjeros y los alemanes, de quienes se conservan menos datos, está justificada para el fin pretendido. Sin embargo, el TJUE resolvió que los datos conservados en el AZR no podían utilizarse para combatir la delincuencia en general, ya que este no es el fin para el que se recogieron los datos en un principio.

Para más información, véase TJUE, asunto C-524/06, Heinz Huber contra Bundesrepublik Deutschland*, 16 de diciembre de 2008.*

Limitación del plazo de conservación

En *S. y Marper contra Reino Unido,* los demandantes solicitaron la supresión de sus expedientes (huellas dactilares, muestras celulares y perfiles de ADN) de la base de datos de ADN utilizada para la identificación de delincuentes en el Reino Unido. Sus juicios habían terminado con su absolución y estaban preocupados por el uso que pudiera hacerse de sus datos en el presente y en el futuro. La policía se negó. El TEDH concluyó que la conservación por tiempo indefinido de las muestras de ADN de personas que habían sido detenidas, pero posteriormente fueron absueltas o se retiraron los cargos presentados, es una violación del derecho a la intimidad. El Tribunal resaltó el riesgo de estigmatización, ya que los datos de personas que no habían sido condenadas por ningún delito eran tratados del mismo modo que los datos de las personas condenadas. El Tribunal también reconoció que el daño que puede causar la retención de estos datos es especialmente importante en el caso de los menores, dada la importancia de su desarrollo e integración en la sociedad.

Para más información, véase TEDH, S. y Marper contra Reino Unido*, n.os 30562/04 y 30566/04, 4 de diciembre de 2008.*

Para recoger y tratar datos personales con el fin de elaborar perfiles, las autoridades policiales y de gestión de fronteras deben cumplir cuatro criterios legales esenciales. La recogida y el tratamiento de los datos deben:

- **estar definidos y regulados por ley (*base jurídica*)**: cualquier limitación de los derechos de respeto a la vida privada y a la protección de los datos debe estar estipulada por ley y respetar dichos derechos en lo esencial. La ley debe cumplir los criterios de claridad y calidad, es decir, que sea accesible al público y suficientemente clara y precisa para que el público entienda su aplicación y consecuencias;

- **tener un fin válido, lícito y apropiado (*fin legítimo*):** los fines legítimos están establecidos en la ley y no se pueden ampliar. Pueden tener que ver con la seguridad nacional, la salud, el orden público o la prevención de la delincuencia;

- **ser indispensables para alcanzar dicho fin (*necesidad*):** el tratamiento de los datos personales debe limitarse a lo que sea necesario para alcanzar los fines para los que se hayan recogido;

- **no ser excesivos (*proporcionalidad*):** las autoridades responsables del tratamiento de datos personales deben alcanzar un equilibrio entre el fin y los medios empleados para conseguirlo. En otras palabras, el valor añadido del tratamiento no debe sobrepasar su impacto negativo potencial.

En el capítulo 3 se explica cómo se aplican estos principios en la práctica.

En la figura 2 se muestra cómo pueden utilizarse estos principios para determinar si una acción puede violar los derechos de respeto a la vida privada y familiar y a la protección de datos (véase también el apartado 2.3.3 sobre los mecanismos de reclamación). El caso de identificación y registro de *Gillan y Quinton contra Reino Unido* ilustra cómo aplicó el TEDH estos principios para determinar si había existido violación del derecho a la protección de datos y la intimidad (véase el recuadro Jurisprudencia).

Figura 2: Violación de la intimidad y la protección de datos: proceso de evaluación

Fuente: *FRA, 2018 [basado en Consejo de Europa (2003),* The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights].

Jurisprudencia

En *Gillan y Quinton contra Reino Unido*, los demandantes, dos nacionales británicos, trataron de impugnar la legalidad de las facultades de identificación y registro que habían sido utilizadas contra ellos por vía de una revisión judicial.

¿Está la medida adoptada estipulada por la ley? La medida era conforme a las secciones 44 a 47 de la Ley de Terrorismo de 2000, que establecía que: 1) con el fin de prevenir actos de terrorismo, cualquier policía podía ser autorizado por oficiales de alto rango a realizar actuaciones de identificación y registro; 2) dicha autorización estaba sujeta a confirmación por el Secretario de Estado y tenía una limitación temporal, pero se podía prorrogar indefinidamente; 3) aunque la finalidad de los registros era encontrar objetos que pudieran utilizarse para cometer actos terroristas, no era necesario que las actuaciones de identificación y registro se basaran en sospechas de que la persona o personas identificadas portaran objetos de esa índole; y 4) las personas que se negasen a someterse al registro podían ser privadas de libertad, multadas o ambas cosas (*Gillan y Quinton*, párr. 76-80).

¿Constituye la medida adoptada una injerencia en la intimidad o la protección de datos? El uso de poderes coercitivos por las autoridades policiales para identificar a una persona y registrar su vestimenta y sus pertenencias representa una clara injerencia en el derecho al respeto de la vida privada. Su gravedad es amplificada por la exposición pública de información personal, que conlleva un elemento de humillación y vergüenza (*Gillan y Quinton*, párr. 63).

Evaluación de proporcionalidad y necesidad: El Tribunal expresó una serie de dudas sobre la proporcionalidad y necesidad de la ley (*Gillan y Quinton*, párr. 80-86):

- el criterio legal para la autorización de las identificaciones no era exigente;
- la amplitud de las facultades legales es tal que los demandantes se enfrentan a enormes obstáculos a la hora de demostrar que una autorización y confirmación pueda exceder las facultades de las autoridades competentes (*ultra vires*) o suponga un abuso de poder;

- el alcance geográfico de la autorización era muy amplio y el límite de tiempo se ampliaba continuamente, por lo que se reducía el carácter específico de la autorización;
- las limitaciones de la discrecionalidad de los agentes eran más de forma que de fondo;
- había pocas perspectivas de recurso judicial porque el agente que realizaba la identificación no tenía obligación de demostrar que sus sospechas eran razonables; por tanto, era prácticamente imposible demostrar que había ejercido sus facultades de manera indebida.

Estas consideraciones llevaron al TEDH a concluir que los artículos pertinentes de la Ley de Terrorismo «no limitan suficientemente ni se encuentran sujetos a una protección legal adecuada contra los abusos» y, por tanto, violaban el artículo 8 del CEDH.

Para más información, véase TEDH, Gillan y Quinton contra Reino Unido*, n.º 4158/05, 12 de enero de 2010.*

Los requisitos relativos a la elaboración de perfiles que se establecen en el marco jurídico reformado sobre protección de datos de la UE se detallan en el capítulo 3.

1.3. ¿Qué efectos negativos puede tener la elaboración ilícita de perfiles para la acción policial y la gestión de fronteras?

La elaboración de perfiles basada únicamente en categorías genéricas, como la raza, el origen étnico o la religión, no solo es ilícita, sino que puede tener desventajas para que las autoridades policiales y de gestión de fronteras desarrollen su labor con eficacia. En esta sección se analizan dos posibles efectos negativos:

- La mayor dificultad radica en que se pueden tensar las relaciones con las comunidades. La elaboración de perfiles puede provocar resentimiento entre las comunidades especialmente afectadas y reducir la confianza en las autoridades policiales y de gestión de fronteras. Esto a su vez puede menoscabar la eficacia de los métodos que dependen de la cooperación ciudadana.

- También existen dudas sobre la eficacia del uso de categorías genéricas de perfiles en la gestión de fronteras o en la acción policial, por ejemplo si el resultado es que se sospecha falsamente de una persona ([17]).

Además, si se elaboran perfiles de manera ilícita, es posible que se presenten reclamaciones o denuncias contra las autoridades, ya sea en forma de supervisión interna a través de las autoridades de reclamaciones contra la policía, órganos de reclamaciones especializados o autoridades supervisoras, o a través de los sistemas judiciales civil y penal (véase la sección 2.3). Determinados agentes y mandos intermedios pueden verse sujetos a sanciones administrativas o penales debido a su participación o consentimiento en actividades de elaboración ilícita de perfiles. Esto puede traducirse en pérdida de recursos y perjudicar la moral y la reputación de las autoridades.

Puntos clave

- **La elaboración ilícita de perfiles debilita la confianza** en las autoridades policiales y de gestión de fronteras, y puede deteriorar las relaciones con las comunidades locales.
- Existen **dudas sobre la eficacia objetiva del uso de perfiles genéricos** en la detección de delitos o en la gestión de fronteras. No hay pruebas concluyentes de que este tipo de perfiles incrementen el éxito de las operaciones policiales o de gestión de fronteras.

1.3.1. Efecto sobre la confianza en la policía y la gestión de fronteras y unas buenas relaciones con la comunidad

Existen estudios que demuestran los efectos negativos que puede tener el uso de perfiles genéricos sobre las personas afectadas y las comunidades a las que pertenecen ([18]). El recuadro siguiente recoge las reacciones de algunas personas tras ser sometidas a identificación y registro o pasar una inspección fronteriza.

([17]) FRA (2017d), p. 51.

([18]) FRA (2017d).

Ejemplos

Efectos de las acciones de identificación y registro y de las inspecciones fronterizas sobre algunas personas

1. Identificaciones policiales – Keskinen, S. et al. (2018)

Entre 2015 y 2017, la Escuela Sueca de Ciencias Sociales de la Universidad de Helsinki entrevistó a 185 personas acerca de sus experiencias al ser objeto de perfiles étnicos. La mayoría de los encuestados relataban experiencias desagradables, irritantes o humillantes. A continuación se ofrecen extractos de algunos testimonios.

«Un poco más tarde, otro agente me paró de nuevo [...] mientras caminaba por la calle con dos amigas blancas: una finlandesa y otra holandesa. E hizo exactamente lo mismo... me hizo la misma pregunta. Yo estaba enfadada porque no sabía por qué me estaba señalando. Le pregunté y se limitó a decir que estaba haciendo su trabajo». (Mujer, treinta y tantos, origen africano)

«Una vez mi madre y mi hermano salieron a caminar por la ciudad y la policía les paró y les pidió los pasaportes. Yo creo que eso es aplicar un perfil étnico. Y después mi hermano [dijo en finés]: "No tenemos el pasaporte, no lo llevamos encima siempre". Y cuando vieron que hablaba finés con fluidez, su actitud fue de "ah, no importa". Me enfadé porque yo sé que el uso de perfiles étnicos es ilegal, pero mi madre y mi hermano no lo sabían. Así que sentí, ya sabes, que habían sido maltratados. Y me enfadé mucho. Una vez les dije que lo que les había pasado era ilegal y obviamente sabían que les habían parado porque [...] no parecían finlandeses, sino que parecían extranjeros». (Mujer, veintitantos, somalí-finlandesa)

«Siempre tienen una descripción parecida. Y yo me pregunto si es que llevan once años buscando a la misma persona que siempre se les escapa, tíos, entonces no estáis haciendo un buen trabajo, porque la descripción que tienen [en el control de fronteras] es siempre parecida y yo siempre encajo en esa descripción [risas]». (Hombre, treinta y pocos, finlandés de origen africano)

Para más información, véase Keskinen, S. et al. (2018), The Stopped – Ethnic Profiling in Finland.

2. Inspecciones fronterizas – FRA (2014a y 2014b)

«Entiendo por qué [el guardia de fronteras] me paró, pero no tenía por qué enviarme aquí [inspección de segunda línea/comisaría de policía] ni tratarme como un delincuente. Lo hacen con todos los europeos del este». (Pasajero serbio, entrevistado en el aeropuerto de Frankfurt)

Pregunta: «¿Cómo califica el trato recibido en la inspección de primera línea?»

Respuesta: «Creo que no fue bueno. Fue humillante. Me trataron mal. Simplemente cogió mi pasaporte, le echó un vistazo y llamó a inmigración. Me hizo algunas preguntas levantándome la voz, pero no entendí nada. Me sacaron de la cola, pero no me respetaron y me asustaron».

P: «¿Por qué se sintió asustado o humillado?»

R: «Porque no sabía qué me iba a pasar y no me explicaban nada. Y había mucha gente y el guardia hablaba con los otros guardias pero no conmigo. Tuve que esperar sin saber por qué estaba allí». (Pasajero de Angola, entrevistado en Schiphol)

«De verdad, entiendo a los guardias fronterizos. Para ellos también es difícil trabajar en esas cabinas durante horas. Así que a veces tienen actitudes negativas —por ejemplo, gritar— con gente como nosotros». (Nacional turco, conductor de camiones que cruza con frecuencia la frontera de Kipi)

La suma de estas experiencias individuales puede traducirse en efectos negativos sobre el grupo ([19]). Esto puede contribuir a un marcado deterioro de las relaciones entre los agentes de policía y de gestión de fronteras y los miembros de las comunidades minoritarias sometidas con frecuencia a actuaciones de identificación y registro o inspecciones fronterizas exhaustivas.

([19]) Naciones Unidas (2007), apdo. 57.

Caso práctico

Identificación y registro en desórdenes públicos (Reino Unido, 2011 y Francia, 2005).

Después de los disturbios ocurridos en varias grandes ciudades británicas en agosto de 2011, la London School of Economics y el periódico *The Guardian* entrevistaron a 270 alborotadores para preguntarles por qué habían participado en los disturbios. El estudio reveló que un factor importante fue la desconfianza y antipatía hacia la policía y que «[l]as reclamaciones más frecuentes tenían que ver con la experiencia cotidiana de la labor policial, ya que mucha gente expresaba una gran frustración por el trato que recibían los miembros de sus comunidades cuando eran identificados y registrados».

Para más información, véase London School of Economics (2011).

En otros Estados miembros de la Unión se observaron dinámicas similares. En Francia, los disturbios de noviembre de 2005 fueron causados por el fallecimiento accidental de dos jóvenes de una minoría mientras eran presuntamente perseguidos por la policía (véase Jobard, 2008, y Body-Gendrot, 2016).

Para más información, véase Hörnqvist (2016).

En relación con esto, el uso de perfiles puede incrementar los niveles de hostilidad existentes en otros encuentros entre algunas personas y la policía u otros cuerpos y fuerzas de seguridad. Esta mayor hostilidad aumenta las probabilidades de que un encuentro rutinario pueda derivar en agresión y conflicto y entrañe riesgos para la seguridad de los agentes y de los miembros de la comunidad por igual.

Con carácter más general, un estudio reciente demuestra que las identificaciones, detenciones, condenas o encarcelamientos tienden a alejar a la gente de otros servicios públicos aparte del sistema de justicia penal, como la sanidad, el empleo y la educación ([20]). Sin menoscabo de las razones legítimas que llevan a la detención de personas condenadas, hay que tener en cuenta que excluir de tales instituciones a segmentos ya marginalizados de la población puede perjudicar la inclusión e integración social de los grupos minoritarios.

([20]) Brayne, S. (2014), pp. 367–391.

Análisis de las conclusiones de la encuesta EU-MIDIS II de la FRA

En 2015 y 2016, la FRA recopiló información de más de 25 500 encuestados de diversas minorías étnicas y origen inmigrante en los 28 Estados miembros de la Unión Europea.

¿Qué información se recopiló?

En relación con el uso de perfiles, se preguntó a los encuestados si pensaban que habían sido identificados por la policía por su condición de inmigrantes o por su pertenencia a una minoría étnica, y por el trato que les dispensó la policía, incluida cualquier posible experiencia de agresión física por parte de los agentes. La encuesta no contenía preguntas acerca de encuentros con personal de gestión de fronteras.

¿Qué indican los resultados?

Identificaciones y origen étnico: Los resultados indican que el 26 % de los encuestados en EU-MIDIS II fueron identificados por la policía durante los 5 años anteriores a la encuesta. De este último grupo, el 33 % declaró que fue debido a su ascendencia étnica e inmigrante.

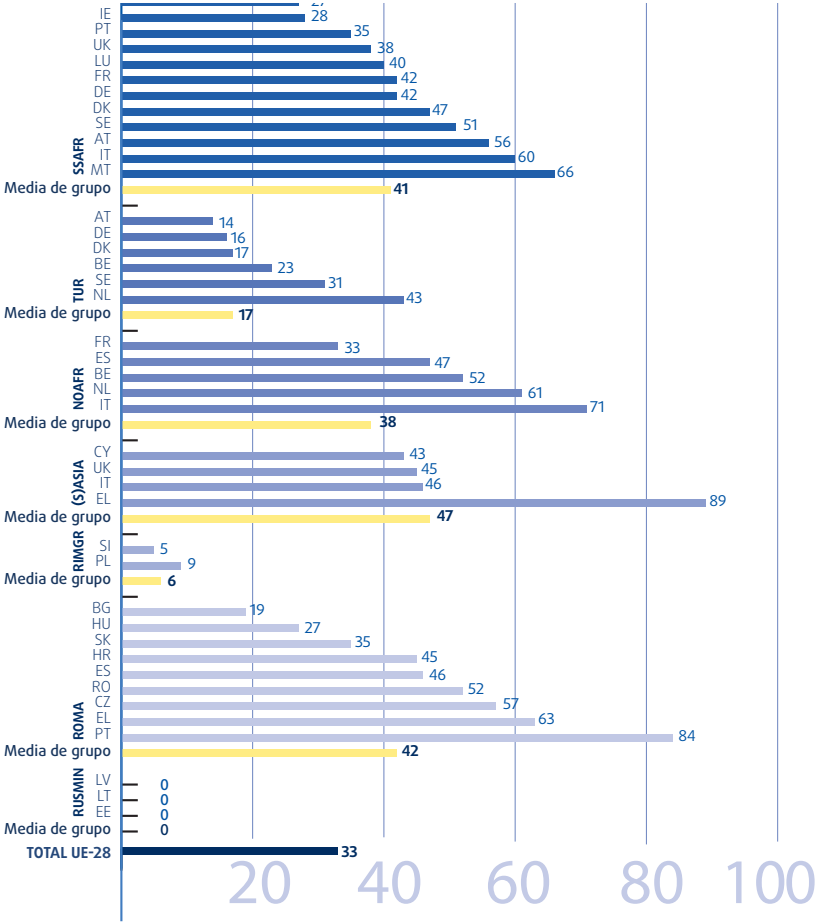
Percepción de la discriminación: Por término medio, casi uno de cada dos encuestados de ascendencia asiática (47 %), subsahariana (41 %) y norteafricana (38 %) que fue identificado en este período afirmó haber sido detenido debido a su condición de inmigrante o pertenencia a una minoría étnica. Del mismo modo, entre los encuestados romaníes identificados, casi 1 de cada 2 personas (42 %) creían que se debía a su origen étnico. Por el contrario, este porcentaje es mucho menor entre los encuestados identificados de origen turco (17 %) (véase la figura 3).

Respeto: Los resultados indican que la mayoría de los encuestados que fueron identificados por la policía en los cinco años anteriores a la encuesta (59 %) consideraban haber sido tratados de forma respetuosa (el 25 % «muy respetuosa» y el 34 % «bastante respetuosa»). 1 de cada 4 encuestados (24 %) afirmó que la manera en que la policía los había tratado no había sido «ni respetuosa ni irrespetuosa». Por otra parte, el 17 % indicó que la policía los trató de manera irrespetuosa (el 8 % «bastante irrespetuosa» y el 9 % «muy irrespetuosa»). Los encuestados romaníes y los encuestados de origen norteafricano que fueron

identificados afirmaron haber experimentado un comportamiento irrespetuoso por parte de la policía durante las identificaciones más recientes (25 % y 21 %, respectivamente) con más frecuencia que otros grupos objetivo.

Para más información, véase FRA (2017b).

Figura 3: Identificaciones policiales más recientes percibidas como aplicación de perfiles étnicos entre las personas identificadas en los cinco años anteriores a la encuesta EU-MIDIS II, por Estado miembro y grupo objetivo (%) [a, b, c, d]



Notas: [a] *De todos los encuestados identificados por la policía en los 5 años anteriores a la encuesta (n = 6 787); resultados ponderados.*

[b] *Los resultados basados en un número reducido de respuestas son menos fiables estadísticamente. Por consiguiente, los resultados basados en entre 20 y 49 observaciones no ponderadas en un total de grupo o basados en celdas con menos de 20 observaciones no ponderadas figuran entre paréntesis. Los resultados basados en menos de 20 observaciones no ponderadas en un total de grupo no se publican.*

[c] *Preguntas: «En los cinco últimos años en [PAÍS] (o desde que está en [PAÍS]), ¿alguna vez ha sido identificado, registrado o interrogado por la policía?»; «¿Cree que LA ÚLTIMA VEZ que fue identificado fue debido a su origen étnico o inmigrante?».*

[d] *Los acrónimos de los grupos objetivo se refieren a los inmigrante de [país/región] y sus descendientes: TUR = Turquía, SSAFR = África Subsahariana, NOAFR = Norte de África, SASIA = Asia Meridional, ASIA = Asia, ROMA = minoría romaní.*

Fuente: FRA, 2017b.

Análisis de la importancia y utilidad de los datos recogidos en las identificaciones policiales

De los 28 Estados miembros de la Unión, el Reino Unido es actualmente el único en el que los datos recogidos en las identificaciones policiales incluyen sistemáticamente información sobre la etnia de la persona identificada (véanse también los apartados 2.2.5 y 2.3.1).

Los datos recogidos miden la «tasa de identificación y registro» de diferentes grupos étnicos en Inglaterra y Gales. Las categorías étnicas utilizadas son las recogidas en el Censo del Reino Unido de 2001. Este censo identificaba 16 categorías, que formaban 5 grandes grupos:

- Blancos: ingleses/galeses/escoceses/norirlandeses/británicos; irlandeses; y cualquier otra ascendencia blanca.
- Grupos étnicos mixtos/múltiples: blancos y negros caribeños; blancos y negros africanos; blancos y asiáticos; y cualquier otro origen étnico mixto/múltiple.
- Asiáticos/asiático-británicos: indios; paquistaníes; bangladesíes; y cualquier otra ascendencia asiática.
- Negros/africanos/caribeños/negros británicos: africanos; caribeños; y cualquier otra ascendencia negra/africana/caribeña.
- Otros grupos étnicos: chinos; y otros grupos étnicos.

Con los datos obtenidos en actuaciones de identificación y registro se compara el número de personas identificadas y registradas de un determinado grupo étnico con el número total de personas de ese grupo étnico residentes en la zona, y se calcula una tasa por cada 1 000 personas.

En 2016-2017, el análisis de los datos recogidos revela 4 identificaciones por cada 1 000 personas blancas, frente a 29 por cada 1 000 personas negras. Las tasas más elevadas se observan entre los tres grupos étnicos negros: otros negros (70 identificaciones por cada 1 000 personas), negros caribeños (28 por cada 1 000) y negros africanos (19 por cada 1 000).

A falta de datos desagregados, es difícil demostrar si la policía actúa de forma diferente con respecto a determinados grupos étnicos y —en tal caso— si ello podría deberse al uso de perfiles discriminatorios. Existen datos desagregados de dominio público en Inglaterra y Gales, desglosados por cuerpo policial. Esto permite determinar si existen prácticas diferenciadas entre cuerpos que puedan considerarse legítimas o que puedan utilizarse para detectar posibles discriminaciones en las prácticas policiales. También se utilizan datos relativos a policías concretos para detectar prácticas discriminatorias en su trabajo.

Para más información, véase la página del sitio web gov.uk sobre identificación y registro, el sitio web de la Independent Office for Police Conduct http://www.policeconduct.gov.uk/ y el sitio web de la Home Office sobre datos públicos acerca de la labor policial y la delincuencia. Véase también FRA (2018). Para obtener orientaciones sobre metodologías de documentación, véase Open Society Justice Initiative (2018b).

Caso práctico

Encuesta sobre las relaciones entre la policía y la ciudadanía en Francia

En 2016, el Defensor del Pueblo francés (*Défenseur des droits)* realizó una encuesta sobre acceso a derechos. El *Défenseur des droits* también actúa como comisión nacional de reclamaciones contra la policía. El estudio comprende una muestra representativa de más de 5 000 personas.

La primera parte del informe presenta los resultados relacionados con el comportamiento de las autoridades policiales. En general, la encuesta indica

que las relaciones entre la ciudadanía y la policía son buenas. La inmensa mayoría de los encuestados afirman confiar en la policía (82 %).

