



NUEVAS TECNOLOGÍAS, VIEJAS INJUSTICIAS

LA DISCRIMINACIÓN Y CRIMINALIZACIÓN
BASADA EN EL ANÁLISIS DE DATOS EN LA
POLICÍA Y LAS CÁRCELES EUROPEAS

ESCRITO POR:

Griff Ferris

Sofia Lyall

FINANCIADO POR:

European
Artificial Intelligence
& Society Fund

Informations concernant la publication

Autores : Griff Ferris, Sofia Lyall

Editor : Chris Jones

Diseño: McKensie Marie

Este informe ha contado con el apoyo de la
European AI & Society Foundation.

Publicado por Statewatch, junio de 2025.

Sobre Statewatch

Statewatch fomenta y lleva a cabo investigaciones críticas, análisis de políticas y labores de periodismo de investigación para crear debates, movimientos y campañas sobre libertades civiles, derechos humanos y estándares democráticos. Comenzamos nuestra andadura en 1991 y nos encontramos en Londres.

statewatch.org

(+44) (0) 203 393 8366

**MayDay Rooms, 88 Fleet Street, London
EC4Y 1DH, UK**

Apoye nuestro trabajo

Apoya nuestro trabajo con una donación:



Suscríbete a nuestra lista de correos:

— [Inscripción en la lista de correo](#)

**Número de registro de organización
benéfica en Reino Unido:** 1154784

**Número de registro de sociedad en Reino
Unido:** 08480724

Denominación social : The Libertarian
Research & Education Trust

Domicilio social: 88 Fleet Street, London
EC4Y 1DH, UK.

Índice

Reconocimientos	4
Definiciones	5
Resumen ejecutivo	7
Introducción	12
Sistemas «predictivos» centrados en la ubicación	23
Sistemas de elaboración de perfiles y «predictivos» de delitos centrados en las personas	38
Sistemas de videovigilancia con IA	49
Bases de datos	53
Conclusión	57
Créditos de las imágenes	64
Notas	65

Reconocimientos

Este trabajo ha sido posible gracias a los equipos de investigación y organizaciones colaboradoras de Bélgica, Francia, Alemania y España.

- Bélgica: Corentin Debailleul, Technopolice Belgium y Ligue des droits humains.
- Francia: Edlira Nano y Félix Tréguer, La Quadrature du Net, con la ayuda de las personas integrantes del grupo de trabajo de Technopolice France de La Quadrature du Net.
- Alemania: Sonja Peteranderl, AlgorithmWatch.
- España: Naiara Bellio, con la colaboración de Ana Valdivia y Javier Sánchez Monedero, AlgoRace.

Expresamos nuestro profundo agradecimiento a todas las personas y grupos que han participado en las entrevistas o han proporcionado información, su experiencia o pericia.

También queremos agradecer el trabajo de aquellas personas y organizaciones que se enfrentan y organizan frente al racismo y la discriminación en los sistemas policiales y jurídico-penales, en los cuales estas nuevas tecnologías constituyen la versión más reciente.

Definiciones

Inteligencia artificial

La Ley de Inteligencia Artificial de la Unión Europea define un sistema de IA como:

«... un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales».¹

Este informe utiliza esta definición, aunque existen varias formas de definir tanto la IA como sus sistemas.² Es importante recalcar que la mayoría de los sistemas automatizados, algorítmicos y basados en análisis de datos que utilizan la policía y las autoridades del sistema jurídico-penal en Europa no usan inteligencia artificial. Algunos de estos sistemas sí que emplean el aprendizaje automático (véase a continuación), un subcampo de la IA. Sin embargo, muchos de estos sistemas utilizan métodos estadísticos clásicos y pueden describirse como sistemas automatizados de toma de decisiones (véase a continuación).