En lo que respecta concretamente a las verificaciones de identidad, la encuesta revela que la mayoría de la gente no es sometida a estas verificaciones: el 84 % de los encuestados manifiesta no haber sido identificado en los 5 últimos años (el 90 % de las mujeres y el 77 % de los hombres). Quienes dicen haber sido identificados declaran en general pocos casos de comportamiento que viole la ética profesional de las fuerzas de seguridad durante la verificación de identidad más reciente, como trato informal (16 %), brutalidad (8 %) o insultos (7 %). Sin embargo, el 29 % habla de falta de cortesía, y más de la mitad de los encuestados (59 %) que habían sido identificados señalan que no les explicaron las razones de la verificación. En general, se percibe que las verificaciones de identidad tienen más legitimidad cuando las fuerzas de seguridad se toman la molestia de explicar las razones de las mismas.

Los datos también revelan que determinados grupos de personas relatan experiencias más negativas. Los hombres jóvenes de 18 a 24 años tienen casi 7 veces más probabilidades de ser sometidos a verificaciones de identidad frecuentes (es decir, más de 5 veces en los 5 últimos años) que la población en general, y los hombres percibidos como negros o árabes se ven entre 6 y 11 veces más afectados por verificaciones de identidad frecuentes que el resto de la población masculina. Si se combinan estos dos criterios, el 80 % de los hombres menores de 25 años percibidos como árabes o negros han sido identificados al menos una vez en los 5 últimos años (frente al 16 % del resto de encuestados). En comparación con la población en general, este grupo tiene 20 veces más probabilidades de ser sometido a verificaciones de identidad.

Además, los hombres jóvenes percibidos como negros o árabes declaran mayores niveles de comportamiento problemático durante la verificación de identidad más reciente, como el trato informal (el 40 % frente al 16 % de la muestra total), insultos (el 21 % frente al 7 %) o brutalidad (el 20 % frente al 8 %). Estas experiencias negativas y la frecuencia de las verificaciones se asocian a un bajo nivel de confianza en la policía. De hecho, este grupo habla de deterioro de las relaciones con la policía.

Por último, los resultados revelan que pocos de los encuestados (5 %) que indican que se incumplió la ética profesional durante las verificaciones de identidad hacen algo para denunciar esta situación. En general indican que no denuncian sus experiencias porque consideran que no sirve para nada.

Para más información, véase Défenseur des droits (2017).

La aplicación de perfiles genéricos a un grupo minoritario, junto con otras actuaciones estigmatizantes, puede hacer que este grupo adquiera una percepción negativa de sí mismo. Además, el conjunto de la comunidad puede adquirir una percepción negativa de ese grupo. El grupo minoritario se convierte en una «comunidad sospechosa», asociada por los ciudadanos a la delincuencia ([21]). Esto puede crear mayores prejuicios.

El grupo minoritario puede ser el objetivo de una cantidad desproporcionada de recursos policiales, lo cual puede a su vez dar lugar a un mayor número de detenciones o inspecciones en frontera. Esto puede hacer que la propia intensidad de la actuación policial provoque que las sospechas se hagan reales y aumenten las tasas de detención (véase el recuadro) ([22]).

Análisis del riesgo de «profecía autocumplida»

Cuando los policías no basen sus perfiles en motivos razonables sino en prejuicios, es probable que interpreten la información de manera que confirme sus propios sesgos. Esto se llama «sesgo de confirmación». Es lo que ocurre cuando los prejuicios de los policías les generan la expectativa de que una persona actuará ilícitamente basándose en la raza, el origen étnico, el género, la orientación sexual, la religión u otro motivo protegido, real o percibido, de dicha persona. Debido a este tipo de sesgo, es probable que los agentes que tengan tales prejuicios señalen a mayor número de personas que encajen con esta descripción.

Dado que es más probable que se encuentren pruebas de criminalidad en personas sometidas a controles de identificación que en otras personas, esta elaboración de perfiles sesgada vendrá a reforzar los estereotipos que ya

([21]) Observatorio Europeo del Racismo y la Xenofobia (2006), p. 54.

([22]) Harcourt, B. (2004), pp. 1329-1330; House of Commons Home Affairs Committee (2009), apdo. 16; y Naciones Unidas (2007).

pueda tener un agente. Esta falsa «prueba» de que la decisión de identificar a estas personas era correcta se denomina «profecía autocumplida». Esta clase de elaboración de perfiles sesgada es discriminatoria, ilícita, ineficaz y perpetúa los estereotipos.

La figura 4 describe cómo la «profecía autocumplida» perpetúa la criminalización de las personas.

Figura 4: El ciclo de la profecía autocumplida

Fuente: FRA, 2018.

1.3.2. Eficacia del uso de perfiles

También existen dudas acerca de la eficacia del uso de perfiles basados en categorías genéricas para detectar delitos. No está claro si el uso de perfiles incrementa efectivamente la tasa de éxito (o «tasa de acierto») de las operaciones policiales.

Algunas pruebas indican que los porcentajes de identificación de algunas personas no se corresponden necesariamente con los porcentajes de delito entre diferentes grupos étnicos o raciales (véase el recuadro). Conviene señalar que los datos de la justicia penal de la mayoría de Estados miembros no permiten observar la evolución

de un caso individual en el sistema de justicia penal. En este sentido, no es posible determinar si una detención da lugar a enjuiciamiento y sentencia.

Caso práctico

La modificación de los patrones de registro aumenta la «tasa de acierto» (1998-2000, Estados Unidos)

En 1998, el 43 % de los registros realizados por las Aduanas de Estados Unidos afectaron a personas negras y latinas, un porcentaje muy superior a la proporción que representan estas personas entre los viajeros. Se realizó un número especialmente importante de registros en mujeres latinas y negras sospechosas de ser «mulas de drogas», que incluyeron la obligación de someterse a rayos X invasivos o quitarse la ropa. Esto se hizo aplicando un perfil que se basaba en gran medida en la nacionalidad y la etnia. Las tasas de acierto de estos registros fueron bajas en todos los grupos: el 5,8 % en «blancos», el 5,9 % en «negros» y el 1,4 % en «latinos». Fueron especialmente bajas en el caso de las mujeres «latinas», que eran de hecho las que menos probabilidad tenían de llevar drogas encima o en sus cavidades corporales. En 1999, las Aduanas de Estados Unidos modificaron sus procedimientos y eliminaron la raza de entre los factores considerados para realizar identificaciones. En su lugar, se utilizaron técnicas de observación del comportamiento —como nerviosismo o incongruencias en las explicaciones de los pasajeros—, más información de inteligencia, y una supervisión más estrecha de las decisiones de identificación y registro. En 2000, las desigualdades raciales en los registros realizados en aduanas casi habían desaparecido. El número de registros realizados descendió un 75 % y la tasa de acierto pasó de tan solo un 5 % a más del 13 %, y prácticamente se igualó para todos los grupos étnicos.

Para más información, véase Harris (2002) y Estados Unidos (2000).

Ineficacia de la elaboración ilícita de perfiles (2007-2008, Hungría)

Un estudio realizado en Hungría reveló que las personas romaníes eran sometidas de manera desproporcionada a verificaciones de identidad. El 22 % de las personas identificadas por la policía pertenecían a la comunidad romaní, mientras que la proporción de las personas romaníes en el conjunto

de la población era del 6 %. El número desproporcionadamente elevado de verificaciones de identidad realizadas a personas romaníes no se traducía en pruebas de comportamiento ilícito: el 78 % de las verificaciones de identidad realizadas a personas romaníes no tuvieron un resultado policial, mientras que el 19 % estaban relacionadas con faltas (*) (en comparación con el 18 % de los controles realizados a la población en general). Además, los porcentajes de detención eran parecidos en la comunidad romaní y en el conjunto de la población.

Para más información, véase Tóth, B. M. y Kádár, A. (2011).

(*) «Las faltas son infracciones cuasi penales, cuya gravedad no alcanza el nivel penal (es decir, no están recogidas en el Código Penal). Las faltas pueden ser desde infracciones sancionables con hasta 60 días de encarcelamiento, como la prostitución o las amenazas físicas, hasta infracciones sancionables con medidas menos severas (p. ej. una multa, confiscación de bienes o prohibición de acceso a determinados eventos). Algunos ejemplos de este tipo de faltas son pequeños hurtos o infracciones de tráfico». *Véase Kádár, A., Körner, J., Moldova, Z. y Tóth, B. (2008), p. 23.*

También existen dudas acerca de las razones por las que se identifica a determinadas personas. En un estudio del Reino Unido se indica que «[u]n alarmante 27 % (2 338) de los expedientes de identificación y registro examinados [...] no contenían motivos razonables para efectuar el registro, aunque muchos de estos expedientes habían sido aprobados por los supervisores». ([23]) Según dicho estudio, esto indica que «puede que las fuerzas policiales no estén cumpliendo debidamente los requisitos del deber de igualdad en el sector público, que les obliga a tomar en la debida consideración la necesidad de eliminar la discriminación ilícita y promover la igualdad de oportunidades, fomentar las buenas relaciones y, con ese fin, velar por que se recojan, analicen y publiquen adecuadamente datos que demuestren que disponen de suficiente información para comprender los efectos de su trabajo».

([23]) Reino Unido, Her Majesty's Inspectorate of Constabulary (HMIC) (2013), p. 6.

2 Elaboración lícita de perfiles: principio y práctica

Este capítulo se centra en el uso de perfiles por la policía de primera línea, especialmente en las actuaciones de identificación y registro, así como por los agentes encargados de la gestión de fronteras, en particular en las inspecciones fronterizas de segunda línea. El capítulo explica los principios y prácticas fundamentales que contribuyen a reducir el riesgo de elaboración ilícita de perfiles. Estas medidas se pueden adoptar tanto en los niveles de dirección como de operación. Toma en cuenta los diferentes contextos jurídicos y prácticos de las actuaciones de identificación y registro y de las inspecciones fronterizas.

En el contexto de la gestión de fronteras, el Código de Fronteras Schengen [Reglamento (UE) n.º 2016/399 ([24])] establece normas unificadas que regulan los controles en las fronteras exteriores de la UE. Esto significa que varios de los principios descritos en este capítulo —por ejemplo, en relación con la información que debe facilitarse a los nacionales de terceros países sometidos a una inspección de segunda línea— están estipulados por ley y son vinculantes en los Estados miembros. Además, Frontex tiene la importante misión de promover el mantenimiento de un elevado nivel de exigencia en los controles fronterizos. En particular, el Reglamento de 2016 sobre la Guardia Europea de Fronteras y Costas obliga a los Estados miembros a seguir los planes de estudios comunes elaborados por Frontex en la formación de los guardias de fronteras. Publicado en 2012, el plan de estudios común incorpora una sección consagrada a los derechos fundamentales que también incluye la elaboración de perfiles (véase el apartado 2.2.3 sobre formación específica).

([24]) Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen), DO L 77 de 23.3.2016.

Análisis de los motivos para realizar una inspección de segunda línea en la frontera

Dado el carácter sistemático de los controles fronterizos, todos los viajeros pasan por una inspección básica de primera línea en la que se verifican los documentos de viaje y cualquier otro requisito de entrada. Además, algunos viajeros pueden estar sometidos a una inspección de segunda línea. Esto puede deberse a diversos motivos: una correspondencia con la información contenida en una base de datos, el hecho de portar consigo documentos de viaje sospechosos, que encajen con un perfil de riesgo o que se comporten de manera sospechosa.

Durante la inspección de primera línea, el guardia de fronteras puede servirse de la información obtenida comparando los datos contenidos en el documento de viaje de lectura mecánica (que incluye identificadores biométricos) con los datos almacenados en bases de datos nacionales, europeas e internacionales como el Sistema de Información de Schengen, el Sistema de Información de Visados y las bases de datos de Europol e Interpol. En la práctica, una remisión a una inspección de segunda línea con frecuencia ocurre como resultado de una coincidencia en una de las bases de datos.

Sin embargo, se puede someter a una persona a una inspección de segunda línea por otras razones, por ejemplo, cuando encaja en un perfil de riesgo o si el agente alberga otros motivos para sospechar de ella. El Catálogo Schengen de la UE establece que la finalidad de las inspecciones fronterizas de primera línea, que deben realizarse de conformidad con el Código de Fronteras Schengen, debe consistir en caracterizar a los viajeros y detectar a las personas sospechosas para que sean objeto de una minuciosa inspección de segunda línea (*). Por lo tanto, los guardias de fronteras deben evaluar un conjunto de indicadores y criterios diferentes para determinar si una persona puede estar intentando entrar de manera irregular, puede plantear un riesgo para la seguridad o, por ejemplo, puede ser víctima de trata. Tanto si aplican un perfil de riesgo específico ya existente como si no, los guardias de fronteras utilizan perfiles en estas situaciones.

Debido a la necesidad de garantizar que los viajeros circulen con fluidez, los guardias de fronteras disponen de un tiempo limitado para efectuar una evaluación objetiva que permita determinar si una persona debe someterse a una inspección de segunda línea. La información de Frontex revela que los agentes de los Estados miembros disponen, por término medio, de apenas

doce segundos para decidir si deben señalar a una persona para someterla a inspección adicional (**). Por lo tanto, se encuentran bajo una presión importante para tomar con rapidez una decisión correcta.

(*) Consejo de la Unión Europea (2009), Recomendación 43.
(**) Agencia de la Guardia Europea de Fronteras y Costas (Frontex) (2015).

Los principios y las herramientas prácticas que aparecen en este capítulo ofrecen información destinada a fomentar análisis y medidas que pueden ayudar a los agentes y a sus organizaciones a mantener sus actividades de elaboración de perfiles dentro de la ley. Los tres principios claves analizados son:

- Respetar la dignidad de las personas.
- Velar por que los perfiles se basen en motivos razonables y objetivos.
- Garantizar la rendición de cuentas.

Subyacente y ligado a cada uno de ellos debe señalarse la importancia de asegurar que los policías y los guardias de fronteras operan dentro de la ley en el momento de recurrir a los perfiles.

2.1. Respeto a la dignidad de las personas

Puntos clave

- Asegurar un **encuentro cualitativamente bueno** no basta de por sí para evitar el uso discriminatorio de los perfiles. Sin embargo, sí puede contribuir a que el encuentro discurra por mejores cauces y se reduzcan los posibles efectos negativos de las actuaciones de identificación y registro. En la gestión de fronteras, mantener una conducta profesional y respetuosa es una obligación legal.
- **Una conducta profesional y respetuosa** se traduce por lo general en un encuentro más satisfactorio para el interesado.
- **Explicar las razones de la identificación** a la persona afectada contribuye a incrementar la confianza en las operaciones policiales y de gestión de fronteras, y reduce la percepción de que se utilizan perfiles discriminatorios.
- El respeto y la cortesía **nunca justifican que se lleven a cabo inspecciones fronterizas o actuaciones policiales de identificación y registro de carácter ilícito**.

Respetar la dignidad de las personas no solo es un derecho fundamental de por sí, sino un principio fundamental de las operaciones policiales y de gestión de fronteras. En las operaciones de primera línea, la forma que tengan los agentes de policía y de gestión de fronteras de hablar y tratar con las personas a las que identifiquen, así como la información que faciliten, es crucial.

Siempre hay que recordar que, no importa la cortesía y profesionalidad que muestren los agentes, señalar a una persona es una experiencia intrusiva que debe basarse siempre en motivos lícitos. La percepción de que se utilizan perfiles discriminatorios también va ligada a la frecuencia y al número de interacciones con las autoridades policiales y de gestión de fronteras. Esto subraya la importancia de velar por que siempre existan motivos objetivos y razonables para identificar a una persona.

¿Qué dicen las normas?

«Los controles fronterizos deben realizarse de tal manera que se respete plenamente la dignidad humana. Deben efectuarse con profesionalidad y de manera respetuosa, y ser proporcionados a los objetivos perseguidos».
Considerando 7 del Código de fronteras Schengen

«Todos los viajeros tienen derecho a ser informados sobre la naturaleza del control y a un trato profesional, amistoso y cortés, de conformidad con el Derecho internacional, comunitario e interno aplicable».
Sección 1.2 del Manual práctico para guardias de fronteras (Manual Schengen)

«El personal de policía debe actuar con integridad y respeto hacia la población, teniendo especialmente en cuenta la situación de los individuos que formen parte de grupos particularmente vulnerables».
Recomendación 44 del Código Europeo de Ética de la Policía

No siempre es fácil conseguir que los policías y los guardias de fronteras sean corteses e informativos en situaciones tensas y difíciles. Sin embargo, las pruebas demuestran que mantener un tono respetuoso aumenta notablemente el grado de satisfacción con el encuentro ([25]). La figura 5 ilustra algunos elementos de un encuentro respetuoso.

([25]) FRA (2014b).

Figura 5: Tres elementos de un encuentro respetuoso

Fuente: FRA, 2018.

Ciertos elementos de las inspecciones fronterizas están regulados por el Código de Fronteras Schengen, como la obligación de realizar las inspecciones de manera profesional y respetuosa o facilitar información sobre la finalidad y el procedimiento de la inspección (Código de Fronteras Schengen, considerando 7, artículo 7 y artículo 8, apartado 5). El uso de una lengua común, por otra parte, no es un requisito absoluto en el contexto de la gestión de fronteras debido a la variabilidad intrínseca del tráfico fronterizo. No obstante, el Código de Fronteras Schengen obliga a los Estados miembros a fomentar el aprendizaje, por parte de los guardias de fronteras, de las lenguas necesarias para desempeñar sus funciones (artículo 16, apartado 1). El Catálogo Schengen, que contiene una serie de recomendaciones y buenas prácticas para el control de las fronteras exteriores, recomienda además que los guardias de fronteras tengan la capacidad de comunicarse en lenguas extranjeras relacionadas con sus obligaciones cotidianas. A modo de buena práctica, hace referencia a un conocimiento satisfactorio de las lenguas de los países vecinos, así como de otras lenguas en función de la naturaleza del tráfico en frontera. Lo ideal es que en cada turno se incluyan agentes con competencias lingüísticas adecuadas ([26]).

La falta de consideración y respeto durante las identificaciones policiales pueden afectar directamente a la eficacia de la labor policial (véase el apartado 1.3.2). El Código de Práctica de la Ley de pruebas policiales y criminales elaborado en el Reino Unido establece que: «Todas las identificaciones y registros deben llevarse a cabo con cortesía, consideración y respeto hacia la persona afectada. Esto afecta de

([26]) Consejo de la Unión Europea (2009), Recomendaciones 27 y 41.

manera importante a la confianza de los ciudadanos en la policía. Debe hacerse todo lo razonablemente posible por reducir al mínimo el sentimiento de vergüenza que pueda experimentar la persona registrada» ([27]).

Algunos componentes importantes del respeto a la dignidad, como explicar los motivos de la identificación y asegurarse de que la persona afectada tenga la oportunidad de manifestar sus opiniones, son elementos básicos de los procedimientos policiales y de gestión de fronteras. Los formularios de identificación y registro pueden contribuir a ofrecer un medio estructurado de proporcionar esta información (véase el apartado 2.3.1).

En el contexto de la gestión de fronteras, los formularios estándar son una herramienta útil para informar a los viajeros acerca de la finalidad y el procedimiento de la inspección de segunda línea. Pueden facilitar la comunicación con los viajeros, siempre que se distribuyan y se complementen con explicaciones verbales adicionales si es necesario. El Código de Fronteras Schengen exige que las personas sometidas a una inspección de segunda línea reciban información por escrito en una lengua que entiendan —o que se pueda razonablemente suponer que entienden— acerca de la finalidad y el procedimiento de la inspección. La información debe:

- estar disponible en todas las lenguas oficiales de la UE y en las lenguas de los países fronterizos con el país de que se trate; e
- indicar que el viajero puede solicitar el nombre o el número de identificación de servicio del agente que realice la inspección, el nombre del paso fronterizo y la fecha de cruce de la frontera.

Los elementos de un encuentro respetuoso asociados a la comunicación y las aptitudes interpersonales son más difíciles de establecer en los procedimientos de operación y pueden requerir una mayor inversión en formación. Las dificultades para que el agente mantenga un tono positivo durante el encuentro pueden deberse a:

- que sus aptitudes para la comunicación sean limitadas;
- que no sea capaz de articular el motivo de la actuación; y
- que no sea capaz de vencer sus prejuicios personales e institucionales y estereotipos negativos, así como las hostilidades que ya puedan haberse generado en algunos segmentos de la comunidad.

([27]) Reino Unido, Home Office (2014a), sección 3.1.

2.2. Motivos razonables y objetivos

Puntos clave

- Las actuaciones policiales y de gestión de fronteras basadas en información de inteligencia específica y actualizada tienen más probabilidades de ser objetivas.
- Para que sean lícitas, las actuaciones de identificación y registro y las inspecciones fronterizas de segunda línea, deben basarse en **motivos de sospecha razonables y objetivos**. Las «corazonadas» no son motivos razonables ni objetivos para identificar y registrar a una persona o someterla a una inspección fronteriza de segunda línea.
- Características protegidas como la raza, el origen étnico, el género o la religión pueden ser algunos de los factores que las autoridades policiales y la guardia de fronteras tengan en cuenta para ejercer sus competencias, pero **no pueden ser ni la única ni la principal razón por la que se señale a una persona concreta**.
- Los perfiles basados única o principalmente en alguno de los motivos protegidos constituyen discriminación directa y son ilícitos.

La objetividad es un principio importante de la acción policial y de la gestión de fronteras. En el contexto del uso de perfiles, una persona solo debe ser sometida a identificación y registro o a una inspección de segunda línea si existen motivos de sospecha razonables y objetivos. Justificaciones objetivas pueden ser el comportamiento de la persona, información de inteligencia especifica, o circunstancias que vinculen a una persona o personas con actividades presuntamente ilícitas.

Para garantizar la objetividad en la elaboración de perfiles es necesario:

- evitar los sesgos, por ejemplo a través de orientaciones claras y formación específica; y
- hacer un uso efectivo de la información de inteligencia y de otro tipo.

2.2.1. Evitar sesgos

El Código Europeo de Ética de la Policía ofrece orientaciones sobre conducta policial en ámbitos como la acción e intervención policial, la rendición de cuentas por parte de la policía y la supervisión de la policía ([28]). Subraya el principio general de que:

([28]) Consejo de Europa, Comité de Ministros (2001), Recomendación Rec(2001)10 del Comité de Ministros a los Estados miembros sobre el Código Europeo de Ética de la Policía, 19 de septiembre de 2001.

«[l]a policía debe llevar a cabo sus misiones de manera equitativa, inspirándose, en particular, en los principios de imparcialidad y no discriminación» ([29]).

Señalar a una persona utilizando *como factor único o determinante* su raza, origen étnico, género, orientación sexual, religión, discapacidad u otros motivos prohibidos, reales o percibidos, viola derechos fundamentales. También puede tener importantes consecuencias negativas para las autoridades públicas y para las comunidades (véase la sección 1.3).

Los perfiles discriminatorios pueden ser reflejo de sesgos individuales e institucionales. Además de sesgos personales, pueden generarse estereotipos y comportamientos discriminatorios a partir de prácticas concretas de las autoridades policiales y de gestión de fronteras. Aumentar la transparencia de los procedimientos y prácticas institucionales puede contribuir a corregir la discriminación y la perpetuación de los estereotipos.

Reconocer la existencia de sesgos muy arraigados puede ser difícil. Los agentes de policía y de gestión de fronteras pueden creer que señalan a personas basándose en motivos razonables y objetivos (como el comportamiento), cuando estas decisiones son efectivamente reflejo de sus sesgos.

En el momento de identificar a una persona, los agentes suelen justificar su decisión de señalar a esa persona en una «corazonada» o «intuición», que seguramente se base en un conjunto de conocimientos y experiencias anteriores, pero que quizá también sea reflejo de un sesgo consciente o subconsciente. Para evitar el uso ilícito de perfiles, los agentes deben reflexionar sobre si su decisión está justificada por información objetiva. Una «corazonada» no es un objetivo razonable u objetivo para identificar y registrar a una persona o someterla a una inspección adicional en frontera.

2.2.2. Orientaciones claras para los agentes

Es especialmente importante ofrecer orientaciones prácticas, comprensibles y fáciles de aplicar a los agentes de policía y de gestión de fronteras de primera línea para ayudarlos a evitar el uso ilícito de perfiles. Estas orientaciones pueden adoptar muchas formas: pueden incorporarse a la legislación, ser dictadas por las propias autoridades policiales y de gestión de fronteras o impartidas en el día a día por oficiales de alto rango. Tomar ejemplos de la vida real para demostrar qué debe hacerse en situaciones concretas puede resultar más eficaz que la explicación de normas y procedimientos.

([29]) Véase la nota anterior, apdo. 40.

Los agentes que ocupen puestos de mando deben informar al personal de que la raza, el origen étnico, el género, la orientación sexual, la religión u otros motivos prohibidos, reales o percibidos, no pueden ser los factores determinantes para adoptar medidas policiales o de gestión de fronteras contra una persona, porque serían discriminatorios. Aclarar cuándo y cómo pueden utilizarse características personales puede contribuir a reducir el riesgo de que se produzcan diferentes interpretaciones, así como la influencia de los estereotipos y los prejuicios. Las orientaciones también deben tratar cuestiones relacionadas con la intimidad y la protección de datos.

El cuadro 3 muestra algunos tipos de orientaciones que pueden utilizarse y elementos importantes que deberían tenerse en cuenta.

Cuadro 3: Tipos, características de las orientaciones y participación de las partes interesadas

Tipos de orientaciones	Características de las orientaciones	Participación de las partes interesadas

• procedimientos operativos normalizados
• códigos de conducta
• orientaciones habituales proporcionadas por oficiales de alto rango
	• detalladas y específicas
	• comprenden todas las actividades en las que pueden utilizarse perfiles sesgados:
	  • identificación y registro
	  • detenciones
	  • controles fronterizos
	  • uso de la fuerza, etc.
		• elaborar orientaciones con otras partes interesadas
		• facilitar las orientaciones a las comunidades
		• animar a las comunidades a comentar las orientaciones

Fuente: FRA, 2018.

Caso práctico

Código de práctica y el enfoque de los embajadores (policía neerlandesa)

La policía neerlandesa ha elaborado un código de práctica junto con organizaciones de la sociedad civil como Amnistía Internacional, que describe los cuatro principios de una identificación profesional:

☑ Una selección de personas legítima y justificable.

☑ Explicación del motivo que justifica la actuación de identificación y registro.

- ☑ Uso de una comunicación profesional.
- ☑ Los agentes deben reflexionar sobre sus prácticas, aportar comentarios y debatir entre sí.

Es difícil modificar prácticas que no se perciben como problemáticas, por ejemplo una labor policial proactiva que pueda traducirse en el uso de perfiles étnicos. La policía de Ámsterdam ha desarrollado un planteamiento ascendente en virtud del cual se involucra a los agentes de campo (embajadores) en los equipos, asistidos por sus directivos y formadores. El primer paso es incrementar la concienciación mediante la demostración y el análisis de los efectos que tienen las identificaciones proactivas sobre las personas afectadas, y mediante la introducción de un marco alternativo equitativo y eficaz. El segundo paso es que los agentes adopten esta nueva práctica.

Para más información en neerlandés, véase el sitio web de la policía.

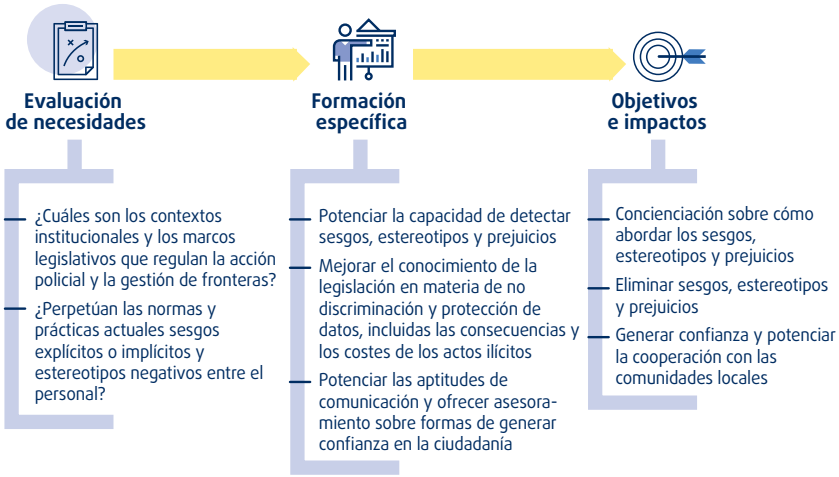
2.2.3. Formación específica

La formación para policías y guardias de fronteras es otra herramienta importante para minimizar el riesgo de uso ilícito de perfiles. Existen muchos tipos diferentes de formación, que pueden impartirse en diferentes etapas de la carrera de un agente, incluida la formación de contratación inicial, la formación en servicio y la formación profesional continua. Sea cual sea el tipo, los módulos de formación deben tener en cuenta la cultura de organización y ofrecer cursos que incorporen estrategias para sustituir y contrarrestar estereotipos. Por último, evaluar el impacto de la formación es crucial para determinar cómo ha contribuido a cambiar la percepción de los agentes y mejorar su práctica, así como para detectar carencias que puedan hacer necesaria formación adicional. La figura 6 destaca algunas cuestiones que se han de tener en cuenta para diseñar formación específica.

Algunos tipos de formación para policías y guardias de fronteras están ya muy desarrollados en algunos países, como la «formación en la diversidad» y la «formación en la sensibilidad». La formación en materia de diversidad trata de abordar los sentimientos personales en relación con la etnias, las diferencias y los estereotipos, y el modo en que influyen en nuestra vida cotidiana. Sin embargo, algunos cursos sobre diversidad no abordan necesariamente la discriminación. Algunos estudios alegan que la formación cultural y en diversidad puede de hecho señalar y reforzar las diferencias, de

modo que en lugar de reducir los estereotipos, los incremente ([30]). La «formación en sensibilidad cultural» (frente a la «formación en diversidad general») tiene por objeto educar a los policías y fuerzas de seguridad acerca de la cultura de determinados grupos étnicos con los que tienen encuentros frecuentes, pero a los que no conocen. Esta formación aborda «qué debe hacerse y qué no», y ofrece orientaciones sobre la cortesía desde diferentes perspectivas étnicas, religiosas o nacionales. La formación en sensibilidad cultural es más eficaz cuando se diseña y se imparte con la ayuda y participación de personas de las comunidades pertinentes.

Figura 6: El proceso y los objetivos en el desarrollo de formación específica



Fuente: *FRA, 2018.*

Caso práctico

Formación sobre elaboración lícita de perfiles

Formación sobre elaboración de perfiles para policías (Italia)

Desde 2014, el Observatorio Italiano para la Seguridad contra los Actos de Discriminación (*Osservatorio per la sicurezza contro gli atti discriminatori*) cuenta con un módulo de formación sobre perfiles étnicos para agentes

([30]) Wrench, J. (2007).

y cadetes de policía. Se centra en particular en los presuntos sesgos que pueden influir en los perfiles, sus consecuencias en términos de eficacia de las actividades policiales, y el impacto negativo que pueden tener para las relaciones con las comunidades. 5 000 personas han participado en este módulo de formación hasta la fecha. Desde 2017, también se ha incorporado un módulo de formación electrónica en los cursos de reciclaje para la policía.

Para más información, véase el sitio web de la Policía Nacional italiana.

Herramienta de derechos fundamentales en la formación de la guardia de fronteras (UE)

El plan de estudios común (PEC) para guardias de fronteras europeos establece el nivel mínimo de aptitudes y conocimientos que debe tener todo guardia de fronteras europeo. Contiene capítulos sobre sociología y derechos fundamentales. Hay apartados concretos sobre no discriminación (1.5.4) y sobre perfiles étnicos (1.7.10) para uso de los formadores. El PEC pone de relieve posibles riesgos vinculados a prejuicios, racismo, discriminación racial, xenofobia, islamofobia, homofobia, y otras actitudes intolerantes relacionadas con la elaboración de perfiles. La actualización del PEC de 2017 incluye secciones sobre nuevas competencias, sobre todo en el ámbito de los derechos fundamentales.

Además, Frontex ha diseñado un manual para formadores en consultas con universidades y organizaciones internacionales (véase Frontex, 2013). Los formadores encontrarán en él metodologías para mejorar los conocimientos y aptitudes de los guardias de fronteras en el ámbito de los derechos fundamentales y la protección internacional. Este manual menciona expresamente la elaboración de perfiles y establece normas básicas para evitar la discriminación. Se imparte formación periódicamente. Sin embargo, no existe ningún mecanismo permanente para valorar el cumplimiento de los objetivos de formación.

Para más información, véase Frontex (2012).

Jornadas de estudio sobre perfiles para oficiales de alto rango (Bélgica)

En 2015, el Centro de Policía y Seguridad (CPS) radicado en Gante (Bélgica), con la colaboración del organismo belga de igualdad (Unia), organizó una jornada de estudio sobre elaboración de perfiles étnicos (*Profilage ethnique:*

l'égalité sous pression?). Se trataron distintos aspectos de la cuestión, por ejemplo si los policías de ascendencia migrante pueden mejorar las relaciones con las comunidades de minorías étnicas y cómo; con qué frecuencia utiliza la policía perfiles étnicos; y cómo se ha evaluado esto.

En 2016, Unia organizó dos jornadas de estudio para oficiales de policía del norte de Bruselas a fin de concienciarlos sobre el uso de perfiles étnicos y animarlos a reflexionar sobre el uso de perfiles por los agentes de primera línea. Policías de España y del Reino Unido explicaron ejemplos de buenas prácticas a un público integrado por miembros de cuerpos policiales, investigadores y ONG. En particular, demostraron que si se reduce el uso de perfiles basados en el origen étnico, aumentan las detenciones de personas en busca y captura. Señalaron que esto fue posible porque se documentaron correctamente todas las identificaciones, además de garantizarse la transparencia en relación con los motivos que las justificaron. La formación tenía por objeto adquirir un conocimiento común de las prácticas de elaboración de perfiles étnicos para apoyar la investigación futura de las prácticas ejercidas actualmente por la policía en este terreno.

Para más información, véase Bélgica (2015 y 2017).

La formación debe abordar los sesgos y estereotipos que pueden estar integrados en las propias instituciones policiales y de gestión de fronteras. Es preciso examinar el contexto institucional general y las políticas internas —como los mecanismos de reclamación existentes, la presencia de un «código de silencio» entre compañeros, etc.— antes de impartir formación sobre la prevención de prácticas ilícitas de elaboración de perfiles. Los planes de estudios deben abordar los sesgos y estereotipos integrados en actuaciones policiales como las de identificación y registro, detención, retención y uso de la fuerza.

Los oficiales de alto rango y los mandos intermedios desempeñan un papel clave para que la formación tenga éxito, tanto en su calidad de participantes como por la importancia que confieran a la formación ([31]). Como destinatarios de la formación, los oficiales de alto rango pueden aprender nuevas prácticas y aptitudes que pueden transmitir a los agentes de primera línea. La cultura de organización, instaurada en gran medida por los altos mandos, tiene una influencia importante en el

([31]) Véase Comisión Europea (2017b).

comportamiento cotidiano de los policías y guardias de fronteras, incluida su forma de interactuar con los ciudadanos.

Los oficiales de alto rango también pueden velar por que la formación tenga una consideración positiva. El comportamiento del personal que ocupa puestos de mando —por ejemplo cómo comunican los supervisores los objetivos de la formación a los agentes, o si los agentes creen que son seleccionados aleatoriamente o porque son «agentes problemáticos»— puede afectar al grado de interés y participación en la formación. Animar a los agentes a participar activamente en los programas de formación y a estar dispuestos a cambiar su comportamiento para mejorar su trabajo cotidiano puede reforzar el impacto de la formación ([32]).

Una vez finalizada la formación, debe ser revisada y evaluada para valorar su impacto en el nivel de concienciación y los cambios de comportamiento.

Análisis de los principios rectores de la formación

La formación especializada es clave para que los perfiles se utilicen de forma lícita. La Comisión Europea estableció un conjunto de principios clave por los que debería regirse una formación eficaz y de calidad en relación con los delitos de odio. Los mismos principios se aplican a la formación sobre el uso lícito de perfiles.

Formación sobre delitos de odio dirigida a las autoridades policiales y penales: diez principios rectores clave

Garantizar el impacto y la sostenibilidad:

☑ Integrar la formación en un proceso más amplio para combatir la discriminación.

☑ Diseñar una metodología para satisfacer las necesidades de formación.

Establecer objetivos y crear sinergias:

☑ Adaptar los programas al personal.

([32]) Miller, J. y Alexandrou, B. (2016).

☑ Cooperar con la sociedad civil de manera estructurada.

Elegir la metodología correcta:

☑ Combinar diferentes metodologías.

☑ Formar a los formadores.

Transmitir contenidos de calidad:

☑ Diseñar un plan de formación con contenidos de calidad.

☑ Diseñar módulos formativos contra la discriminación.

Control y evaluación de los resultados:

☑ Vincular la formación a procesos de revisión del desempeño.

☑ Asegurar un control y una evaluación periódicos de los métodos de formación.

Para más información, véase Comisión Europea (2017a).

Sin embargo, la formación por sí sola no es eficaz para contrarrestar los sesgos inherentes a los agentes. Lo que hace falta es un cambio en el pensamiento institucional. Por tanto, las autoridades deben considerar intervenciones en varios sentidos para contrarrestar los sesgos personales e institucionales (véase el caso práctico).

Caso práctico

Combatir el «racismo institucional» en la policía

A raíz de las inquietudes expresadas acerca del papel que pudo tener la raza en la mala gestión de la investigación sobre el asesinato racista de Stephen Lawrence en el Reino Unido, el Gobierno británico puso en marcha un amplio estudio para determinar «las conclusiones que se podían extraer de cara a la investigación y el enjuiciamiento de los delitos con motivación racial».

El informe de este estudio, publicado en 1999, ponía de relieve el problema del «racismo institucional» presente en la Policía Metropolitana, incluida la disparidad de cifras de identificación y registro, por la considerable

preocupación que suscitaba en las comunidades afectadas. Las recomendaciones del estudio, que iban desde la sensibilización contra el racismo hasta la documentación y denuncia de incidentes, se inscribían en un llamamiento general a una mayor apertura, rendición de cuentas y recuperación de la confianza por el servicio policial.

Las revisiones publicadas en 2009, diez años después del estudio, destacaron mejoras en la interacción de la policía con las comunidades étnicas minoritarias y en su investigación de los delitos con motivación racial. Sin embargo, señalan que las personas negras todavía tienen muchas más probabilidades de ser objeto de identificación y registro que sus homólogas blancas.

Para más información, véase Reino Unido, Home Office (1999); Reino Unido, Equality and Human Rights Commission (2009); y Reino Unido, House of Commons Home Affairs Committee (2009).

2.2.4. Motivos razonables de sospecha: uso de la información de inteligencia y otras informaciones

Cuando los agentes de policía y de gestión de fronteras señalan a una persona, normalmente basan su decisión en un conjunto de elementos. Entre ellos cabe mencionar una información de inteligencia más «objetiva» y específica, el comportamiento, la vestimenta o los objetos que la persona lleve con ella, así como los conocimientos «subjetivos» basados en la experiencia.

Todos estos elementos pueden representar una «señal» de actividad ilegal. Sin embargo, la información debe combinarse y utilizarse con precaución. Las pruebas demuestran que para los agentes puede ser difícil distinguir entre los elementos objetivos y subjetivos en la práctica, como en el ejemplo citado en el recuadro.

Ejemplo

«Es muy subjetivo. Son tus sensaciones acerca de una persona y de un caso, pero también hay cuestiones probatorias de discrepancias en lo que dicen, incoherencias entre ellos y lo que dice su reagrupante, incoherencias entre lo que dicen y su documentación, entre lo que dicen y todo lo que pueden

llevar en su equipaje. Por tanto hay pruebas, pero [estas cosas por sí solas no] van totalmente contra alguien. Son todos los aspectos de la persona lo que el agente ha de tener en cuenta».
(Agente de inmigración en un gran aeropuerto británico)

Para más información, véase FRA (2014a), p. 46.

Análisis sobre la detección de personas que traten de entrar en un país de manera irregular

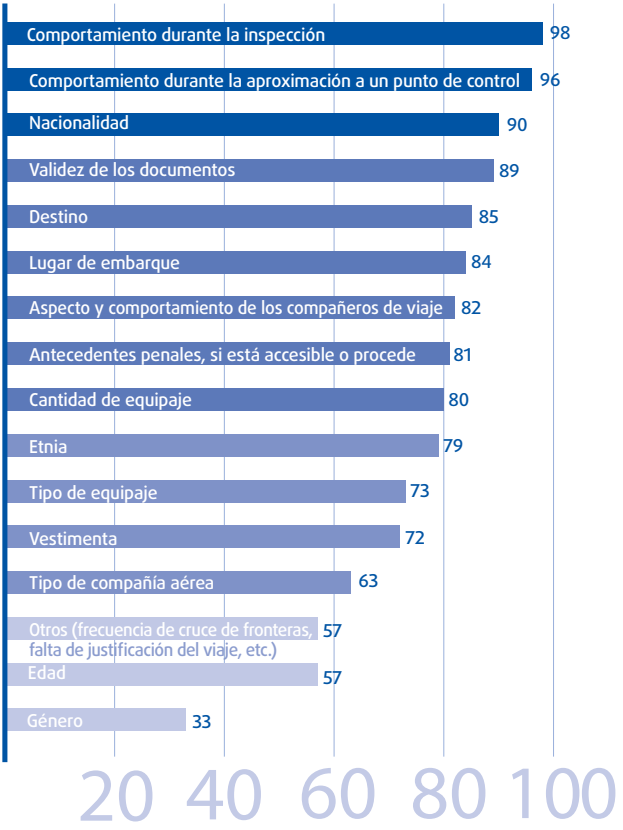
Un estudio realizado por la FRA en 2012 en grandes aeropuertos revela que los guardias fronterizos tienen en cuenta una serie de factores para decidir si una persona podría estar tratando de entrar en el país de manera irregular. A menudo se trata de una combinación de criterios «objetivos» —como el comportamiento de la persona cuando se acerca al punto de control y durante la inspección, el tipo y cantidad de equipaje que lleva, y la validez de sus documentos de viaje— y de experiencia personal de anteriores inspecciones en frontera, como se observa en la figura 7.

Los guardias de fronteras señalan el comportamiento durante la inspección o durante la aproximación al punto de control como el factor más útil para reconocer si una persona trata de entrar al país de manera irregular. Sin embargo, también se consideran importantes factores como la nacionalidad y la etnia, que podrían ser indicativos del uso de perfiles discriminatorios.

La vestimenta, que también se considera un indicador útil, es un ejemplo de cómo la información aparentemente «objetiva» puede utilizarse de manera sesgada en la práctica. Algunos tipos de vestimenta pueden vincularse a perfiles de riesgo específicos. Por ejemplo, las víctimas de trata de personas de una determinada nacionalidad pueden llevar normalmente ciertos tipos de prendas de vestir. Sin embargo, la vestimenta también puede indicar que una persona pertenece a un determinado grupo étnico o religioso. Aunque haya otras razones suficientes para justificar la inspección de segunda línea, las personas que se sientan muy identificadas con su origen étnico o contexto religioso, que hayan tenido experiencias negativas anteriores o que no reciban una explicación adecuada del agente, pueden percibir que el trato es discriminatorio.

Para más información, véase FRA (2014a). En relación con los perfiles de las víctimas de trata, véase Frontex (2017).

Figura 7: Indicadores que se consideran útiles o muy útiles para reconocer si una persona trata de entrar en el país de manera irregular antes de que los agentes hablen con ella (%)



Nota: *Se registraron entre 206 y 216 respuestas válidas de un total de 223. Los encuestados que no contestaron a una cuestión determinada han sido excluidos del cómputo de los resultados. No respondieron entre 7 y 17 personas, según la cuestión.*

Fuente: *FRA, Border guard survey, 2012 (question 17).*

Una buena información de inteligencia sobre patrones de comportamiento o eventos puede aumentar la objetividad en el uso de perfiles. Podría estar relacionada con actividades criminales o bien, en el caso de la gestión de fronteras, con la migración

irregular o la delincuencia transfronteriza. Cuando las actuaciones policiales y de gestión de fronteras se basan en información de inteligencia específica y oportuna, como la obtenida sobre una persona o un contexto específicos, es más probable que sean objetivas y menos probable que se basen en estereotipos.

Además de información de inteligencia y elementos objetivos, se puede utilizar de manera legítima información acerca de características protegidas, reales o percibidas, como la raza, el origen étnico, la nacionalidad, el género o la religión, como componente añadido a los análisis de elaboración de perfiles en determinadas circunstancias. Para que el uso de esta información sea lícito, debe estar regulado por ley, respetar los derechos y libertades afectados en lo esencial, ser proporcionado (es decir, cumplir con un equilibrio de intereses) y necesario (es decir, no debe haber medios menos restrictivos disponibles). Debe existir una razón justificable, al margen de los motivos protegidos, para que los agentes traten a una persona de manera diferente a otros ciudadanos. La razón también debe estar específicamente relacionada con esa persona concreta, como en el ejemplo descrito en el recuadro.

Ejemplo

Según los testigos, el sospechoso de un robo llevaba deportivas rojas y una gorra de béisbol negra, medía entre 1,60 y 1,70 m y parecía de origen chino. En estas circunstancias, las autoridades policiales podían considerar legítimamente que el origen étnico era pertinente para determinar si una persona podía ser sospechosa, ya que disponían de información de inteligencia específica.

Análisis de las descripciones detalladas de los sospechosos

Una buena descripción de un sospechoso puede reducir el riesgo de elaboración ilícita de un perfil. La descripción de un sospechoso consiste en detalles acerca de esa persona, como el color de la piel, el cabello y los ojos, la altura y el peso, y la vestimenta. Estos detalles son facilitados por la víctima del delito o por los testigos, o provienen de otra información de inteligencia específica. Una buena descripción puede ser utilizada por los agentes en sus actuaciones de identificación y registro dirigidas a detener sospechosos, o como justificación para que una persona que pasa por el control fronterizo sea sometida a una inspección de segunda línea.

Sin embargo, cuando los policías reciben la descripción de un sospechoso excesivamente genérica, que menciona la raza, la etnia o características similares, no deben utilizar esa descripción como justificación de sus

operaciones. En estos casos, es probable que se identifique a demasiadas personas inocentes que casualmente compartan esas mismas características. Por el contrario, deben tratar de obtener más información operativa específica para orientar sus investigaciones.

Para más información, véase Comisión Europea (2017b).

La información que parece objetiva puede no obstante incorporar sesgos. Factores aparentemente objetivos, como la hora, el día, el lugar, etc., pueden utilizarse como indicadores de motivos de discriminación prohibidos, como la raza, el origen nacional, el género, la orientación sexual o la religión, reales o percibidos, como se observa en el ejemplo siguiente.

Ejemplo

Se realiza una operación de identificación y registro alrededor del mediodía en la zona X. Sin embargo, este es el tiempo de oración más importante para los musulmanes. Dado que la zona X está cerca de una mezquita, factores supuestamente objetivos como la hora, la fecha y el lugar podrían de hecho servir como indicadores para una operación de identificación y registro basada en el motivo discriminatorio prohibido que es la religión.

Del mismo modo, estar atentos a ciertos comportamientos sospechosos puede parecer una manera objetiva de detectar posibles infracciones. Sin embargo, los agentes pueden interpretar el comportamiento de una persona de diferentes maneras, en función de otras características de esa persona. Las pruebas demuestran que el conocimiento y la interpretación de la información de inteligencia en la práctica pueden ser muy diferentes según los agentes y que a menudo no se corresponden con auténticos patrones delictivos ([33]).

Si se facilitase información de inteligencia oportuna y detallada a los agentes, por ejemplo en la reunión informativa de la jornada que tiene lugar antes de iniciarse cada turno, estos actuarían con menor discrecionalidad y sabrían cómo ejercer sus facultades más concretamente en relación con los patrones delictivos actuales y con los problemas de seguridad detectados. De este modo se reduce la influencia del sesgo. Es más efectivo mejorar la calidad y el uso de la información de inteligencia para analizar factores de comportamiento o información específica cuando se combina con una mayor supervisión y vigilancia del modo en que los agentes ejercen sus facultades.

([33]) United Kingdom National Policing Improvement Agency (NPIA) (2012).

Caso práctico

Garantizar la objetividad en la elaboración de perfiles

Reuniones previas al inicio de la jornada (UE)

El Catálogo Schengen recomienda que antes de cada turno, el agente de guardia facilite información sobre posibles indicadores de riesgo y perfiles de riesgo. La superposición entre turnos puede dar tiempo suficiente para que el personal del turno entrante y el saliente intercambien información, así como para celebrar una sesión informativa adecuada.

Para más información, véase Consejo de la Unión Europea (2009).

Programa de formación SDR (Países Bajos)

El programa de formación de búsqueda, detección y reacción (SDR, por sus siglas en inglés) está dirigido a prevenir actos delictivos o terroristas antes de que se produzcan mejorando la capacidad del personal de seguridad en relación con los perfiles conductuales. Esto implica no prestar atención a características inalterables como el color de la piel, y centrarse por el contrario en las conductas individuales para tomar decisiones de acción policial. Dado que los indicadores de conducta sospechosa son contextuales, la formación se matiza según el entorno. Se rechaza la idea de que existe una solución única para todas las situaciones. Una vez detectado un patrón de conducta pertinente, los agentes deben actuar de manera «sensible». En la mayoría de los casos, mantendrán una conversación informal con el sospechoso en lugar de ejercer sus facultades policiales formales. El programa incluye clases teóricas, además de la formación aplicada y práctica.

Para más información, visite el sitio web de SDR Academy.

Herramienta de identificación y registro «práctica profesional autorizada» (APP) (Reino Unido)

El College of Policing del Reino Unido ha elaborado orientaciones sobre «prácticas profesionales autorizadas» (APP, por sus siglas en inglés) que comprenden varios aspectos del trabajo policial. La APP sobre identificación y registro explica qué es esta operación, por qué es importante ejercer estas facultades correctamente, y qué características tiene una operación lícita

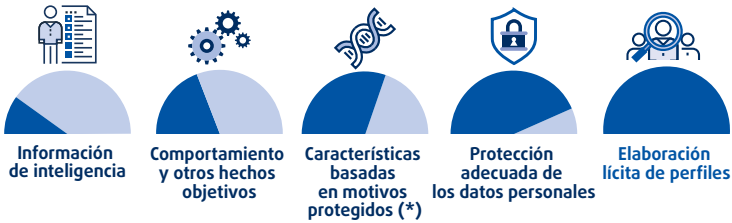
de identificación y registro. Explica que los siguientes aspectos favorecen la licitud y eficacia de los encuentros de identificación y registro:

- **Equidad**: la decisión del agente de identificar y registrar a una persona debe basarse exclusivamente en factores objetivos apropiados. Nunca se puede parar a una persona basándose única o principalmente en características protegidas o factores como condenas anteriores.
- **Legalidad**: la actuación de identificación y registro debe tener una base legal que se aplique de manera lícita.
- **Profesionalidad**: durante un encuentro de identificación y registro, el agente debe cumplir las normas de conducta profesionales, especialmente el Código Ético, comunicarse de manera efectiva con la persona afectada y tratarla con dignidad y respeto.
- **Transparencia**: el encuentro individual debe documentarse con exactitud. Deben garantizarse la supervisión y el control eficaces de las actuaciones de identificación y registro, así como su escrutinio público.

Para más información, véase Reino Unido, College of Policing (2016).

La figura 8 ilustra los distintos elementos que pueden utilizarse en un proceso de elaboración lícita de perfiles; cómo se combinen dependerá de la naturaleza del caso concreto.

Figura 8: Combinación de elementos

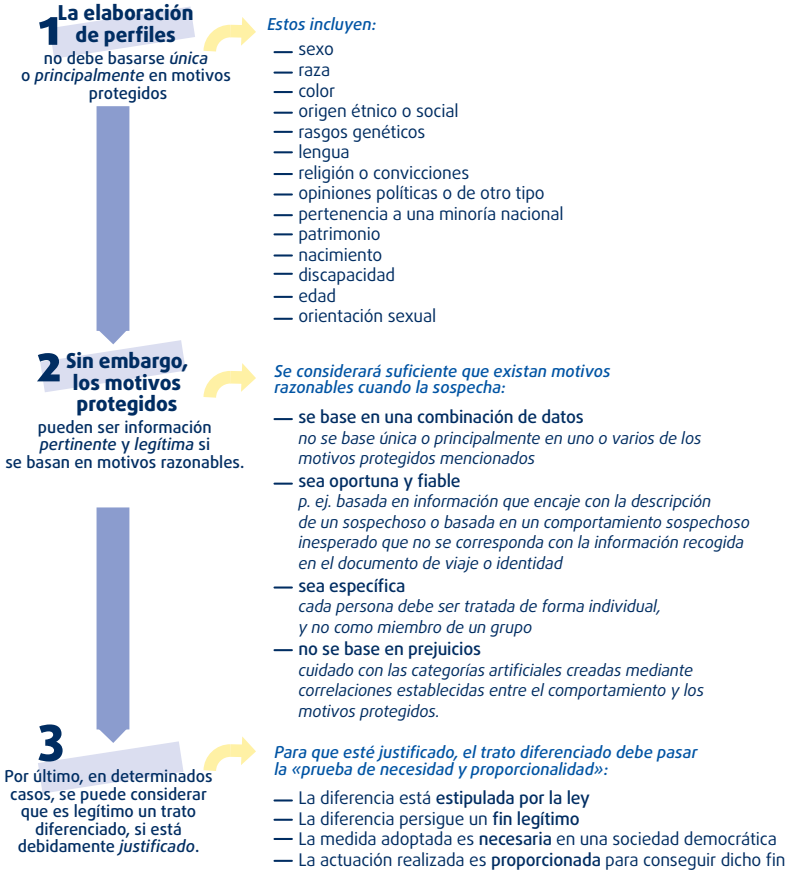


(*) Véase la lista de motivos protegidos en virtud del Derecho de la Unión en la figura 9. Un perfil nunca debe basarse única o fundamentalmente en características protegidas.

Fuente: FRA, 2018.

La figura 9 indica cómo se pueden combinar estos elementos para asegurarse de que los perfiles elaborados no sean discriminatorios.

Figura 9: Elementos de la elaboración de perfiles sin discriminación



Notas: *La lista de motivos protegidos varía según los Estados miembros. Véase una lista de motivos de discriminación incluidos en el Código Penal de cada uno de los Estados miembros en FRA (2018d). Véase también el sitio web de Equinet (European Network of Equality Bodies), que recoge los motivos de discriminación contemplados por los organismos de igualdad nacionales.*

Fuente: *FRA, 2018.*

2.2.5. Formularios de identificación y registro para la elaboración de perfiles policiales

Los formularios de identificación y registro pueden ayudar a los agentes a reflexionar sobre si las identificaciones que llevan a cabo se basan en motivos razonables, y permiten a los oficiales de alto rango vigilar posibles prácticas discriminatorias en las actuaciones de identificación y registro de agentes concretos. Aunque a veces se consideran molestos, también permiten documentar las identificaciones que, cuando se cotejan, ofrecen datos que pueden indicar si se están realizando de manera lícita ([34]) y pueden ayudar a promover la apertura y la rendición de cuentas. Para documentar esta información, además de cumplimentar formularios en papel, pueden utilizarse nuevas tecnologías, como *apps* móviles.

En el recuadro de análisis, se describen algunos aspectos importantes que han de incorporarse al diseño de los formularios de identificación y registro.

Análisis de lo que hace que un formulario de identificación y registro sea adecuado

Para ser útiles, los formularios de identificación y registro tienen que estar bien diseñados. En primer lugar, cumplimentar los formularios aumenta la carga de trabajo de los agentes. Si no están claramente diseñados y son razonablemente breves, se corre el riesgo de que los agentes no los cumplimenten por entero o que lo hagan de manera superficial. En segundo lugar, unos buenos formularios permiten extraer y cotejar datos fácilmente para facilitar el control y evaluación de las actuaciones de identificación y registro.

Siempre que sea posible, los formularios de identificación y registro deberán:

- Utilizar campos con varias opciones de respuesta, que son más rápidos de cumplimentar y más fáciles de procesar estadísticamente.
- Presentar una lista exhaustiva de opciones para cada enunciado.
- Evitar enunciados ambiguos.
- Ser fáciles de entender, tanto para el agente como para la persona identificada.

([34]) United Kingdom, Stop Watch (2011).

- Incluir:
  - los motivos legales del registro (es preferible incluir explicaciones sencillas que una lista de normas);
  - la fecha, hora y lugar de registro de la persona o vehículo;
  - el objeto del registro, p. ej. objetos que estén buscando los agentes;
  - el resultado de la identificación;
  - el nombre y la comisaría a la que pertenecen los agentes que realizan el registro;
  - se pueden documentar los datos personales de las personas registradas, como su nombre, dirección y nacionalidad. Sin embargo, la persona afectada puede negarse a facilitar esta información.

Para que sean efectivos, los formularios deben cumplimentarse en el momento de realizar la identificación.

Deberá facilitarse una copia a la persona identificada o a la persona a cargo del vehículo registrado. En el Reino Unido, las personas identificadas tienen derecho a solicitar una copia del expediente en un plazo de tres meses desde la identificación. De este modo, el formulario no solo es una prueba de identificación para la policía, sino también para la persona identificada.

Para más información, véase Reino Unido, West Midlands Police (2012), p. 7; y Reino Unido, Home Office (2014a).

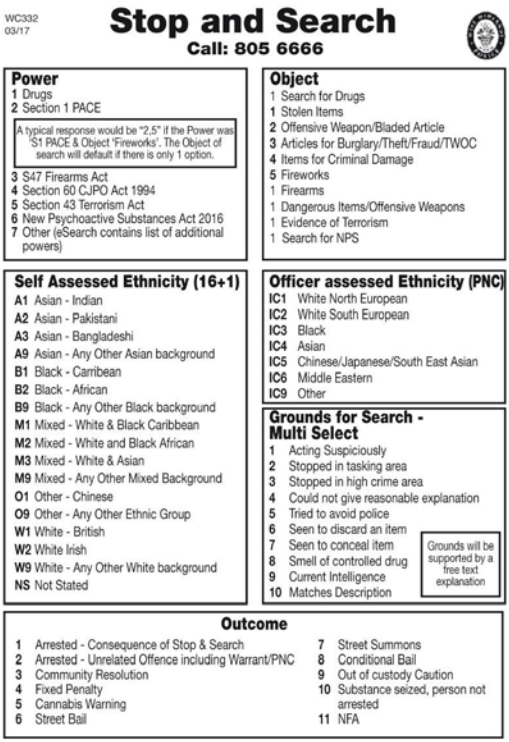
Caso práctico

Formulario de identificación y registro (Reino Unido)

Veáse a continuación una reproducción del formulario de identificación y registro utilizado por la Policía de West Midlands en el Reino Unido.

Se observa que la persona identificada debe declarar si pertenece a una de las categorías de etnia contempladas, que incluyen las opciones «otra» o «no indicada». El agente que realiza la identificación puede añadir su percepción si no está de acuerdo con lo indicado por la persona identificada.

El Código de práctica para el ejercicio de las facultades de identificación y registro en el Reino Unido establece que los agentes deben explicar a las personas identificadas que la información sobre la etnia «es necesaria para obtener una imagen fiel de la actividad de identificación y registro y para contribuir a mejorar el seguimiento étnico, corregir prácticas discriminatorias y promover un ejercicio eficaz de las competencias policiales».



WC332
03/17

Stop and Search
Call: 805 6666

Power
1 Drugs
2 Section 1 PACE

A typical response would be "2,5" if the Power was 'S1 PACE & Object 'Fireworks'. The Object of search will default if there is only 1 option.

3 S47 Firearms Act
4 Section 60 CJPO Act 1994
5 Section 43 Terrorism Act
6 New Psychoactive Substances Act 2016
7 Other (eSearch contains list of additional powers)

Object
1 Search for Drugs
1 Stolen Items
2 Offensive Weapon/Bladed Article
3 Articles for Burglary/Theft/Fraud/TWOC
4 Items for Criminal Damage
5 Fireworks
1 Firearms
1 Dangerous Items/Offensive Weapons
1 Evidence of Terrorism
1 Search for NPS

Self Assessed Ethnicity (16+1)
A1 Asian - Indian
A2 Asian - Pakistani
A3 Asian - Bangladeshi
A9 Asian - Any Other Asian background
B1 Black - Carribean
B2 Black - African
B9 Black - Any Other Black background
M1 Mixed - White & Black Caribbean
M2 Mixed - White and Black African
M3 Mixed - White & Asian
M9 Mixed - Any Other Mixed Background
O1 Other - Chinese
O9 Other - Any Other Ethnic Group
W1 White - British
W2 White Irish
W9 White - Any Other White background
NS Not Stated

Officer assessed Ethnicity (PNC)
IC1 White North European
IC2 White South European
IC3 Black
IC4 Asian
IC5 Chinese/Japanese/South East Asian
IC6 Middle Eastern
IC9 Other

Grounds for Search - Multi Select
1 Acting Suspiciously
2 Stopped in tasking area
3 Stopped in high crime area
4 Could not give reasonable explanation
5 Tried to avoid police
6 Seen to discard an item
7 Seen to conceal item
8 Smell of controlled drug
9 Current Intelligence
10 Matches Description

Grounds will be supported by a free text explanation

Outcome
1 Arrested - Consequence of Stop & Search
2 Arrested - Unrelated Offence including Warrant/PNC
3 Community Resolution
4 Fixed Penalty
5 Cannabis Warning
6 Street Bail
7 Street Summons
8 Conditional Bail
9 Out of custody Caution
10 Substance seized, person not arrested
11 NFA

Para más información, véase Reino Unido, West Midlands Police (2017a); y Reino Unido, Home Office (2014a), p. 19.

Muchas fuerzas están dejando de recoger datos de identificación y registro en formularios, y prefieren utilizar tecnologías como *apps* para teléfonos móviles, sistemas de radio, terminales de datos móviles u ordenadores portátiles. Estas tecnologías pueden agilizar el proceso de documentación y reducir la burocracia, pero también pueden entrañar nuevos riesgos, especialmente en relación con el uso algorítmico de datos personales (véase el capítulo 3).

Caso práctico

Documentación sobre la marcha de las actuaciones de identificación y registro

«eSearch» (West Midlands Police, Reino Unido)

Adoptado en abril de 2014, este sistema se basa en una llamada entre el agente sobre el terreno y un miembro del personal del Centro de Contacto (sala de control). Los datos de identificación y registro se documentan inmediatamente en el Centro de Contacto y se incorporan a una base de datos. Posteriormente se puede acceder a esta información y utilizarla para examinar la eficacia de las actuaciones de identificación y registro, tanto interna como externamente. eSearch ha transformado la manera de documentar las actuaciones de identificación y registro. Los expedientes se pueden visualizar mucho más rápidamente en los sistemas policiales, lo que resulta ventajoso para la información y la integración en la labor policial operativa.

Para más información, véase Reino Unido, West Midlands Police (2014) y Reino Unido, West Midlands Police (2016).

***App* móvil para agentes de primera línea (West Midlands Police, Reino Unido)**

Una nueva *app* móvil presentada en octubre de 2017 tiene por objeto aumentar la rapidez y eficacia de las actuaciones de identificación y registro. La *app* eSearch permite a los agentes introducir la información de los encuentros callejeros directamente en la *app* a través de sus teléfonos móviles, sin necesidad de llamar al Centro de Contacto. Cada identificación recibe un número de referencia único, y el GPS registra su localización automáticamente. Se estima que esta *app* reducirá las comunicaciones con el Centro de Contacto en casi mil llamadas mensuales.

Para más información, véase Reino Unido, West Midlands Police (2017b).

Los oficiales de alto rango han de velar por que las operaciones de identificación y registro sean lícitas. El ejemplo siguiente ilustra cómo pueden los oficiales de alto rango mantener la supervisión. También deben velar por que las actuaciones de identificación y registro no se utilicen como medida del desempeño en función del número de identificaciones realizadas.

Caso práctico

Firma de expedientes de identificación y registro (Reino Unido)

Desde agosto de 2014, todos los expedientes de identificación y registro del Reino Unido deben ser firmados por el supervisor del agente que haya realizado el registro. Los expedientes se registran como conformes o no conformes a las normas pertinentes. En este último caso, el agente informante debe consignar por qué en el expediente de identificación y registro.

Para más información, véase Reino Unido, Home Office (2014a).

2.3. Rendición de cuentas

Puntos clave

- Los agentes de policía y de gestión de fronteras deben **rendir cuentas** de que la elaboración de perfiles se efectúa conforme a la ley.
- **Recopilar datos fiables, precisos y oportunos** sobre las actividades de elaboración de perfiles es crucial para garantizar la rendición de cuentas.
- **Unos mecanismos de reclamación efectivos** pueden tener efectos disuasorios en relación con los abusos de poder y ayudar a inspirar y restablecer la confianza de los ciudadanos en las operaciones de las autoridades policiales y de gestión de fronteras.
- **Las reuniones de valoración con miembros de la ciudadanía** para escuchar sus opiniones, analizar la aplicación de perfiles y conocer su valoración de las operaciones son la oportunidad de aprender lecciones importantes y mejorar las prácticas de elaboración de perfiles.

La rendición de cuentas es un principio esencial de la gobernanza democrática. En términos muy generales, consiste en dar respuestas a quienes tienen derecho a exigir cuentas ([35]). La rendición de cuentas no solo se refiere a las decisiones individuales, sino también a las institucionales (por lo que se llama «responsabilidad institucional»). Igual que los funcionarios y organismos públicos, los agentes de policía

([35]) Bovens, M., Schillermans, T. y Goodlin, R. E. (2014), pp. 1–11.

y de gestión de fronteras, así como sus organizaciones, deben rendir cuentas de sus decisiones y actuaciones a los ciudadanos. Esto incluye rendir cuentas de que la elaboración de perfiles se realiza conforme a la ley.

Recoger datos fiables, precisos y oportunos es crucial para garantizar la rendición de cuentas. Dado que gran parte de los datos contienen información personal sensible, deben tratarse con arreglo a las normas y procedimientos de protección de datos (véase el capítulo 3).

Lista de control de rendición de cuentas

La lista de control siguiente contiene una serie de medidas básicas que pueden adoptar las autoridades policiales y de gestión de fronteras para asegurarse de que pueden rendir cuentas de sus decisiones y actuaciones en relación con la elaboración y aplicación de perfiles. Esta lista puede orientar a los agentes para mejorar su capacidad de rendición de cuentas, pero no cabe suponer que se trata de cuestiones obligatorias tanto para los agentes de policía como para los de gestión de fronteras. Según el contexto, puede que algunas recomendaciones no sean de aplicación a las particularidades de la gestión de fronteras.

1. Detectar

- ☑ Reconocer y **asumir** el problema de elaboración ilícita de perfiles. Los sesgos y los estereotipos existen y entrañan riesgos para las personas implicadas, incluidos los agentes y las comunidades locales.
- ☑ **Recopilar y utilizar datos desagregados**: es una herramienta importante para valorar la eficacia y el desempeño.
- ☑ Participar en paneles externos organizados por la comunidad o la sociedad civil para recibir **valoraciones** sobre las prácticas utilizadas y aumentar la confianza en las operaciones realizadas.

2. Recoger información

- ☑ Garantizar la capacidad de rendición de cuentas **documentando** las actividades de elaboración y utilización de perfiles.

- ☑ Siempre que se adopten las garantías necesarias, la **videovigilancia** o las **cámaras corporales** pueden aumentar la capacidad de rendición de cuentas y proporcionar pruebas que respalden las actuaciones para modificar patrones de comportamiento sesgado.
- ☑ Crear **formularios de identificación y registro** que deban ser cumplimentados por los policías tras cada identificación.

3. Actuar y prevenir

- ☑ Realizar **evaluaciones** para determinar si existen normas y prácticas que perpetúen sesgos explícitos o implícitos y estereotipos negativos.
- ☑ Introducir cursos específicos o **sesiones de formación** dedicadas a corregir los sesgos y estereotipos personales e institucionales.
- ☑ **Proporcionar información** a las personas identificadas para incrementar la percepción de que la actuación es justa, y darles información suficiente para que decidan si procede o no interponer recurso. Para los casos en que se somete a la persona a una inspección de segunda línea en los pasos fronterizos, facilitar información es una obligación legal.
- ☑ Mostrar **tolerancia cero** en la organización a los incidentes sesgados.
- ☑ Establecer **mecanismos internos** de supervisión y control, como paneles internos para analizar si las identificaciones se basan en motivos razonables.
- ☑ Asegurarse de que los **indicadores de desempeño** estén ligados a la prevención de sesgos y estereotipos.
- ☑ Establecer **mecanismos de reclamaciones** como disuasión de los abusos de poder y garantizar la rendición de cuentas.

Fuente: FRA, 2018.

2.3.1. Vigilancia interna

Las autoridades policiales y de gestión de fronteras tienen una misión importante de liderazgo y dirección para establecer unos valores que defiendan los derechos individuales y el principio de no discriminación, tanto en la organización como en sus tratos con los ciudadanos. También contribuyen a establecer un clima de rendición

de cuentas y transparencia. La comunicación abierta entre el personal (tanto horizontal como vertical) y el establecimiento de normas claras de comportamiento, como códigos de conducta profesional, son dos elementos internos que deben existir para mejorar la rendición de cuentas. También la selección y la formación del personal son importantes (véase el apartado 2.2.3).

De acuerdo con el Derecho de la Unión, cualquier autoridad u organismo público debe designar un **delegado de protección de datos,** cuya misión es asesorar a las fuerzas policiales y fronterizas en relación con sus obligaciones de protección de datos, incluida la documentación de sus actividades de tratamiento de datos o la realización de evaluaciones de impacto de la protección de datos. En el contexto de la elaboración de perfiles, el delegado de protección de datos, por ejemplo, asesora y vigila que los datos personales recogidos para o durante la elaboración de perfiles sean tratados y conservados de forma lícita.

Análisis del papel de los delegados de protección de datos

La **Directiva sobre la policía** obliga a los Estados miembros a designar un delegado de protección de datos, que tiene los siguientes cometidos:

- vigilar el cumplimiento de la legislación aplicable en relación con la protección de los datos personales, que incluye:
  - asignar responsabilidades;
  - formar y concienciar al personal;
  - auditorías;
- asesorar sobre la evaluación de impacto de la protección de datos y vigilar su realización;
- actuar como punto de contacto para la autoridad de control.

El delegado de protección de datos debe participar de manera integral y oportuna en todas las cuestiones relacionadas con la protección de los datos personales.

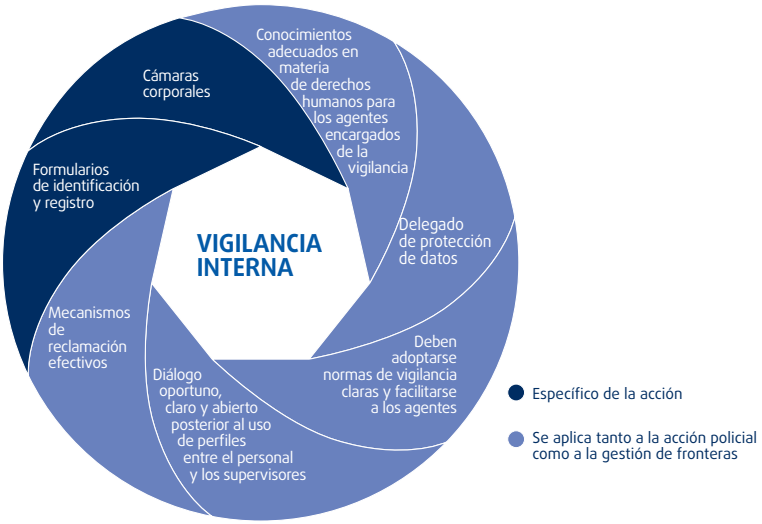
Véanse los artículos 32 a 34 de la Directiva sobre la policía.

En las fuerzas policiales, la vigilancia interna de la elaboración de perfiles puede formar parte de una gran variedad de otras medidas destinadas a documentar los encuentros entre las autoridades y la población en general (véase la figura 10), que incluyen el uso de:

- **formularios de identificación y registro**: es una herramienta práctica y útil para animar a los agentes a realizar identificaciones bien motivadas, y promover la apertura y la rendición de cuentas ante la ciudadanía (véase el apartado 2.2.5);
- **cámaras corporales**: siempre que se adopten las garantías necesarias, pueden aumentar la confianza entre las comunidades y la policía, y actuar como factor de disuasión en relación con los usos indebidos de la fuerza y la discriminación (véase el apartado 2.3.2).

Estas medidas también pueden utilizarse en las actividades de vigilancia interna de las organizaciones de gestión de fronteras. Por ejemplo, el Catálogo Schengen recomienda documentar el número de personas sometidas a inspecciones de segunda línea y los motivos para hacerlo. Además, los diferentes contextos de los controles fronterizos, las infraestructuras existentes en los pasos fronterizos y la presencia de superiores *in situ* crean otras oportunidades de vigilancia interna. Por ejemplo, puede que se disponga de equipos tecnológicos adicionales, como los de videovigilancia.

Figura 10: Elementos de la vigilancia interna



Fuente: *FRA, 2018.*

Siempre que se adopten las garantías necesarias, las imágenes de vídeo pueden aportar pruebas para determinar cómo se utilizan los perfiles, y para el caso de que se presenten reclamaciones. Por ejemplo, pueden confirmar si el comportamiento de una persona que esperaba la inspección de primera línea era motivo suficiente para someterla a una inspección de segunda línea.

A diferencia de lo que ocurre en las actuaciones de identificación y registro, los viajeros básicamente esperan que haya videovigilancia en los pasos fronterizos por su carácter público y por consideraciones de seguridad. No obstante, el uso de este tipo de herramientas debe respetar el derecho a la intimidad y las normas de protección de datos aplicables.

Documentar las actuaciones puede tener ventajas a corto y largo plazo. El ejemplo de los formularios de identificación y registro demuestra que:

- **A corto plazo**, los formularios de identificación y registro pueden facilitar la rendición de cuentas sobre el terreno. En el Reino Unido, toda persona identificada recibe una copia de este formulario o un recibo que indica dónde pueden obtenerla. Contiene los motivos detallados de la identificación, así como información de dónde y cómo reclamar. De este modo, la persona afectada puede conocer el motivo de la identificación e impugnarla si la considera injusta.

- **A largo plazo**, el análisis de estos expedientes permite a la fuerza policial determinar si las facultades de identificación y registro se aplican de forma desproporcionada a miembros de grupos minoritarios, y adaptar las directrices para los agentes en consecuencia. Estos expedientes pueden hacerse públicos para aumentar la transparencia y fomentar la confianza de los ciudadanos en el ejercicio de las facultades de identificación y registro.

Expedientes de las actuaciones: ¿qué dice la ley?

Para garantizar la licitud del tratamiento de los datos, la Directiva sobre la policía exige que las autoridades policiales documenten todas las categorías de actividades de tratamiento bajo su responsabilidad. Más aún, en los sistemas de tratamiento automatizados, deben conservar los registros «log» que permiten saber quién ha consultado o revelado datos personales, cuándo ha ocurrido, quién ha recibido los datos, y la justificación del tratamiento (véase el apartado 3.1.3).

Artículos 24 y 25 de la Directiva sobre la policía

Caso práctico

Examen de los expedientes para detectar la desproporción en las actuaciones de identificación y registro (Reino Unido)

El Código de Práctica de la Ley de pruebas policiales y criminales adoptado en Inglaterra y Gales (Reino Unido) impone a las fuerzas policiales la obligación legal de examinar el ejercicio de las facultades de identificación y registro para detectar si se están «ejerciendo en virtud de imágenes estereotipadas o generalizaciones inadecuadas». Se debe detectar e investigar todo ejercicio aparentemente desproporcionado de estas facultades por determinados agentes o grupos de agentes o en relación con determinados segmentos de la comunidad, y deben adoptarse medidas adecuadas para corregirlo. Además, la policía debe adoptar medidas para que los expedientes sean examinados por representantes de la comunidad, y explicar el ejercicio de las facultades de identificación y registro en el ámbito local.

Para más información, véase Reino Unido, Home Office (2014a).

La policía del Reino Unido ha adoptado varias herramientas para aumentar la transparencia facilitando el acceso a los datos de identificación y registro. En el sitio web, www.police.uk los usuarios pueden introducir su código postal para ver información detallada acerca del número y carácter de las identificaciones en su ámbito local. La información publicada se obtiene de los formularios de identificación y registro cumplimentados. Además, el cuadro de control de identificación y registro de la Policía Metropolitana contiene datos de todas las actuaciones de identificación y registro realizadas en Londres, que incluyen el porcentaje de personas identificadas que pertenecen a minorías étnicas en comparación con la población total. Los usuarios pueden acceder a datos detallados en línea de diferentes maneras, como por ejemplo:

- un mapa que muestre la localización exacta de las operaciones de identificación y registro realizadas en una zona concreta cada mes. Esta herramienta también ofrece información detallada sobre la actuación de identificación y registro (objeto, tipo, resultado y si formaba parte de una operación policial), sobre la persona (género, intervalo de edad, etnia declarada por la persona y etnia apreciada por el agente), y la legislación que respalda la licitud de la actuación (véase la figura 11); y

- una visión general de estadísticas y gráficos que presentan las actuaciones policiales de identificación y registro. De este modo, la información se puede agregar y descargar.

Aunque esta práctica fomenta la transparencia y la confianza, puede afectar a los derechos a la intimidad y la protección de datos de las personas afectadas. Es posible que se pueda deducir la identidad de una persona a partir de la combinación de datos disponibles en esta u otras herramientas en línea. Es necesario evaluar y, en su caso, corregir este tipo de riesgos.

2.3.2. Cámaras corporales

Es cada vez más frecuente que las fuerzas policiales lleven cámaras corporales, que pueden contribuir a garantizar la rendición de cuentas, mejorar la calidad de los encuentros individuales, y modificar los patrones de comportamiento sesgado. También pueden contribuir a mitigar situaciones peligrosas. Al igual que la policía graba imágenes, cada vez es más habitual que los ciudadanos filmen las identificaciones y otras interacciones con la policía. Estas imágenes también pueden utilizarse para revisar la práctica policial.

Caso práctico

Eficacia de las cámaras corporales

En el Reino Unido, un estudio realizado en 2015 sobre el uso de 500 cámaras por 814 agentes de la Policía Metropolitana reveló que no existía «ningún efecto general sobre el número o tipo de identificaciones y registros realizados; ningún efecto sobre el porcentaje de detenciones por delitos violentos; y ninguna prueba de que las cámaras modificasen el trato dispensado por los agentes a víctimas o sospechosos». Los informes de evaluación de ensayos parecidos realizados por otras fuerzas policiales muestran poca o ninguna evidencia de que estos aparatos hayan tenido algún efecto positivo en la reducción de la delincuencia, las reclamaciones contra agentes o el uso de la fuerza.

Para más información, véase Big Brother Watch (2017).

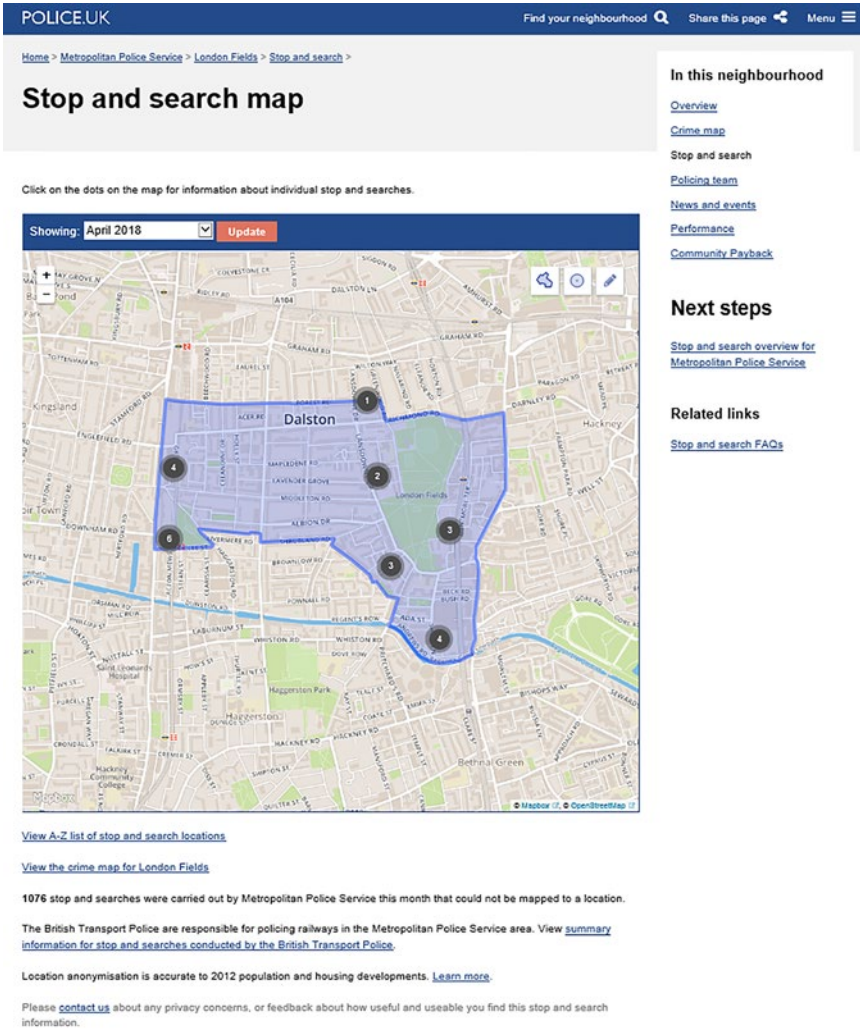
En Francia, se desplegaron cámaras corporales en trescientas localidades durante un período piloto de dos años. En junio de 2018, una revisión del Ministerio del Interior destacó los efectos y resultados positivos del ensayo. En particular, el informe destacaba que las cámaras corporales disuadían a las personas identificadas de insultar o hablar agresivamente a la policía. Los informes de los municipios indicaban que el uso de cámaras individuales reducía la agresividad y los insultos contra los policías. Algunos municipios señalaron que las cámaras corporales parecían haber mitigado situaciones que, de otro modo, podrían haber terminado con la comisión de un delito contra los policías. Aunque estos informes indican que la utilidad de las cámaras corporales es concretamente su efecto disuasorio, algunas imágenes se utilizaron como prueba en juicios para identificar a delincuentes. Por último, varios municipios destacaron la utilidad educativa del dispositivo, ya que algunos policías recibieron formación sobre procedimientos y técnicas de intervención visualizando las grabaciones realizadas durante las intervenciones. Tras el período piloto, se ha presentado un proyecto de ley al Parlamento francés con el fin de armonizar el uso de este tipo de cámaras en todas las fuerzas policiales y ampliarlas a bomberos y funcionarios de prisiones.

Para más información, véase Francia, Ministerio del Interior (2018).

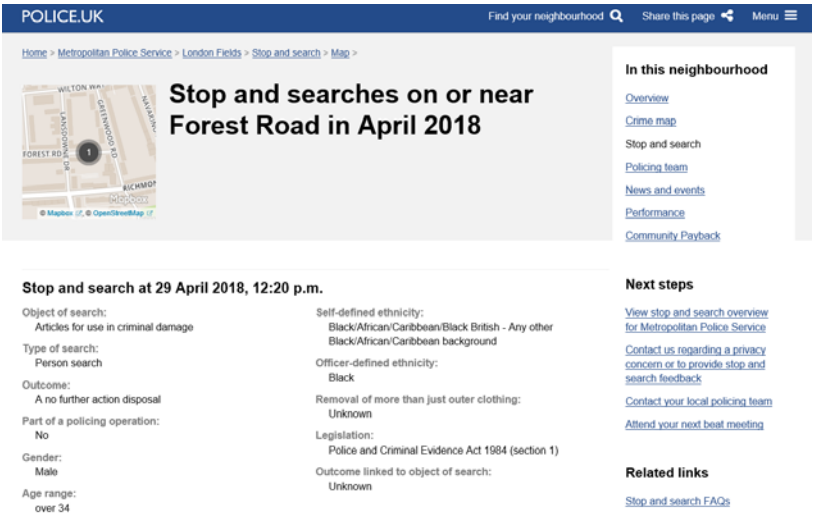
En 2012-2013, se realizó un ensayo con cámaras corporales de doce meses de duración en Rialto (Estados Unidos), para determinar si el uso de este tipo de cámaras favorecería un comportamiento socialmente aconsejable entre los agentes que las llevaran. Los resultados demuestran que, durante el período de prueba y en comparación con 2011, el uso de la fuerza bajó de 60 a 25 casos, y las reclamaciones contra la policía se redujeron de 28 a 3.

Para más información, véase Farrar, T. (2018).

Figura 11: Herramienta en línea que muestra datos de las actuaciones de identificación y registro realizadas en Londres



Fuente: Reino Unido, Home Office, página web del mapa de identificación y registro.



Fuente: Reino Unido, Home Office, página web sobre registros específicos.

Sin embargo, el uso de cámaras corporales por parte de la policía suscita algunas inquietudes importantes en relación con los derechos fundamentales y las operaciones. Hacen falta garantías y políticas claras en relación con su empleo, a fin de abordar los siguientes problemas:

- No está claro **qué importancia tienen las cámaras corporales para detectar y prevenir la elaboración ilícita de perfiles**. Las cámaras capturan incidentes individuales y no permiten recoger datos estadísticos que pudieran utilizarse para determinar si las operaciones de identificación y registro son discriminatorias. Más bien sirven para revisar y analizar encuentros individuales y contribuir a mejorar su calidad.

- El uso de cámaras corporales podría tener efectos **negativos en las relaciones con las comunidades minoritarias**, si creen que se actúa específicamente contra ellas. Establecer garantías y políticas en consultas con las comunidades locales puede ayudar a promover el uso de cámaras corporales como herramienta para mejorar la rendición de cuentas y no como medio de estigmatizar a grupos minoritarios.

- El uso de cámaras corporales tiene **consecuencias para los derechos a la intimidad y la protección de datos**, así como para otros derechos humanos fundamentales. Por ejemplo, podrían afectar a la libertad de reunión pacífica si se utilizasen para vigilar manifestaciones públicas. A menudo no está claro cuando deberían encenderse y apagarse las cámaras, y qué ocurre si un agente olvida o decide no conectar la cámara: hacen falta directrices claras en este sentido. Las empresas privadas que presten este servicio deben tener claro que no pueden utilizar las imágenes para sus propios fines. El uso de cámaras corporales debe estar regulado por ley, para garantizar que se cumplan los derechos fundamentales.

Análisis del uso eficaz de las cámaras corporales

Cumplir tres principios importantes puede contribuir a garantizar que las cámaras corporales se utilicen eficazmente:

- **Autenticidad**: las imágenes deben estar claramente vinculadas al incidente. Deben registrarse la fecha y la hora (p. ej. mediante una marca de tiempo) y la localización exacta (p. ej. mediante GPS) del incidente.
- **Fiabilidad**: las imágenes deben cargarse en un sistema central mediante un procedimiento riguroso, seguro y confidencial. Estas imágenes deben cumplir los principios de protección de datos y respeto de la vida privada y, por tanto, no deben conservarse durante un período de tiempo superior al especificado por la ley.
- **Admisibilidad**: para que sean útiles en procesos penales, las imágenes deben ser admisibles ante los órganos jurisdiccionales. Para ello puede ser necesario:
  - Evitar grabar vídeo de forma continua, que constituye una injerencia inadmisible en el derecho a la intimidad de los policías y de las personas filmadas.
  - Informar a las personas afectadas de que pueden ser filmadas y obtener su consentimiento (cuando sea necesario).
  - Conservar las imágenes con un nivel de seguridad adecuado, y llevar un control del acceso a las imágenes tanto por los policías como por los ciudadanos.

Para más información, véase Coudert et al. *(2015), p. 8.*

Los avances tecnológicos obligarán a establecer nuevas garantías para asegurar que las cámaras corporales se utilicen de forma lícita. Por ejemplo, las cámaras capaces de reconocer automáticamente la cara de una persona comparándola con entradas anteriores en una base de datos generan nuevos problemas en relación con los derechos a la intimidad y la protección de datos.

Caso práctico

Uso de cámaras corporales por la policía: tarjeta de resultados (Estados Unidos)

Para aumentar la transparencia y la rendición de cuentas de las cámaras corporales, las organizaciones estadounidenses Leadership Conference on Civil and Human Rights y Upturn desarrollaron una herramienta para evaluar y estructurar la información que se puede extraer de las imágenes filmadas con estas cámaras.

La herramienta propone ocho criterios de evaluación:

1. Si las imágenes se hacen públicas y el departamento de policía tiene fácil acceso a las mismas.

2. Si se explica claramente la discrecionalidad de los agentes respecto de cuándo grabar.

3. Si se resuelven las dudas relativas a la intimidad.

4. Si los agentes deben revisar las imágenes antes de redactar su informe inicial.

5. Si las imágenes no marcadas deben eliminarse en un período predeterminado.

6. Si las imágenes están protegidas contra manipulaciones y usos indebidos.

7. Si las imágenes se facilitan a personas que presenten reclamaciones.

8. Si el uso de tecnologías biométricas para identificar a las personas que aparecen en las imágenes está limitado o no.

Este tipo de iniciativas pueden contribuir a reforzar la rendición de cuentas porque establecen normas y fomentan la implantación de mecanismos para determinar si las imágenes se obtienen y se utilizan debidamente.

Para más información, véase el sitio web de Leadership Conference on Civil and Human Rights y Upturn sobre la tarjeta de resultados.

2.3.3. Mecanismos de reclamación

Unos mecanismos de reclamación efectivos pueden tener efectos disuasorios en relación con los abusos de poder y ayudar a inspirar y restablecer la confianza de los ciudadanos en las operaciones de las autoridades policiales y de gestión de fronteras. Suelen ser complementarios a los canales legales formales que permiten a las personas impugnar la actuación o decisión de una autoridad pública ante un tribunal independiente e imparcial.

Para que sean eficaces, es esencial que:

- **Los ciudadanos puedan acceder fácilmente a los mecanismos de reclamación**: la experiencia demuestra sistemáticamente que los ciudadanos son reacios a presentar reclamaciones, por ejemplo porque el proceso es largo o costoso, o porque temen repercusiones negativas. Si los mecanismos de reclamación son fácilmente accesibles a través de plataformas en línea, como sitios web o *apps*, los ciudadanos pueden animarse a utilizarlos. Además, las organizaciones pueden ayudar a los ciudadanos a presentar reclamaciones, ya sea haciéndolo en su nombre o mediante mecanismos de recurso colectivo, como está previsto en el artículo 80, apartado 2, del RGPD.

- **Las reclamaciones se tramiten de forma transparente**: esto contribuye a incrementar la confianza en estos mecanismos.

- **Los órganos de reclamación sean independientes** de la organización, o de la parte de la organización contra la que se reclama.

Existen mecanismos muy diversos que tramitan diferentes tipos de reclamaciones. La figura 12 brinda una visión general de algunos de los mecanismos de reclamación disponibles en los Estados miembros y a escala de la UE.

Figura 12: Visión general de los mecanismos de reclamación de los Estados miembros

Fuente: *FRA, 2018.*

Los mecanismos que ofrecen a los policías la posibilidad de dialogar con los ciudadanos para escuchar sus quejas, analizar el uso de perfiles y obtener reacciones acerca de sus operaciones ofrecen una oportunidad de extraer lecciones importantes para mejorar los procesos que regulan la elaboración de perfiles. También crean el medio para involucrar a los ciudadanos en las actividades de los cuerpos y fuerzas de seguridad (véase el caso práctico).

Caso práctico

Mecanismos de reclamación públicos en el sector de los cuerpos y fuerzas de seguridad

Paneles de escrutinio público (West Midlands Police — Reino Unido)

Cada uno de los ocho distritos policiales (Boroughs) de la West Midlands Police (WMP) celebra una reunión bimestral del panel de escrutinio de operaciones de identificación y registro, presidido por representantes de la ciudadanía. Estos paneles examinan los expedientes de identificación y registro, velan por que la WMP respete la ley, y ofrecen a las comunidades un canal para comunicar sus quejas y plantear sus inquietudes. El orden del día y las actas de las reuniones se publican en internet. La WMP ha adoptado una serie de prácticas adicionales relativas a la participación de la comunidad con el afán de que las identificaciones callejeras sean más equitativas y estén mejor orientadas, y que los agentes sean más responsables.

Para más información, véase la página web de la West Midlands Police sobre identificación y registro y Her Majesty's Inspectorate of Constabulary (2016).

Paneles de motivos razonables (Northamptonshire Police — Reino Unido)

La Policía de Northamptonshire ha instaurado los «paneles de motivos razonables» cuya finalidad es ofrecer a los ciudadanos la posibilidad de contribuir a mejorar sus operaciones de identificación y registro. Estos paneles constituyen un canal de debate sobre el ejercicio de las facultades de identificación y registro y sus efectos sobre las comunidades. Están presididos por un inspector jefe e integrados por un agente de primera línea y dos miembros de la comunidad, entre los que pueden figurar delincuentes o exdelincuentes. Además de mejorar la comunicación entre la policía y los ciudadanos, este panel está investido de autoridad para destituir a agentes

y obligarlos a someterse a formación adicional con el fin de mejorar sus operaciones de identificación y registro.

Para más información, véase la página web de Northamptonshire Police sobre el panel y Open Society Justice Initiative (2018a).

Red informal de mecanismos de reclamaciones contra la policía

La Red de Autoridades Policiales Independientes sobre Denuncias (IPCAN) constituye una red informal consagrada al intercambio y la colaboración entre estructuras independientes encargadas del control externo de las fuerzas de seguridad. Se creó en 2013 y agrupa a autoridades competentes en materia de reclamaciones de 20 países. Estos organismos, pertenecientes fundamentalmente a los Estados miembros de la Unión, atienden y tramitan reclamaciones contra las fuerzas de seguridad públicas y, en ocasiones, contra las privadas.

Para más información sobre la IPCAN, visite su sitio web.

En la gestión de fronteras, se pueden establecer mecanismos para que los ciudadanos puedan presentar denuncias sobre el terreno o *ex post*. La posibilidad de acceder a estos mecanismos aumenta la transparencia y la rendición de cuentas, y fomenta el respeto mutuo y las buenas relaciones entre los guardias de fronteras y los ciudadanos. La opción de presentar una reclamación *ex post* a un órgano superior en lugar de (solo) directamente en el paso fronterizo genera un grado de supervisión y puede influir positivamente en la disposición de los viajeros a denunciar posibles incidentes ([36]).

Estudio de caso

Mecanismos públicos de reclamación en la gestión de fronteras

Mecanismo de reclamación interno en el aeropuerto de Manchester (Reino Unido)

En el aeropuerto de Manchester, el Central Allocation Hub es un punto central de contacto para todos los pasajeros que deseen presentar una denuncia. Las reclamaciones se pueden presentar por correo electrónico,

([36]) FRA (2014b).

por carta, por teléfono o por fax, o bien presencialmente, y en inglés o en galés. Las directrices de la Border Force (Fuerza de Fronteras) del Reino Unido presentan las posibles maneras de resolver las denuncias. Las faltas leves, como descortesía, brusquedad o mal comportamiento, normalmente se resuelven a nivel local. Ello pasa por clarificar los problemas con el cliente, explicando los procedimientos operativos, acordando actuaciones adicionales y ofreciendo una disculpa si procede. Las denuncias sobre faltas graves se asignan por lo general a la Professional Standards Unit. Las directrices de la Border Force incluyen una prueba para determinar indicios de posible discriminación, que constituiría una falta grave. Si existen pruebas iniciales sólidas de que el trato dispensado a un viajero obedece a ajenos a la raza, el caso se remite por lo general a una resolución en el ámbito local.

Para más información, véase FRA (2014a), p. 74.

Mecanismo de reclamaciones individuales de Frontex (UE)

Tras la adopción del nuevo Reglamento de la Agencia Europea de la Guardia de Fronteras y Costas (Frontex) en 2016, Frontex creó un mecanismo de reclamaciones individuales con el fin de vigilar el respeto de los derechos fundamentales en las actividades de la Agencia, que incluyen proyectos piloto, operaciones de retorno, operaciones conjuntas, intervenciones rápidas en frontera, despliegue de equipos de apoyo a la gestión de las migraciones e intervenciones de retorno. Cualquier persona cuyos derechos se hayan visto directamente afectados por las actuaciones del personal que participe en dichas actividades de Frontex —incluido el perteneciente a autoridades públicas nacionales— puede presentar una denuncia al agente de derechos fundamentales de Frontex, que es quien decide si es admisible y la envía al director ejecutivo, así como a las autoridades del Estado miembro afectado, si en la presunta violación ha participado personal nacional. La reclamación se puede presentar en cualquier lengua, por correo electrónico, por carta o a través de un formulario de denuncia en línea, disponible en el sitio web de Frontex: http://frontex.europa.eu/complaints/.

Centrarse en los derechos de los agentes de policía

Los policías gozan de los mismos derechos y libertades que otras personas, y están protegidos por las normas de derechos humanos en el desempeño de sus funciones. Pueden remitirse a sus derechos tal como figuran en diversos

documentos internacionales sobre derechos humanos internacionales, como el Convenio Europeo de Derechos Humanos (CEDH) o el Pacto Internacional de Derechos Civiles y Políticos (PIDCP). El Código Europeo de Ética de la Policía especifica que «[e]l personal de la policía debe beneficiarse, por regla general, de los mismos derechos civiles y políticos que los demás ciudadanos. Solo caben restricciones a estos derechos cuando son necesarias para el ejercicio de las funciones de la policía en una sociedad democrática, de conformidad con la ley y con el Convenio Europeo de Derechos Humanos». Una excepción es el artículo 11 del CEDH, relativo al derecho de libertad de reunión y asociación.

En el desempeño de sus funciones, especialmente cuando ejerce facultades policiales, un agente de policía no actúa como ciudadano particular, sino como órgano del Estado. Por lo tanto, la obligación del Estado de respetar y proteger los derechos humanos afecta directamente a las opciones de que dispone un policía para responder a una agresión. Los derechos de los oficiales de policía, que pueden sufrir lesiones o la muerte en el desempeño de sus funciones, también deben ser respetados y protegidos, por ejemplo facilitándoles equipo de protección, planificando cuidadosamente las operaciones policiales o adoptando medidas preventivas. Podría revelarse necesario limitar los derechos que les asisten en el desempeño de sus funciones, pero estas limitaciones deben reflejar el principio de proporcionalidad. Dada la particularidad de su labor en tanto que órgano del Estado, un policía puede enfrentarse a una limitación de sus derechos mayor que la de un «ciudadano ordinario». Si tomamos el ejemplo de una manifestación que se vuelve violenta, un «ciudadano ordinario» podría huir o pedir ayuda, mientras que un agente de policía está obligado a proteger los derechos humanos de los demás y a restaurar el orden público.

Para más información, véase FRA (2013).

3 Elaboración algorítmica de perfiles

La elaboración algorítmica de perfiles incluye técnicas informáticas paso a paso que analizan datos con el fin de detectar tendencias, patrones o correlaciones ([37]). Mediante la elaboración de perfiles, la persona es seleccionada «en virtud de sus relaciones con otras personas, identificadas por el algoritmo, en lugar de por su comportamiento real» y «las decisiones de las personas se estructuran de acuerdo con la información disponible acerca del grupo», en lugar de por sus propias decisiones personales ([38]).

La elaboración algorítmica de perfiles puede ser un procedimiento eficaz para que las organizaciones policiales y responsables de la gestión de fronteras utilicen datos con el fin de prevenir, detectar e investigar delitos. No obstante, la recogida y el tratamiento de grandes conjuntos de datos suscitan una serie de inquietudes por lo que se refiere a los derechos fundamentales. Además de la importancia de evitar la discriminación, la elaboración algorítmica de perfiles introduce nuevos riesgos, especialmente en relación con los derechos a la intimidad y la protección de datos. Este capítulo se centra en primer lugar en estos nuevos riesgos. A continuación, ilustra los retos en materia de derechos fundamentales asociados con el uso de la elaboración algorítmica de perfiles en bases de datos de gran escala con fines de seguridad y gestión de fronteras, e indica algunas maneras de minimizar dichos riesgos.

([37]) Para más información sobre algoritmos, véase FRA (2018b), p. 4.

([38]) Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S. y Floridi, L. (2016).

Centrarse en la policía predictiva

Las autoridades policiales utilizan varias aplicaciones de *software* para predecir cuándo y dónde se cometerá un delito. Algunos ejemplos son: PredPol en el Reino Unido y Estados Unidos, Criminality Awareness System (CAS) en los Países Bajos, y Precobs en Alemania y Suiza. Sin embargo, la eficacia de estos modelos predictivos para la prevención de la delincuencia todavía no ha sido objeto de una evaluación adecuada. Las pruebas obtenidas hasta la fecha revelan resultados contradictorios, como se observa en los ejemplos siguientes.

Prueba de campo de policía predictiva en Kent (Reino Unido) y Los Ángeles (Estados Unidos)

La policía del Reino Unido y de Estados Unidos llevó a cabo un experimento para comparar —con respecto a un enfoque más tradicional— un algoritmo totalmente automatizado para la detección de zonas críticas en materia de delincuencia y la consiguiente planificación de patrullas policiales.

Las conclusiones demuestran que el algoritmo automatizado obtuvo mejores resultados en la detección de futuros delitos. Predijo un porcentaje de 1,4 y 2,2 veces mayor de actuaciones delictivas que un analista criminal utilizando prácticas de inteligencia criminal y mapas de delincuencia tradicionales. Además, las patrullas basadas en la herramienta predictiva son más eficaces, con una reducción media del 7,4 % en el número de delitos.

Para más información, véase Mohler, G. O. et al. *(2016).*

Programa PILOT (Predictive Intelligence Led Operational Targeting) en Shreveport (Estados Unidos)

Este programa utiliza un modelo predictivo para detectar pequeñas zonas que presentan un mayor riesgo de delitos contra la propiedad y para aplicar un modelo de intervención en dichas zonas con el fin de prevenir dichos delitos contra la propiedad. Se compararon los resultados de tres distritos que aplicaron el programa PILOT con otros tres en los que se desarrolló la labor policial tradicional. No hubo pruebas estadísticas de una mayor reducción de los delitos contra la propiedad en los tres distritos PILOT examinados.

Para más información, véase Hunt, P. et al. *(2014).*

***Software* Beware (Estados Unidos)**

«Beware» permite a los agentes contestar llamadas de emergencia codificadas por colores (rojo, amarillo y verde), que indican el nivel de amenaza de la persona o localización afectada. Este *software* efectúa búsquedas en bases de datos, en particular informes sobre detenciones, registros de la propiedad, bases de datos comerciales, búsquedas de internet en profundidad, publicaciones en redes sociales y otras bases de datos de acceso público.

No se han evaluado ni las fortalezas ni las debilidades de este sistema. Sin embargo, la falta de supervisión del proceso decisorio y el carácter reservado del algoritmo, protegido por secretos comerciales, han generado dudas por lo que a la rendición de cuentas se refiere. Además, la posible inexactitud de los datos recogidos o de la información deducida del análisis puede reducir la eficacia general de la herramienta.

Para más información, véase American Civil Liberties Union (2016).

Caso práctico

Evaluación de repercusiones y riesgos de la actuación policial predictiva: la herramienta de evaluación ALGO-CARE

Deben tenerse en cuenta los posibles efectos negativos del uso de la policía predictiva para obtener una perspectiva equilibrada y transparente de sus repercusiones sobre la sociedad. Un análisis realizado por un grupo integrado por académicos y agentes de policía concluyó que, dado que la policía predictiva todavía se encuentra en fase experimental en el Reino Unido, era necesario examinar con detalle sus repercusiones sobre la sociedad y las personas físicas. El estudio sostiene que algunas decisiones podrían repercutir excesivamente en la sociedad y en las personas físicas como para que influya en ellas una tecnología emergente; estos casos deberían sustraerse de la influencia del proceso de decisión algorítmico.

El grupo elaboró un marco de decisión denominado ALGO-CARE para desplegar herramientas de evaluación algorítmica en el contexto de la labor policial. Este marco tiene por objeto orientar a los agentes de policía a la

hora de evaluar los posibles riesgos de utilizar la policía predictiva. También intenta traducir principios clave de Derecho público y derechos humanos en consideraciones prácticas y orientaciones que puedan ser analizadas por organismos públicos.

La herramienta de evaluación invita a los policías a examinar el uso de la policía predictiva a través de ocho pasos complementarios:

- **Asesoramiento**: examinar el alcance de la intervención humana.
- **Licitud**: examinar la justificación legal para utilizar el algoritmo.
- **Granularidad**: examinar si el algoritmo puede entrar en un grado de detalle suficiente en un caso concreto.
- **Titularidad**: asegurar que el cuerpo de policía dispone de la titularidad legal y la capacidad técnica para acceder, mantener, actualizar y corregir el código fuente regularmente.
- **Impugnabilidad**: asegurar que están en vigor mecanismos de supervisión y auditoría.
- **Exactitud:** examinar si el algoritmo es adecuado para los fines del trabajo policial, si puede ser validado periódicamente y si la probabilidad y los efectos de su inexactitud representan un riesgo aceptable.
- **Responsabilidad:** examinar la equidad, rendición de cuentas y transparencia del algoritmo.
- **Explicabilidad:** examinar la accesibilidad de la información en relación con las normas de decisión y el efecto de cada factor sobre el resultado final.

Para más información, véase Oswald, M. et al. *(2017).*

3.1. El marco de protección de datos por el que se rige la elaboración algorítmica de perfiles

El desarrollo e incremento en el uso de nuevas tecnologías —incluido el creciente uso de grandes conjuntos de datos para facilitar la toma de decisiones— llevó a la UE a efectuar una amplia revisión de su normativa sobre tratamiento de datos personales en 2016. Los dos nuevos instrumentos —el Reglamento General de Protección de Datos (RGPD) y la Directiva sobre la policía— establecen principios y normas importantes que se aplican a cualquier decisión basada en procesos informatizados, incluida la elaboración algorítmica de perfiles.

El RGPD y la Directiva sobre la policía entraron en vigor en mayo de 2018, por lo que en el momento de redactarse la presente guía se dispone de pocos ejemplos prácticos de la aplicación. El apartado 1.2.2 describe las normas jurídicas que regulan los derechos a la intimidad y la protección de datos, y explica algunas de las diferencias principales entre el RGPD y la Directiva sobre la policía (véase el cuadro 2). Este capítulo se basa en dicha información para describir y explicar los requisitos legales en materia de elaboración algorítmica de perfiles establecidos por el RGPD y la Directiva sobre la policía. Dichos requisitos incluyen:

- Los datos deben ser tratados con un fin específico, con una base jurídica específica.
- Es obligatorio informar a las personas físicas cuando se vayan a tratar sus datos personales.
- Los datos deben conservarse de manera segura.
- Es preciso detectar y prevenir el tratamiento ilícito de datos.

Los policías y los guardias de fronteras que necesiten información adicional sobre los requisitos legales descritos en el presente capítulo deberán consultar con el delegado de protección de datos de su organización. Además, el *Manual sobre la legislación europea de protección de datos* elaborado por la FRA, el SEPD y el Consejo de Europa ofrece orientaciones adicionales sobre la aplicación de la Directiva sobre la policía y el RGPD ([39]).

([39]) FRA, SEPD y Consejo de Europa (2018).

Puntos clave

- La elaboración algorítmica de perfiles debe ser **legítima**, **necesaria** y **proporcionada.**
- Los datos no deben tratarse sin un **fin específico con una base jurídica específica.**
- Las personas físicas tienen derechos específicos descritos en detalle en las disposiciones del RGPD y en la Directiva sobre la policía, que incluyen:
  - **el derecho a ser informadas,** que incluye recibir información significativa sobre la lógica aplicada en el algoritmo,
  - el derecho **de acceso a sus datos personales,**
  - el derecho **a presentar una reclamación** ante una autoridad de control, y
  - derecho a la **tutela judicial efectiva.**
- Los datos se deben recoger, tratar y conservar **de manera segura**.
- Se debe **prevenir** y **detectar** el tratamiento ilícito de datos.

3.1.1. Los datos deben tratarse con un fin específico

Todo tratamiento de datos personales debe tener una base jurídica. Esto significa que debe llevarse a cabo para alcanzar **un fin específico** estipulado por ley.

Antes de llevar a cabo cualquier tratamiento, un agente debe conocer sus fines. Pueden tratarse, entre otros, de los siguientes:

- ¿Tiene por objeto el tratamiento de datos detectar una infracción penal?
- ¿Tiene por objeto el tratamiento mantener la seguridad pública?
- ¿Tiene por objeto el tratamiento combatir el terrorismo?

Una vez establecida correctamente la finalidad, los agentes sabrán cuál es el marco jurídico aplicable y las consiguientes obligaciones legales. El cuadro 4 explica cómo determinar cuál es el marco jurídico aplicable.

Cuadro 4: Determinación del marco jurídico correcto en función de la finalidad del tratamiento

1. ¿Cuál es la finalidad del tratamiento?

- prevención, investigación, detección o enjuiciamiento de infracciones penales;
- ejecución de sanciones penales;
- protección de la seguridad pública.

- cualquier otro fin

↓

2. Se aplica la Directiva sobre la policía

↓

3. El Derecho nacional o de la Unión define (*)

- qué datos personales pueden ser tratados;
- los fines específicos del tratamiento de datos.

↓

2. Se aplica el Reglamento General de Protección de Datos

↓

3. El tratamiento solo se permite cuando es:

- **autorizado** por el interesado;
- necesario para la ejecución de un **contrato**;
- necesario para cumplir con **obligaciones legales**;
- necesario para proteger los **intereses vitales** de una persona; o
- necesario para el **interés público**.

↓

4. ¿Están los fines de la elaboración de perfiles exentos de la Directiva sobre la policía?	4. ¿Están los fines de la elaboración de perfiles exentos del RGPD?
El derecho a la información, el derecho de acceso a los datos personales, y el derecho a solicitar la modificación o supresión de los datos pueden estar limitados (total o parcialmente) en los siguientes casos: • para evitar la obstrucción de **pesquisas**, investigaciones o procedimientos oficiales o legales; • para evitar que se perjudique la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales; • para proteger la seguridad pública; • para proteger la seguridad nacional; • para proteger los derechos y libertades de otras personas.	Las obligaciones (de transparencia, información y notificación de infracciones) y los derechos (de acceso, rectificación, supresión, oposición o no sometimiento a decisiones automatizadas) recogidos en el RGPD **pueden estar limitados** por el Derecho nacional o de la Unión con el fin de proteger: • la seguridad, defensa o seguridad pública nacionales; • la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, en particular la protección y la prevención de las amenazas para la seguridad pública; • otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, en particular en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; • la protección de la independencia judicial y de los procedimientos judiciales; • la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; • una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en casos específicos; • la protección del interesado o de los derechos y libertades de los demás; • la ejecución de demandas civiles.

Nota: *(*) Las legislaciones nacionales por las que se transpone la Directiva sobre la policía están disponibles en el sitio web de Eur-Lex.*

Fuente: *FRA, 2018.*

3.1.2. Las personas físicas deben ser informadas

El artículo 13 de la Directiva sobre la policía y los artículos 13 y 14 del RGPD obligan a informar a las personas físicas cuando se proceda al tratamiento de sus datos personales. El cuadro 5 describe cómo y cuándo comunicar información a la persona cuyos datos son objeto de tratamiento.

Cuadro 5: Obligación de facilitar a las personas físicas información sobre elaboración de perfiles: tipos de datos, medios de comunicación y excepciones

Obligación de notificación: lista de control	
¿A quién?	Persona cuyos datos son objeto de tratamiento
¿Cómo?	• lenguaje claro y sencillo • formato fácilmente accesible • en el mismo formato que la petición, *preferiblemente por medios electrónicos*
¿Qué?	**Acerca del tratamiento**: • el nombre y los datos de contacto de su autoridad • los datos de contacto de su delegado de protección de datos • los fines del tratamiento • la base jurídica para el tratamiento • el plazo máximo de conservación de los datos • los tipos de personas/organizaciones que recibirán los datos **Acerca de los derechos de las personas físicas:** • el derecho a **presentar una reclamación** ante una autoridad de control y los datos de contacto de la misma • el derecho a solicitar **acceso** a sus datos personales • **rectificación** o **supresión** de datos personales • el derecho a solicitar la **limitación** del tratamiento
Excepciones	• Por peticiones excesivas (es decir, repetitivas) o manifiestamente infundadas • Cuando no se puede confirmar con claridad la identidad del solicitante • Cuando comunicar información supondría una obstrucción a las investigaciones • Cuando la comunicación de información perjudicaría la prevención/investigación de infracciones penales • Para proteger la seguridad pública o nacional • Para proteger los derechos de otras personas físicas

Fuente: *FRA, 2018.*

Análisis del «derecho a la explicación»

En los casos de elaboración de perfiles, el RGPD obliga a facilitar a la persona física «información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas» del tratamiento de datos. Esta información debe facilitarse tanto en el momento de recoger los datos (notificación) como en el caso de que el interesado solicite información adicional (derecho de acceso). Este derecho no está mencionado expresamente en la Directiva sobre la policía. Sin embargo, el considerando 38 especifica que «[el tratamiento automatizado] debe estar sujeto a las garantías apropiadas, lo que incluye informar de manera específica al interesado [...], en particular para que [...] pueda [...] obtener una explicación de la decisión adoptada tras dicha evaluación, o ejercer su derecho a impugnar la decisión».

Este «derecho a la explicación» puede resultar difícil de aplicar en la práctica. Algunas personas pueden tener los conocimientos digitales necesarios para comprender el código de un algoritmo, mientras que para otras basta recibir información simplificada sobre la finalidad del tratamiento y las interconexiones de los datos utilizados. La clave para evaluar si la explicación facilitada es significativa es su objetivo. Una persona debe recibir información suficiente para entender la finalidad, la justificación y los criterios que llevaron a tomar una decisión.

El derecho a una explicación no es absoluto (véase el paso 4 del cuadro 4). Los Estados miembros pueden limitar este derecho por ley en varios casos, en particular por razones de seguridad nacional; defensa; seguridad pública; prevención, investigación, detección o enjuiciamiento de infracciones penales; ejecución de sanciones penales, protección del interesado o de los derechos y libertades de otros; o ejecución de demandas civiles.

No obstante, facilitar información razonable sobre la finalidad y las consecuencias previstas del tratamiento constituye una buena práctica aconsejable. La adopción de procedimientos sencillos para explicar la lógica aplicada y los criterios utilizados para adoptar una decisión servirá en última instancia para mejorar la transparencia y la rendición de cuentas.

Para más información, véase el RGPD, artículos 13 a 15 (derecho a la información y derecho de acceso), artículo 22 (decisiones individuales

automatizadas, incluida la elaboración de perfiles), y el artículo 23 (limitaciones); y la Directiva sobre la policía, artículo 11 (mecanismo de decisión individual automatizado, incluida la elaboración de perfiles) y los artículos 13 a 15 (derecho a la información y derecho de acceso).

Véase también Grupo de Trabajo del Artículo 29 (2018a).

3.1.3. Mantener los datos seguros: expedientes, registros «log» y normas de conservación

Las autoridades responsables de la recogida y el tratamiento de datos personales con fines de elaboración de perfiles no solo deben tratar los datos de manera lícita, sino también velar por que los datos no sean:

- accesibles por parte de personas no autorizadas,
- utilizados para fines distintos del fin original, ni
- conservados durante más tiempo del necesario.

A este fin, las autoridades y los agentes de policía y de gestión de fronteras deben velar por que se apliquen medidas adecuadas para proteger la integridad y la seguridad de los datos. Deben controlar todo acceso, y uso de los datos, mediante la creación y el mantenimiento de registros de todas las actividades de tratamiento o categorías de actividades de tratamiento (artículo 30 del RGPD y artículo 24 de la Directiva sobre la policía). Estos registros deben contener:

- el **nombre** y los **datos de contacto** de las autoridades y del delegado de protección de datos;
- los **fines** del tratamiento;
- las **categorías de destinatarios** a quienes se comunicaron o se comunicarán los datos personales;
- una descripción de las categorías de interesados y de las categorías de datos personales;

- el **uso de la elaboración de perfiles**;
- una indicación de la **base jurídica** para la operación de tratamiento;
- cuando sea posible, los **plazos** previstos para suprimir las diferentes categorías de datos personales;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refieren el artículo 32, apartado 1, del RGPD o el artículo 29, apartado 1, de la Directiva sobre la policía.

Además, cuando se implemente la elaboración de perfiles informatizada para los fines comprendidos en la Directiva sobre la policía (véase la sección 3.2), las autoridades deberán conservar registros (archivos «log») de las operaciones de recogida, modificación, consulta, divulgación (incluidas transferencias), combinación y supresión de datos.

Estos expedientes y registros ayudarán a los agentes a demostrar que cumplen los requisitos legales durante los controles internos y externos. Por ejemplo, si una persona presenta una reclamación, las autoridades policiales y las autoridades responsables de la gestión de fronteras deberán poner estos expedientes y registros a disposición de las autoridades nacionales encargadas de la protección de datos.

Los datos personales no deben conservarse durante más tiempo del necesario para alcanzar el fin legítimo establecido. Si se conservan durante períodos más largos, deberá justificarse debidamente. En estos casos, las autoridades deberán asegurarse de revisar periódicamente dicha conservación para garantizar su integridad y seguridad.

3.1.4. Es preciso detectar y prevenir el tratamiento ilícito de datos

Es difícil detectar y prevenir el tratamiento ilícito de datos personales. Los conocimientos especializados necesarios para entender algoritmos complejos y grandes bases de datos hacen que sea difícil realizar controles adecuados.

Para resolver este problema, el RGPD y la Directiva sobre la policía incluyen garantías con el fin de orientar a los agentes de policía y de gestión de fronteras antes, durante y después del tratamiento de los datos. Se refieren a:

- evaluaciones de impacto relativas a la protección de datos; y
- protección de los datos desde el diseño y por defecto.

Evaluaciones de impacto

El marco jurídico de la UE obliga a las autoridades policiales y a las autoridades responsables de la gestión de fronteras a realizar evaluaciones de impacto antes de llevar a cabo cualquier tratamiento de datos que pueda entrañar un riesgo elevado para los derechos de las personas físicas (artículo 35 del RGPD y artículo 27 de la Directiva sobre la policía). Esto significa que las evaluaciones de impacto no solo deberán realizarse cuando el resultado del tratamiento pueda violar las normas de protección de datos o la intimidad, sino en cualquier situación que pueda derivar en una violación de *cualquier derecho fundamental*, como pueden ser los derechos a la igualdad y a la no discriminación, a la libertad de expresión e información, a la libertad de pensamiento, de conciencia y de religión, a la educación, a la sanidad, al asilo, y a la protección en caso de devolución, expulsión o extradición. Las evaluaciones de impacto son especialmente importantes si la elaboración de perfiles puede acarrear consecuencias jurídicas para las personas físicas. En estos casos, el RGPD y la Directiva sobre la policía obligan a realizar evaluaciones de impacto.

Las evaluaciones de impacto deben realizarse antes del propio tratamiento automatizado, y su objetivo es doble:

- *a priori*: antes del tratamiento de los datos, una evaluación de impacto relativa a la calidad de los datos o del algoritmo de tratamiento contribuye a detectar y, llegado el caso, a remediar posibles violaciones de los derechos fundamentales;
- *a posteriori*: una vez tratados los datos, el agente puede verse en la obligación de demostrar que ha actuado de manera lícita. La evaluación de impacto puede ayudarle a demostrar que se han adoptado todas las medidas necesarias para garantizar el cumplimiento de la ley.

Las evaluaciones de impacto también ayudarán a los agentes a detectar sesgos ocultos que puedan violar los derechos a la protección de datos y a la no discriminación, y que puedan afectar a la calidad de la elaboración de perfiles (véase el apartado 1.3.2).

Análisis de los riesgos que entraña el uso de «algoritmos dinámicos»

Los «algoritmos dinámicos» son algoritmos que se redefinen y «mejoran» constantemente basados en «bucles de realimentación». Estos bucles son creados por los propios sistemas algorítmicos y no pueden entenderse correctamente ni tampoco expresarse en un lenguaje sencillo (véase el artículo 35 del RGPD y el artículo 27 de la Directiva sobre la policía). A diferencia de los «algoritmos estáticos», que se basan en criterios predeterminados, los «algoritmos dinámicos» generan **nuevas correlaciones** al redefinirse constantemente.

Los algoritmos dinámicos crean el riesgo de que unos programadores expertos ya no conozcan, en un momento determinado, la lógica del algoritmo. Esto genera un importante **riesgo de que se reproduzcan involuntariamente prejuicios existentes** y se perpetúen las desigualdades sociales y la estigmatización de determinados grupos. En estos casos, resulta muy difícil garantizar la rendición de cuentas y la compensación para las personas afectadas.

Por tanto, debe **evitarse o reducirse** el uso de «algoritmos dinámicos» para minimizar el riesgo de que se pierdan de vista los criterios de evaluación. De este modo, los auditores internos y externos pueden evaluar los algoritmos y modificarlos si observan que no son lícitos. Si se justifica el uso de algoritmos dinámicos, se revisarán y probarán los indicadores de riesgo a fin de comprobar que no resultan en que la elaboración de perfiles sea ilícita.

Para más información, véase Gandy, O. (2010) y Korff, D. (2015).

Una evaluación de impacto puede variar significativamente en función del tipo y el volumen de los datos personales tratados, y del tipo y la finalidad del tratamiento. Puede incluir una verificación de la calidad de los datos, controles técnicos de los algoritmos de tratamiento, o una revisión completa de los objetivos del tratamiento, etc. La figura 13 establece los criterios mínimos que deben evaluarse.

Figura 13: Requisitos mínimos de las evaluaciones de impacto

Fuente: *FRA, 2018.*

El Grupo de Trabajo del Artículo 29 (ahora reemplazado por el Comité Europeo de Protección de Datos), que agrupa a las autoridades nacionales de protección de datos de los Estados miembros, elaboró directrices que ofrecen información adicional sobre las evaluaciones de impacto relativas a la protección de datos. Estas directrices incluyen un mapa detallado de los criterios que deben aplicarse en las evaluaciones de impacto ([40]).

Integración de la licitud «desde el diseño» y «por defecto»

Con independencia de si una evaluación de impacto detecta o no la posibilidad de una violación de derechos fundamentales, se pueden aplicar medidas para evitar cualquier riesgo de ilegalidad. Esto es lo que se conoce como «protección de datos desde el diseño» y «protección de datos por defecto» (artículo 25 del RGPD y artículo 20 de la Directiva sobre la policía).

([40]) Grupo de Trabajo del Artículo 29 (2017a).

La protección de datos desde el diseño tiene por objeto garantizar que, *antes* y *durante* el tratamiento de los datos, se apliquen medidas técnicas y organizativas para garantizar los principios de protección de datos. Por ejemplo, cuando sea viable, los datos personales podrían «seudonimizarse». La seudonimización es una medida por la que no se pueden atribuir datos personales a una persona sin información adicional, que se conserva por separado.

La «clave» que permite reidentificar a los interesados debe conservarse por separado y de manera segura ([41]). Al contrario que los datos anonimizados, los datos seudonimizados siguen siendo datos personales y, por tanto, deben respetar las normas y los principios de protección de datos.

La protección de datos por defecto garantiza que «solo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento» ([42]). Esto afecta a:

- la cantidad de datos personales recogidos y conservados;
- los tipos de tratamiento que pueden afectar a datos personales;
- el plazo máximo de conservación;
- el número de personas con autorización de acceso a dichos datos personales.

Análisis de la rendición de cuentas

El objetivo principal de la protección de datos desde el diseño y de la protección de datos por defecto es ayudar a las autoridades y los agentes de policía y gestión de fronteras a diseñar programas de elaboración algorítmica de perfiles que cumplan los requisitos de derechos fundamentales, en particular los principios de **licitud**, **transparencia** y **seguridad**.

Sin embargo, este tipo de medidas también pueden demostrar cómo cumplen las autoridades con el requisito legal de **rendición de cuentas**. Las autoridades responsables del tratamiento de datos tienen la obligación legal de aplicar «medidas técnicas y organizativas» para demostrar que cumplen con la

([41]) FRA, SEPD y Consejo de Europa (2018), p. 83.

([42]) Reglamento General de Protección de Datos (RGPD), artículo 25.

legislación de la UE. Por ejemplo, si una persona presenta una reclamación, las autoridades judiciales y de protección de datos nacionales pueden solicitar a las autoridades que demuestren cada uno de estos puntos:

- La legitimidad, necesidad y proporcionalidad de la elaboración de perfiles informatizada.
- La licitud del fin perseguido.
- La información facilitada a los interesados.
- La integridad y seguridad de los datos.
- Las medidas y los controles de calidad aplicados antes y durante las operaciones de elaboración de perfiles.

3.2. Bases de datos a gran escala para los fines de la gestión de las fronteras y la seguridad

La UE ha desarrollado varios sistemas o mecanismos TI a gran escala para recoger y tratar datos que puedan utilizarse con fines de gestión de las fronteras y de la migración y, en cierta medida, con fines policiales. Son ejemplos ilustrativos de algunos de los retos comunes vinculados al uso de la elaboración algorítmica de perfiles, así como posibles garantías.

El cuadro 6 presenta brevemente estos sistemas y mecanismos TI de la UE. El anexo recoge una lista detallada de los sistemas TI a gran escala actuales y previstos en la UE, a fecha de marzo de 2018.

Cuadro 6: Instrumentos de la UE que requieren el tratamiento de grandes cantidades de datos con fines de gestión de fronteras y acción policial

Base de datos	Abreviatura	Finalidad principal
Sistema de Información de Schengen de segunda generación	*SIS II*	Introducir y procesar alertas sobre personas buscadas o desaparecidas con el fin de proteger la seguridad, introducir y procesar alertas sobre nacionales de terceros países (NTP) con el fin de denegar la entrada o la estancia, e introducir y procesar alertas sobre NTP sujetas a una decisión de retorno.
Sistema de Información de Visados	*VIS*	Facilitar el intercambio de datos entre Estados miembros de Schengen sobre solicitudes de visados.
Dactiloscopio europeo	*Eurodac*	Determinar el Estado miembro responsable de examinar una solicitud de protección internacional y ayudar a controlar la inmigración y los movimientos secundarios irregulares.
Sistema de Entradas y Salidas	*SES*	Calcular y controlar la duración de la estancia autorizada de los NTP y localizar a quienes la sobrepasan.
Registro de nombres de los pasajeros	*PNR*	Recoger, tratar e intercambiar datos de pasajeros de vuelos de terceros países («vuelos extra-UE») (*). Estrictamente hablando, se utiliza únicamente con fines policiales.
Información Anticipada sobre los Pasajeros	*API*	Recoger y tratar datos de pasajeros de vuelos de terceros países («vuelos extra-UE») con fines de gestión de fronteras y acción policial.
Sistema Europeo de Información y Autorización de Viajes	*SEIAV*	Evaluar si un NTP exento de visado entraña un riesgo para la seguridad, la migración irregular o la salud pública.
Sistema Europeo de Información de Antecedentes Penales para nacionales de terceros países	*ECRIS-TCN*	Compartir información sobre condenas anteriores de NTP.

Nota: *(*) Además, el artículo 2 de la Directiva (UE) 2016/681 ofrece a los Estados miembros la opción de tratar datos de vuelos intra-UE.*

Fuente: *FRA, 2018.*

Los sistemas TI a gran escala de la UE se utilizan en distintos procesos relacionados con la migración, incluido el proceso de evaluación de riesgos previo a la llegada, el proceso de asilo, el proceso de solicitud de visados, durante las inspecciones en frontera, en el momento de expedir permisos de residencia, en las detenciones de migrantes en situación irregular, durante los procedimientos de retorno y para expedir prohibiciones de entrada. Los sistemas TI establecidos por la UE, incluidos los creados inicialmente con fines de asilo y gestión de la migración, también se utilizan cada vez más en el contexto de la seguridad interior, como en el caso de las inspecciones policiales y en la lucha contra la delincuencia grave y el terrorismo.

La mayoría de los sistemas creados al amparo del Derecho de la UE tratan de identificar a una persona específica buscando correspondencias de datos alfanuméricos o biométricos (actualmente, huellas dactilares) con información ya introducida en el sistema. Con algunas excepciones notables (véase «Análisis de la elaboración algorítmica de perfiles en los instrumentos de la UE»), los sistemas propiamente dichos no contienen ningún algoritmo que permita encajar a una persona con un perfil. No obstante, pueden utilizarse para generar estadísticas anonimizadas, por ejemplo sobre características que se consideren motivos protegidos, como el sexo o la edad (véase el apartado 1.2.1).

Estas estadísticas podrían utilizarse para crear perfiles de riesgo que se apliquen en futuras decisiones de gestión de fronteras o acción policial. Dentro del régimen general aplicable a la interoperabilidad de los sistemas TI de la UE, la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA) tendrá la responsabilidad de administrar el repositorio central para la presentación de informes y estadísticas. Este repositorio utilizará información de bases de datos de la UE ya existentes (Sistema de Entrada y Salida, SEIAV, Sistema de Información de Schengen y Sistema de Información de Visados) para generar estadísticas e informes analíticos para organismos de la UE y nacionales ([43]).

([43]) Comisión Europea (2017), *Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (fronteras y visados) y por el que se modifican la Decisión 2004/512/CE del Consejo, el Reglamento (CE) n.º 767/2008, la Decisión 2008/633/JAI del Consejo, el Reglamento (UE) 2016/399 y el Reglamento (UE) 2017/2226*, COM(2017) 793 final, Estrasburgo, 12 de diciembre de 2017; Comisión Europea (2017), *Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE (cooperación policial y judicial, asilo y migración)*, COM(2017) 794 final, Bruselas, 12 de diciembre de 2017.

Análisis de la elaboración algorítmica de perfiles en instrumentos de la UE

Algunos instrumentos de la UE ya existentes contemplan el uso de estadísticas derivadas de sus datos para generar perfiles de riesgo. Además de permitir la detección de sospechosos «conocidos», contienen una funcionalidad de elaboración algorítmica de perfiles que identifica a personas «desconocidas» que puedan ser de interés para las autoridades policiales y de gestión de fronteras.

El **Sistema Europeo de Información y Autorización de Viajes (SEIAV)** ([44]), adoptado en septiembre de 2018 pero que todavía no estaba operativo en el momento de finalizarse esta Guía, determinará si los nacionales de terceros países exentos de visado entrañan un riesgo para la migración irregular, la seguridad o la salud pública antes de otorgarles autorización para viajar. La información facilitada por los viajeros durante el proceso de solicitud se comparará automáticamente con las bases de datos pertinentes de la UE y de ámbito internacional, y con un conjunto de indicadores de riesgo («normas de detección») contenidos en el propio sistema SEIAV. Un algoritmo desarrollado por Frontex comparará el perfil individual del viajero (basado en indicadores como la edad, el sexo, la nacionalidad, el lugar de residencia, el nivel académico y la profesión) con estos indicadores de riesgo para determinar si la solicitud debe remitirse a revisión manual.

Los datos del Registro de Nombres de Pasajeros (PNR) son recogidos por transportistas aéreos a partir de la información facilitada por los pasajeros en los sistemas de reserva de vuelos, como fechas e itinerario de viaje, datos de contacto y de pago, información sobre equipajes, y otras «observaciones generales» como preferencias dietéticas. No existe ninguna base de datos central de la UE que recoja estos datos, pero la Directiva del PNR ([45]) obliga a los transportistas aéreos a facilitar los datos a las unidades nacionales de información sobre los pasajeros (UIP), que a continuación analizan la información con el fin de combatir el terrorismo y la delincuencia grave. Además de detectar los movimientos transfronterizos de personas conocidas, estos datos pueden

([44]) Comisión Europea (2018), *Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226*, artículo 33, apartado 5.

([45]) *Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave*, DO L 119 de 4.5.2016, artículo 6, apartado 4.

utilizarse para identificar amenazas todavía desconocidas tratando los datos de los pasajeros con arreglo a indicadores de riesgo específicos («criterios predeterminados»). Estos criterios son establecidos por las UIP y actualizados de acuerdo con los nuevos datos y patrones disponibles en el sistema.

3.2.1. Minimizar los riesgos para los derechos fundamentales del tratamiento de datos en bases de datos de gran escala

En la elaboración de perfiles (incluida la algorítmica), se utilizarán datos exhaustivos de viajeros como la nacionalidad, el sexo y la edad, a una escala que no era posible en el pasado. Aunque estos datos se anonimicen, su tratamiento no está exento de riesgos. El sesgo consciente o inconsciente en la selección de indicadores de riesgo, en el diseño de los algoritmos o en la interpretación de los resultados podría dar lugar a actuaciones operativas que podrían acarrear discriminación de ciertas categorías de personas ([46]).

En este apartado se analizan algunos de estos riesgos y se proponen algunas maneras de minimizarlos. Se basa en la publicación de la FRA *Twelve operational fundamental rights considerations for law enforcement when processing PNR data* (véase el caso práctico). Aunque formuladas en el contexto específico del tratamiento de datos del PNR, algunas de estas consideraciones son aplicables con carácter más general, y pueden considerarse garantías para mitigar los riesgos derivados de la elaboración algorítmica de perfiles.

Caso práctico

Directrices operativas de la FRA para establecer sistemas PNR nacionales

En 2014, a falta de legislación de la UE sobre el PNR, la Comisión Europea solicitó a la FRA que elaborase unas directrices prácticas relativas al tratamiento de los datos del PNR con fines policiales para aquellos Estados miembros que planeaban establecer sus propios sistemas PNR nacionales. Estas directrices se centraron en los derechos al respeto a la vida privada (artículo 7 de la Carta), la protección de los datos personales (artículo 8 de la Carta) y la no discriminación (artículo 21 de la Carta). Algunas de las garantías propuestas se introdujeron posteriormente en la Directiva PNR de la UE.

([46]) Para más información, véase FRA (2017e), y FRA (2018a).

Las doce consideraciones sobre derechos fundamentales para la acción policial en el tratamiento de datos del PNR son:

- Utilizar los datos del PNR únicamente para combatir el terrorismo y los delitos transnacionales graves.
- Limitar el acceso a la base de datos del PNR a una unidad especializada.
- No solicitar acceso directo a las bases de datos de las compañías aéreas.
- Eliminar los datos sensibles del PNR.
- Establecer garantías estrictas de seguridad y trazabilidad contra abusos.
- Reducir la probabilidad de falsos positivos.
- Ser transparentes con los pasajeros.
- Permitir el acceso de los interesados a sus datos del PNR y su rectificación.
- No permitir la identificación de los interesados ni la conservación de datos durante más tiempo del necesario.
- Transferir los datos extraídos del PNR únicamente a las autoridades públicas nacionales competentes.
- Transferir datos extraídos del PNR a terceros países únicamente en condiciones estrictas.
- Realizar una evaluación objetiva y transparente del sistema PNR.

Para más información, véase FRA (2014c).

El tratamiento de datos que revelen características protegidas debe ser necesario y proporcionado

Dada la naturaleza de la elaboración algorítmica de perfiles, el uso de características personales relacionadas con motivos protegidos entraña un riesgo de discriminación especialmente elevado ([47]). En el contexto de la UE, la legislación del SEIAV y del PNR prohíbe basar los indicadores de riesgo en criterios que conlleven un riesgo de discriminación elevado, como la raza, el origen étnico y las creencias religiosas. Sin

([47]) Supervisor Europeo de Protección de Datos (2018).

embargo, incluso en ausencia de estos datos, es posible establecer una marcada correlación entre otros tipos de datos y estas características, de modo que actúen efectivamente como indicadores de dichas características protegidas. Por ejemplo, la categoría de «observaciones generales» del PNR, que pueden contener las preferencias dietéticas de los viajeros, podría revelar ciertas creencias religiosas.

Una combinación específica de los datos utilizados por el algoritmo también puede situar a una categoría de personas en desventaja. Por ejemplo, puede ser desfavorable para ciertas personas por razón de su origen étnico o social o su pertenencia a una minoría nacional, que son características protegidas en virtud del artículo 21 de la Carta. Por ejemplo, si un perfil de riesgo del SEIAV relativo al riesgo de migración irregular se basa en la combinación de una determinada nacionalidad y un grupo profesional, puede ocurrir que se aplique a un grupo étnico o nacionalidad que, en un determinado país, trabaje normalmente en un determinado sector económico, como la construcción o la agricultura ([48]).

- El tratamiento de datos que revele características protegidas por el artículo 21 de la Carta debe limitarse a lo que sea estrictamente necesario y proporcionado, y nunca provocar discriminación. Antes de cualquier tratamiento, la autoridad competente deberá evaluar los datos para detectar posibles características protegidas y eliminar datos cuyo tratamiento sería ilícito. A modo de buena práctica, esto debe complementarse mediante un programa de detección y eliminación con un glosario de «términos sensibles» actualizado periódicamente.

Los criterios de elaboración de perfiles deben ser específicos y dirigidos

El uso de **criterios genéricos de elaboración de perfiles** entraña otro riesgo. Los instrumentos actuales de la UE permiten desarrollar algoritmos de elaboración de perfiles con un alto grado de discrecionalidad. Para evaluar el riesgo de migración irregular, el SEIAV contempla el uso de estadísticas europeas y nacionales sobre el porcentaje de estancias autorizadas sobrepasadas y denegaciones de entrada. No obstante, en lo que respecta a los riesgos para la seguridad, en general se refiere únicamente a información relativa a determinados indicadores de seguridad y amenazas. La Directiva del PNR ofrece indicaciones generales para el diseño de algoritmos, pero no especifica qué criterios aplicar para identificar a personas que puedan

([48]) Véase también FRA (2017a).

estar involucradas en delitos terroristas o delitos graves, o qué ponderación asignar a un criterio concreto.

Los criterios excesivamente genéricos dan lugar a un número significativo de «falsos positivos», es decir, personas asociadas erróneamente con un determinado perfil de riesgo. Algunos de estos «falsos positivos» también podrían ser de carácter discriminatorio. Por ejemplo, una definición genérica del criterio «condena penal anterior» obligaría a personas LGBT a comunicar antecedentes penales relacionados con determinadas conductas sexuales criminalizadas en algunos países terceros.

- Los criterios de evaluación deben ser predefinidos, dirigidos, específicos, proporcionados y basados en hechos. Los criterios de evaluación deben ponerse a prueba con muestras anonimizadas. Deben someterse a revisiones periódicas por un auditor interno para determinar si siguen estando justificados por sus objetivos específicos.

- Antes de transmitir una alerta basada en un tratamiento automatizado para la adopción de medidas, la autoridad competente deberá revisar manualmente los datos conjuntamente con otra información, a fin de determinar si la persona encaja con el perfil de riesgo y eliminar falsos positivos. Los destinatarios de los datos deben proporcionar una valoración de las medidas adoptadas en virtud de la alerta.

Los datos tratados deben ser precisos y fiables

El estudio de la FRA confirma que los actuales sistemas TI de gran escala contienen una gran cantidad de datos inexactos ([49]). **La inexactitud o la falta de fiabilidad de los datos** pueden tener multitud de efectos negativos en el contexto de la elaboración algorítmica de perfiles con fines de gestión de fronteras o acción policial. Los datos inexactos pueden afectar negativamente a las personas, pero también dar lugar a que se establezcan correlaciones incorrectas y se obtenga una imagen distorsionada que ponga en peligro la eficacia del trabajo policial y de gestión de fronteras.

Esto es especialmente pertinente en los casos de datos introducidos por ciudadanos, como en los datos del PNR y las aplicaciones del SEIAV, que pueden ser más

([49]) Véase FRA (2018c), pp. 81-98.

propensos a errores que los registros oficiales. Del mismo modo, el análisis de las cuentas en redes sociales, que está previsto por algunos sistemas de autorización de viajes fuera de la UE, conlleva un riesgo elevado de introducción de información poco fiable en el proceso de elaboración de perfiles. Además, entraña un riesgo específico de que se recoja información que revele datos personales sensibles protegidos por la Carta, como la opinión política o información relativa a la vida sexual.

- Proporcionar información exacta a los interesados sobre la recogida, conservación y tratamiento de sus datos y sobre los principios de protección de datos aplicables. A los interesados se les deben comunicar sus derechos, incluidos los mecanismos de compensación de que dispongan.

- Permitir que los interesados soliciten la rectificación de sus datos cuando estos sean inexactos y que sean informados de si dichos datos han sido rectificados o suprimidos.

- Establecer mecanismos efectivos de compensación administrativa y judicial en el caso de que se haya violado algún derecho de protección de datos, por ejemplo si se deniega el acceso o no se rectifican o suprimen los datos inexactos.

Conclusión

La elaboración de perfiles es una herramienta legítima utilizada por agentes de policía y guardias de fronteras con fines de prevención, investigación y enjuiciamiento de actividades penales, así como de prevención y detección de la inmigración irregular.

Para que sea lícita, legítima y efectiva, la elaboración de perfiles debe utilizarse dentro de los límites previstos por la ley. En particular, la elaboración de perfiles debe respetar los requisitos de igualdad de trato y protección de los datos personales.

Esto se conseguirá mediante una combinación de elementos. Toda actividad de elaboración de perfiles debe:

- tratar a las personas por igual, con respeto y dignidad;
- evitar la elaboración de perfiles basados en sesgos;
- ser razonable, objetiva y basada en información de inteligencia; y
- proteger adecuadamente los datos personales y la vida privada de los interesados.

Los policías y guardias de fronteras disponen de diferentes herramientas para velar por que estos principios sean conocidos, entendidos y aplicados en la práctica:

- antes de elaborar perfiles, los agentes deben recibir orientación y formación;
- durante la elaboración de perfiles, deberán registrarse y conservarse los detalles de la actividad;
- tras la elaboración de perfiles, las acciones de los agentes deben ser objeto de vigilancia y evaluación para detectar aspectos susceptibles de mejora.

Mediante la prevención de actividades ilícitas de elaboración de perfiles no solo se consigue que los policías y guardias de fronteras respeten la ley, sino que sus acciones sean entendidas y aceptadas por los ciudadanos. Promover la confianza en la acción de la policía y los guardas responsables de la gestión de fronteras mejora la eficacia de dicha acción y, por tanto, contribuye a incrementar los niveles de seguridad y protección de la sociedad en su conjunto.

Anexo

Cuadro 7: Sistemas TI de gran escala existentes y previstos en la UE

Sistema TI	Finalidad principal	Personas a las que se refiere	Aplicabilidad	Instrumento jurídico/propuesta	Identificadores biométricos
Dactiloscopia europea (Eurodac)	Determinar el Estado miembro responsable del examen de una solicitud de protección internacional *Ayudar a controlar la inmigración y los movimientos secundarios irregulares*	Solicitantes y beneficiarios de protección internacional, *migrantes en situación irregular*	EU-28+ PAS	Reglamento (UE) n.º 603/2013 (Reglamento Eurodac) *COM(2016) 272 final (propuesta Eurodac)*	
Sistema de Información de Visados (VIS)	Facilitar el intercambio de datos entre Estados miembros de Schengen sobre solicitudes de visados	Solicitantes de visados y reagrupantes	EU-24 (sin CY, HR, IE ni UK)[1] + PAS	Reglamento (CE) n.º 767/2008 (Reglamento VIS)	
Sistema de Información de Schengen (SIS II) — policía	Garantizar la seguridad en los Estados miembros de la UE y de Schengen	Personas desaparecidas o buscadas	EU-26 (sin CY ni IE)[2] + PAS	Decisión 2007/533/JAI del Consejo (Decisión SIS II) *COM(2016) 883 final (propuesta de policía SIS II)*	
Sistema de Información de Schengen (SIS II) — fronteras	Introducir y tratar alertas con el fin de denegar la entrada o la estancia en los Estados miembros de Schengen	Migrantes en situación irregular	EU-25 (sin CY, IE ni UK)[2] + PAS	Reglamento (CE) n.º 1987/2006 (Reglamento SIS II) *COM(2016) 882 final (propuesta de fronteras SIS II)*	
Sistema de Información de Schengen (SIS II) — retorno	*Introducir y tratar alertas de nacionales de terceros países sujetos a una decisión de retorno*	*Migrantes en situación irregular*	*EU-25 (sin CY, IE ni UK)[2] + PAS*	*COM(2016) 881 final (propuesta de retorno SIS II)*	

Sistema de Entradas y Salidas (SES)	*Calcular y supervisar la duración de la estancia autorizada de nacionales de terceros países e identificar a los que superan su estancia autorizada*	*Viajeros que llegan para una estancia de corta duración*	*EU-22 (sin BG, CY, HR, IE, RO ni UK)[3] + PAS*	*Reglamento (UE) 2017/2226 (Reglamento SES)*	
Sistema Europeo de Información y Autorización de Viajes (SEIAV)	*Evaluar si un nacional de un tercer país exento de visado entraña un riesgo para la seguridad, la migración irregular o la salud pública*	*Viajeros exentos de visado*	*EU-26 (sin IE ni UK)[3] + PAS*	*COM(2016) 731 final (propuesta SEIAV)*	*Ninguno*
Sistema Europeo de Información de Antecedentes Penales para nacionales de terceros países (ECRIS-TCN)	*Compartir información sobre condenas anteriores de nacionales de terceros países*	*Nacionales de terceros países con antecedentes penales*	*EU-27 (sin DK)[4]*	*COM(2017) 344 final (propuesta ECRIS-TCN)*	
Interoperabilidad – Repositorio de identidad común	*Establecer un marco para la interoperabilidad entre SES, VIS, SEIAV, Eurodac, SIS II y ECRIS-TCN*	*Nacionales de terceros países comprendidos en Eurodac, VIS, SIS II, SES, SEIAV y ECRIS-TCN*	*EU-28[5] + PAS*	*COM(2017) 793 final (Propuesta interoperabilidad fronteras y visados)* *COM(2017) 794 final (Propuesta interoperabilidad cooperación policial, asilo y migración)*	

Nota: *Los sistemas previstos y los cambios previstos en los sistemas se muestran en cursiva.*

 *: Huellas dactilares*  *: Huellas de las palmas*  *: Imagen facial*  *: Perfil de ADN.*

EU-XX: Europa de los XX (número de Estados miembros). PAS: Países asociados a Schengen, es decir, Islandia, Liechtenstein, Noruega y Suiza.

1 *Irlanda y el Reino Unido no participan en VIS. Dinamarca no está vinculada por el Reglamento, pero se ha incorporado voluntariamente al VIS. El VIS todavía no se aplica en Croacia y Chipre y solo en parte en Bulgaria y Rumanía, de acuerdo con la Decisión (UE) 2017/1908 del Consejo, de 12 de octubre de 2017.*

2 *Chipre e Irlanda todavía no están conectados al SIS. Dinamarca no está vinculada por el Reglamento ni por la Decisión del Consejo, pero se ha incorporado voluntariamente al SIS II, y deberá decidir de nuevo si lo hace cuando se adopten las propuestas SIS II. El Reino Unido participa en el SIS, pero no puede utilizar ni acceder a las alertas de denegación de entrada o estancia en el espacio Schengen. Bulgaria, Rumanía y Croacia no pueden emitir alertas Schengen de denegación de entrada o estancia en el espacio Schengen, ya que todavía no forman parte del espacio Schengen.*

3 *Dinamarca podría optar por incorporarse voluntariamente al SES y al SEIAV.*

4 *El ECRIS-TCN no se aplica en Dinamarca. El Reino Unido e Irlanda podrían optar por incorporarse voluntariamente.*

5 *Dinamarca, Irlanda y el Reino Unido tomarán parte ya que participan en los sistemas TI que se han hecho interoperables.*

Fuente: *FRA, de acuerdo con los instrumentos jurídicos vigentes y propuestos, 2018.*

Referencias

Agencia Europea de la Guardia de Fronteras y Costas (Frontex) (2012): *Common core curriculum, EU border guard basic training*, marzo de 2012.

Agencia Europea de la Guardia de Fronteras y Costas (Frontex) (2013): *Fundamental rights training for border guards, Trainers' Manual*, 2013.

Agencia Europea de la Guardia de Fronteras y Costas (Frontex) (2015): *Twelve seconds to decide. In search of excellence: Frontex and the principle of best practice*, 2015.

Agencia Europea de la Guardia de Fronteras y Costas (Frontex) (2017): *Handbook on risk profiles on Trafficking in Human Beings*, 2017.

Akhgar, B.; Saathoff, G. B.; Arabnia, H. R.; Hill, R.; Staniforth, A., y Bayerl, P. S. (2015): *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*, Butterworth-Heinemann, 2015.

American Civil Liberties Union (ACLU) (2016): *Eight Problems With Police «Threat Scores»,* 13 de enero de 2016.

Big Brother Watch: *Smile you're on body worn camera Part II – Police, The use of body worn cameras by UK police forces*, agosto de 2017.

Body-Gendrot, S. (2016): «Making sense of French urban disorders in 2005», *European Journal of Criminology*, vol. 13, n.º 5, pp. 556–572.

Bovens *et al.* (2014): «Public accountability», en: Bovens, M., Schillermans, T. y Goodlin, R. E. (ed.), *The Oxford handbook of public accountability*, Oxford, Oxford University Press, 2014.

Brayne, S. (2014): «Surveillance and system avoidance: criminal justice contact and institutional attachment», *American Sociological Review*, vol. 79, n.º 3, pp. 367–391.

Buolamwini, J., y Gebru, T. (2018): *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, MIT Media Lab and Microsoft Research, 2018.

Center on Privacy and Technology at Georgetown Law (2016): *The Perpetual Line-up, Unregulated Police Face Recognition in America*, 18 de octubre de 2016.

Centre d'analyse stratégique (2006): *Enquête sur les violences urbaines — Comprendre les émeutes de novembre 2005: les exemples de Saint-Denis et d'Aulnay-Sous-Bois*, París, La Documentation française, 2006.

Comisión Europea (2017a): *Hate crime training for law enforcement and criminal justice authorities: 10 key guiding principles*, febrero de 2017.

Comisión Europea (2017b): *Improving the recording of hate crime by law enforcement authorities, Key guiding principles*, diciembre de 2017.

Comisión Europea contra el Racismo y la Intolerancia (ECRI) (2007): *ECRI General Policy Recommendation No. 11 on combating racism and racial discrimination in policing* adoptada el 29 de junio de 2007, Estrasburgo, 4 de octubre de 2007.

Comisión Europea, Subgrupo de trabajo sobre metodologías de documentación y recogida de datos sobre delitos motivados por el odio (2017): *Improving the recording of hate crime by law enforcement authorities — Key guiding principles*, Bruselas, diciembre de 2017.

Consejo de Europa, Comité de Ministros (2001): *Recomendación Rec(2001)10 del Comité de Ministros a los Estados miembros sobre el Código Europeo de Ética de la Policía*, 19 de septiembre de 2001.

Consejo de la Unión Europea (2009): *Actualización del Catálogo de Schengen sobre control de las fronteras exteriores, retorno y readmisión*, 19 de marzo de 2009.

Coudert, F.; Butin, D., y Le Metayer, D. (2015): «Body-worn cameras for police accountability: opportunities and risks», *Computer Law and Security Review*, vol. 31, pp. 749–762.

De Hert, P., y Lammerant, H. (2016): «Predictive profiling and its legal limits: effectiveness gone forever?», en: van der Sloot, B.; Broeders, D., y Schrijvers, E. (ed.), The Netherlands Scientific Council for Government Policy, *Exploring the boundaries of big data*, Ámsterdam, Amsterdam University Press, pp. 145–173.

Défenseur des droits (2017): *Enquête sur l'accès aux droits. Volume 1 – relations police/population: le case des contrôles d'identité*, 2017

Dinant, J.-M.; Lazaro, C.; Poullet Y.; Lefever, N., y Rouvroy, A. (2008): *Application of Convention 108 to the Profiling Mechanism — Some ideas for the future work of the consultative committee (T-PD)*, Doc. T-PD 01, p. 3.

Estados Unidos, GAO (General Accounting Office) (2000): *U.S. Customs Office: better targeting of airline passengers for personal searches could produce better results,* GAO/GGD-00-38, marzo de 2000.

European network of legal experts in gender equality and non-discrimination (2016): *Links between migration and discrimination — A legal analysis of the situation in EU Member States*, julio de 2016.

Farrar, T. (2018): *Self-awareness to being watched and socially-desirable behavior: A field experiment on the effect of body-worn cameras on police use-of-force*, Police Foundation, 2018.

FRA (Agencia de los Derechos Fundamentales de la Unión Europea), Supervisor Europeo de Protección de Datos (SEPD) y Consejo de Europa (2018): *Manual de legislación europea en materia de protección de datos — Edición de 2018,* Luxemburgo, Oficina de Publicaciones, mayo de 2018.

FRA (Agencia de los Derechos Fundamentales de la Unión Europea) (2013): *Formación de las fuerzas de seguridad del estado basada en los derechos fundamentales*, Luxemburgo, Oficina de Publicaciones, diciembre de 2013.

FRA (2014a): *Fundamental rights at airports: border checks at five international airports in the European Union*, Luxemburgo, Oficina de Publicaciones, 2014.

FRA (2014b): *Fundamental rights at land borders: findings from selected European Union border crossing points*, Luxemburgo, Oficina de Publicaciones, 2014.

FRA (2014c): *Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data*, febrero de 2014.

FRA (2016): *Fundamental Rights Report 2016*, Luxemburgo, Oficina de Publicaciones, 2016.

FRA (2017a): *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel*

Information and Authorisation System (ETIAS), Dictamen de la FRA – 2/2017 [ETIAS], junio de 2017.

FRA (2017b): *Second European Union Minorities and Discrimination Survey — Main results*, Luxemburgo, Oficina de Publicaciones, diciembre de 2017.

FRA (2017c): *Fundamental Rights Report 2017*, Luxemburgo, Oficina de Publicaciones, mayo de 2017.

FRA (2017d): *Segunda encuesta de la Unión Europea sobre las minorías y la discriminación, Musulmanes: algunas conclusiones*, Luxemburgo, Oficina de Publicaciones de la Unión Europea, septiembre de 2017.

FRA (2017e): *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxemburgo, Oficina de Publicaciones, mayo de 2017.

FRA (2018a): *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, Dictamen de la FRA – 1/2018 [Interoperability], abril de 2018.

FRA (2018b): *#BigData: Discrimination in data-supported decision making*, FRA Focus Paper, mayo de 2018.

FRA (2018c): *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxemburgo, Oficina de Publicaciones, febrero de 2018.

FRA (2018d): *Hate crime recording and data collection practice across the EU*, Luxemburgo, Oficina de Publicaciones, junio de 2018.

FRA (2018e): *Fundamental Rights Report 2018*, Luxemburgo, Oficina de Publicaciones, junio de 2018.

FRA y Consejo de Europa (2018): *Handbook on European non-discrimination law – 2018 edition*, Luxemburgo, Oficina de Publicaciones, febrero de 2018.

Francia, Ministerio del Interior (2018): *Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale*, 7 de junio de 2018.

Gandy, O. (2010): «Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems», *J Ethics Inf Technol*, vol. 12, n.º 1, pp. 29-42, 2010.

Gross, S. R. (2002): «Racial Profiling under Attack», D. Livingston, coautor. *Colum. L.* Rev. 102, n.º 5, pp. 1413-38.

Grupo de Trabajo del Artículo 29 (2014): *Dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas*, 536/14/ES, WP 211, Bruselas, 27 de febrero de 2014.

Grupo de Trabajo del Artículo 29 (2017a): *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*, WP 248 rev.01, 4 de octubre de 2017.

Grupo de Trabajo del Artículo 29 (2017b): *Dictamen sobre algunas cuestiones fundamentales de la Directiva sobre protección de datos en el ámbito penal (UE 2016/680)*, 7 de diciembre de 2017.

Grupo de Trabajo del Artículo 29 (2018a): *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, WP251 rev.01, 6 de febrero de 2018.

Grupo de Trabajo del Artículo 29 (2018b): *Opinion on Commission proposals on establishing a framework for interoperability*, WP266, Bruselas, 23 de abril de 2018.

Harcourt, B. (2004): «Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally», *University of Chicago Law Review*, vol. 71, 2004.

Harris, D. (2002): «Flying While Arab: Lessons from the Racial Profiling Controversy», *Civil Rights Journal*, vol. 6, nº 1, invierno 2002.

Harris, D. (2003): *Profiles in Injustice; Why Racial Profiling Cannot Work*, The New Press, 2003.

Hildebrandt, M., y De Vries, K. (2013): *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*, Nueva York, Routledge, 2013.

Hildebrandt, M., y Gutwirth, S. (ed.) (2008): *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Berlín, Springer, 2008.

Hörnqvist, M. (2016): «Riots in the welfare state: The contours of a modern-day moral economy», *European Journal of Criminology*, vol. 13, n.º 5, pp. 573–589.

Hunt, P.; Saunders, J., y Hollywood, J. S. (2014): *Evaluation of the Shreveport predictive policing experiment*, RAND Corporation, 2014.

Jobard, F. (2008): «The 2005 French urban unrests: data-based interpretations», *Sociology Compass*, vol. 2, n.º 4, pp. 1287–1302.

Kádár, A.; Körner, J.; Moldova, Z., y Tóth, B. (2008): *ProjectControl(led) Group, Final Report on the Strategies for Effective Police Stop and Search (STEPSS)*, Budapest, p. 23.

Keskinen, S., *et al.* (2018): *The Stopped – Ethnic Profiling in Finland*, Swedish School of Social Science, University of Helsinki, Helsinki, 3 de abril de 2018.

Korff, D. (2015): *Passenger Name Records, data mining & data protection: the need for strong safeguards*, T-PD(2015)11, Estrasburgo, 15 de junio de 2015.

Miller, J., y Alexandrou, B. (2016): *College of policing stop and search training experiment: Impact evaluation*, College of Policing Limited, 2016.

Mittelstadt, B. D.; Allo, P.; Taddeo, M.; Wachter, S., y Floridi, L. (2016): «The ethics of algorithms: Mapping the debate», *Big Data & Society*, 1 de diciembre de 2016.

Mohler, G. O.; Short, M. B.; Malinowski, S.; Johnson, M.; Tita, G. E.; Bertozzi, A. L., y Brantingham, P. J.: *Randomized Controlled Field Trials of Predictive Policing*, 15 de enero de 2016.

Naciones Unidas (2007): *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*, A/HRC/4/26, 29 de enero de 2007.

Nisbet, R.; Elder, J., y Miner, G. (2009): *Handbook of Statistical Analysis & Data Mining Applications*, Sídney (Canadá), Elsevier, 2009.

Observatorio Europeo del Racismo y la Xenofobia (2016): *Perceptions of discrimination and islamophobia – Voices from members of Muslim communities in the European Union*, 2006.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACDH) (2014): *Principios y directrices recomendados sobre los derechos humanos en las fronteras internacionales*, 23 de julio de 2014.

Open Society Justice Initiative (2018a): *Regulating Police Stop and Search: An Evaluation of the Reasonable Grounds Panel*, diciembre de 2018.

Open Society Justice Initiative (2018b): *The Recording of Police Stops: Methods and Issues*, diciembre de 2018.

Oswald, M.; Grace, J.; Urwin, S., y Barnes, G.: «Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and "Experimental" Proportionality», *Information & Communications Technology Law*, 31 de agosto de 2017.

Reino Unido, Camden y London Prepared (2006): *Major Incident Procedures, What businesses and the voluntary sector need to know*, abril de 2006.

Reino Unido, College of Policing (2016): *Stop and Search*, Authorised Professional Practice (APP), 29 de septiembre de 2016.

Reino Unido, Equality and Human Rights Commission (2009): *Police and racism: what has been achieved 10 years after the Stephen Lawrence Inquiry report?*, 2009.

Reino Unido, Her Majesty's Inspectorate of Constabulary (HMIC) (2013): *Stop and Search Powers: Are the police using them effectively and fairly?*, 2013.

Reino Unido, Her Majesty's Inspectorate of Constabulary (HMIC) (2016): *PEEL: Police legitimacy 2015 An inspection of West Midlands Police*, febrero de 2016.

Reino Unido, Home Office (1999): *The Stephen Lawrence Inquiry. Report of An Inquiry by Sir William Macpherson of Cluny*, febrero de 1999.

Reino Unido, Home Office (2014a): *CODE A: Revised code of practice for the exercise by: police officers of statutory powers of stop and search; police officers and police staff of requirements to record public encounters*, Norwich, The Stationery Office (TSO), 2014.

Reino Unido, Home Office (2014b): *Best use of stop and search scheme*, 2014.

Reino Unido, House of Commons Home Affairs Committee (2009): *The Macpherson Report – Ten Years On,* Twelfth Report of Session 2008–09, 22 de julio de 2009.

Reino Unido, House of Lords (2006): *Opinions of the Lords of appeal for judgment in the cause R [on the application of Gillan (FC) and another (FC)] (demandantes) contra Commissioner of Police for the Metropolis and another (demandados)*, [2006] UKHL 12, 8 de marzo de 2006.

Reino Unido, London School of Economics (2011): *Reading the Riots*, diciembre de 2011.

Reino Unido, National Policing Improvement Agency (NPIA) (2012): *Stop and search, the use of intelligence and geographic targeting, Findings from case study research*, 2012.

Reino Unido, Northamptonshire Police (2018): *Get Involved – Reasonable Grounds Panel*, último acceso en abril de 2018.

Reino Unido, Staffordshire PCC Matthew Ellis, Ethics, Transparency and Audit Panel (2015): *An Independent Report into Stop & Search Encounters by Staffordshire Police,* enero de 2015.

Reino Unido, Stop Watch (2011): *«Carry on Recording» Why police stops should still be recorded*, mayo de 2011.

Reino Unido, West Midlands Police (2012): *Stop and Search Policy*, noviembre de 2012.

Reino Unido, West Midlands Police (2016): *Stop and Search Recommendations*, julio de 2015 (última modificación en junio de 2016).

Reino Unido, West Midlands Police (2017a): *Stop and Search in the West Midlands: Presentation to Den Hague City Council*, abril de 2017.

Reino Unido, West Midlands Police (2017b): *New «app» set to speed up Stop & Search process*, agosto de 2017.

Reino Unido, West Midlands Police (2018): *Stop and Search Scrutiny Panels*, último acceso en abril de 2018.

Reino Unido, West Midlands Police y Crime Commissioner (2014): *Stop and Search Action Plan – Outcome of consultation*, enero de 2014.

Schauer, F. (2003): *Profiles Probabilities and Stereotypes*, Cambridge (MA), The Belknap Press of Harvard University Press, 2003.

Scheinin, M. (2007): United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism: *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, UN Doc. A/HRC/4/26, 29 de enero de 2007.

Supervisor Europeo de Protección de Datos (SEPD) (2015): *Segundo Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves,* Dictamen 5/2015, Bruselas, 24 de septiembre de 2015.

Supervisor Europeo de Protección de Datos (SEPD) (2018): *Dictamen 4/2018 del Supervisor Europeo de Protección de Datos sobre las propuestas de dos Reglamentos por los que se establece un marco para la interoperabilidad de los sistemas de información a gran escala de la UE*, Bruselas, 18 de abril de 2018.

The Guardian (2015): *Northamptonshire police ban stop and search by officers who abuse powers*, 18 de agosto de 2015.

Tóth, B. M., y Kádár, A. (2011): «Ethnic profiling in ID checks by the Hungarian police», *Policing and Society*, vol. 21, n.º 4, pp. 383–394.

Unia (Bélgica): *Annual Report 2016*, Bruselas, septiembre de 2017.

Unia (Bélgica): *Rapport annuel Convention entre Unia et la police fédérale, Budget 2015*, Bruselas, 2015.

Van Brakel, R. (2016): «Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing», en: van der Sloot, B., Broeders, D. y Schrijvers, E. (ed.), The Netherlands Scientific Council for Government Policy (*Wetenschappelijke Raad voor het Regeringsbeleid*), *Exploring the boundaries of big data*, Ámsterdam, Amsterdam University Press, pp. 117–141.

Wrench, J. (2007): *Diversity management and discrimination: immigrants and ethnic minorities in the EU*, Aldershot, Ashgate, 2007.

Zarsky, T. Z. (2011): «Governmental Data Mining and its Alternatives», *Penn State Law Review*, vol. 11, n.º 2, pp. 285–330.

Legislación de la Unión Europea

Derechos fundamentales

Carta de los Derechos Fundamentales de la Unión Europea, 2012/C 326/02, DO C 326 de 26.10.2012.

Explicaciones sobre la Carta de los Derechos Fundamentales , 2007/C 303/02, DO C 303/17 de 14.12.2007.

No discriminación

Directiva 2000/43/CE del Consejo, de 29 de junio de 2000, relativa a la aplicación del principio de igualdad de trato de las personas independientemente de su origen racial o étnico.

Directiva 2000/78/CE del Consejo, de 27 de noviembre de 2000, relativa al establecimiento de un marco general para la igualdad de trato en el empleo y la ocupación.

Protección de datos

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Gestión de fronteras

Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO L 205/63 de 7.8.2007 *(SIS II)*.

Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, DO L 119/132 de 27.4.2016.

Reglamento (CE) n.º 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 381/4 de 28.12.2006).

Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre Estados miembros (Reglamento VIS), DO L 218/60 de 13.8.2008 (*Reglamento VIS*).

Reglamento (UE) n.º 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n.º 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos

de gran magnitud en el espacio de libertad, seguridad y justicia, DO L 180/1 de 29.6.2013.

Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2016, sobre la Guardia Europea de Fronteras y Costas, por el que se modifica el Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo y por el que se derogan el Reglamento (CE) n.º 863/2007 del Parlamento Europeo y del Consejo, el Reglamento (CE) n.º 2007/2004 del Consejo y la Decisión 2005/267/CE del Consejo, DO L 251/1 de 14 de septiembre de 2016.

Reglamento (UE) n.º 1052/2013 del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, por el que se crea un Sistema Europeo de Vigilancia de Fronteras (Eurosur), DO L 295/11 de 6.11.2013.

Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen).

Jurisprudencia

Francia, Tribunal de Casación (*Cour de Cassation*), *Décision 1245*, 9 de noviembre de 2016.

Reino Unido, House of Lords, *R (on the application of Gillan* et al.*) v. Commissioner of Police for the Metropolis et al.*, [2006] UKHL 12, 8 de marzo de 2006.

TJUE, C-524/06, *Heinz Huber contra Bundesrepublik Deutschland*, 16 de diciembre de 2008.

TEDH, *B.S. contra España*, n.º 47159/08, 24 de julio de 2012.

TEDH, *S. y Marper contra Reino Unido*, n.ºs 30562/04 y 30566/04, 4 de diciembre de 2008.

TEDH, *Gillan y Quinton contra Reino Unido*, n.º 4158/05, 12 de enero de 2010.

UNHRC, *Rosalind Williams Lecraft contra España*, Com. n.º 1493/2006, 30 de julio de 2009.

Ponerse en contacto con la Unión Europea

En persona

En la Unión Europea existen cientos de centros de información Europe Direct. Puede encontrar la dirección del centro más cercano en: https://europa.eu/european-union/contact_es

Por teléfono o por correo electrónico

Europe Direct es un servicio que responde a sus preguntas sobre la Unión Europea. Puede acceder a este servicio:

— marcando el número de teléfono gratuito: 00 800 6 7 8 9 10 11 (algunos operadores pueden cobrar por las llamadas);
— marcando el siguiente número de teléfono: +32 22999696; o
— por correo electrónico: https://europa.eu/european-union/contact_es

Buscar información sobre la Unión Europea

En línea

Puede encontrar información sobre la Unión Europea en todas las lenguas oficiales de la Unión en el sitio web Europa: https://europa.eu/european-union/index_es

Publicaciones de la Unión Europea

Puede descargar o solicitar publicaciones gratuitas y de pago de la Unión Europea en: https://publications.europa.eu/es/publications
Si desea obtener varios ejemplares de las publicaciones gratuitas, póngase en contacto con Europe Direct o su centro de información local (https://europa.eu/european-union/contact_es).

Derecho de la Unión y documentos conexos

Para acceder a la información jurídica de la Unión Europea, incluido todo el Derecho de la Unión desde 1952 en todas las versiones lingüísticas oficiales, puede consultar el sitio web EUR-Lex: http://eur-lex.europa.eu

Datos abiertos de la Unión Europea

El portal de datos abiertos de la Unión Europea (http://data.europa.eu/euodp/es) permite acceder a conjuntos de datos de la Unión. Los datos pueden descargarse y reutilizarse gratuitamente con fines comerciales o no comerciales.

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Los avances tecnológicos han favorecido el incremento de la práctica de elaboración de perfiles en muy diversos contextos y, en los últimos tiempos, los Estados miembros han mostrado un mayor interés en el empleo de herramientas para elaborar perfiles como forma de facilitar el trabajo de los agentes de policía y de gestión de fronteras. La elaboración de perfiles se utiliza de forma legítima para prevenir, investigar y perseguir infracciones penales, así como para prevenir y detectar la inmigración irregular. Sin embargo, la elaboración ilícita de perfiles puede menoscabar la confianza en las autoridades y estigmatizar a determinadas comunidades.

En esta guía se explica qué es la elaboración de perfiles, los marcos jurídicos que la regulan, y por qué llevarla a cabo de manera lícita no solo es necesario para respetar los derechos fundamentales, sino también crucial para la eficacia de la actuación policial y la gestión de fronteras. Esta guía contiene también orientaciones prácticas sobre cómo evitar la utilización ilícita de perfiles en las operaciones de vigilancia policial y gestión de fronteras.

FRA – AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA
Schwarzenbergplatz 11 – 1040 Viena – Austria
Tel. +43 158030-0 – Fax +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Oficina de Publicaciones
de la Unión Europea