Sistema automatizado de toma de decisiones

La United Kingdom Office for AI (Oficina de IA de Reino Unido) define los sistemas automatizados de toma de decisiones como aquellos que emplean «únicamente decisiones automatizadas (en las que el juicio humano no está presente)», así como «la toma de decisiones asistida por sistemas automatizados (que ayudan al juicio humano)».³

Aprendizaje automático

El diccionario Cambridge define el aprendizaje automático como el «proceso por el que los ordenadores mejoran su propia capacidad para desempeñar tareas mediante el análisis de datos nuevos, sin que una persona tenga que darle instrucciones a través de un programa, o el estudio de la creación y uso de sistemas informáticos capaces de hacerlo».⁴

Actuación policial «predictiva»:

Principalmente, hay dos tipos de la denominada actuación policial predictiva: una basada en la ubicación o el lugar y otra basada en la persona. Amnistía Internacional define los sistemas de actuación policial predictiva como:

«... programas informáticos que utilizan modelos de datos y algoritmos para evaluar el riesgo de que se cometa un delito. Los sistemas de actuación policial predictiva calculan puntuaciones de riesgo que presuntamente reflejan la probabilidad de que una persona o grupo cometa o sea víctima de un delito (actuación policial predictiva basada en la persona) o de que un lugar concreto sea el futuro escenario de un delito (actuación policial predictiva basada en el lugar). Conforme a estas puntuaciones de riesgo generadas por ordenador, la policía adopta medidas para prevenir o detectar el delito predicho, para lo que dirige sus esfuerzos hacia zonas, personas o grupos de «alto riesgo».⁵





Resumen ejecutivo

Cada vez más, las autoridades de los sistemas policiales y jurídico-penales de toda Europa emplean sistemas y herramientas basados en el análisis de datos para «predecir» dónde se va a cometer un delito, para elaborar perfiles de personas potencialmente delincuentes y evaluar el «riesgo» de delincuencia o criminalidad en el futuro.

Estas supuestas «predicciones», perfiles y evaluaciones de riesgos influyen en las decisiones, actuaciones e intervenciones policiales. Aquí se incluyen las labores de vigilancia y seguimiento, los interrogatorios, la interceptación y registro, la comprobación de identidad, la inhabilitación laboral, la redada en un domicilio, las multas, el uso de la fuerza, la detención, el arresto y la deportación.

Estos sistemas y decisiones basados en el análisis de datos también influyen en las decisiones del sistema jurídico-penal: desde la detención y la prisión preventiva, hasta la acusación, la sentencia y la libertad condicional.

Fuera del sistema jurídico-penal, las decisiones automatizadas también pueden influir o derivar en otras formas de castigo. Por ejemplo, pueden respaldar la denegación o restringir el acceso a servicios públicos básicos como prestaciones sociales o la vivienda.

Este informe resume la investigación original sobre los sistemas automatizados de toma de decisiones y las bases de datos utilizados en los sistemas policiales y jurídico-penales de cuatro países: Bélgica,

Francia, Alemania y España. Se basa en una exhaustiva investigación llevada a cabo por las organizaciones colaboradoras en esos países.⁶ El informe tiene en cuenta:

- cómo se desarrollan los sistemas predictivos de delitos basados en el análisis de datos;
- cómo los utilizan las autoridades policiales y jurídico-penales;
- los resultados de esos sistemas;
- cómo se utilizan esos resultados y cómo influyen en las decisiones, además del impacto que tienen en las personas, grupos y comunidades.

Asimismo, analiza cómo estos sistemas se dirigen y afectan de forma desproporcionada a los grupos y comunidades marginados, como, por ejemplo, las personas y comunidades negras y racializadas, las víctimas de violencia de género, las personas migrantes o procedentes de zonas de clase trabajadora y con dificultades socioeconómicas, así como personas con problemas de salud mental.

La mayoría de estos sistemas se alimentan de datos históricos, por ejemplo de la policía o del sistema jurídico-penal. Este hecho refleja sesgos tanto históricos como actuales en estas instituciones y en la sociedad en general, y conlleva la sobrevigilancia y criminalización de las comunidades marginadas, especialmente de los grupos racializados, las personas migrantes y las personas procedentes de barrios de ingresos bajos.

El uso de estos sistemas en las actuaciones policiales y en el sistema jurídico-penal implica consecuencias significativas para los derechos individuales, incluido el derecho a un juicio justo, a la privacidad y a la no discriminación.

Sistemas de actuación policial «predictiva» centrados en la ubicación

En toda Europa, las fuerzas policiales están desarrollando e implementado métodos de actuación policial «predictiva» centrados en la ubicación. Estos sistemas algorítmicos se desarrollan para «predecir» dónde y cuándo se cometerá un delito. De esta forma, la policía puede asignar recursos a estos lugares. Los sistemas de



«predicción» geográfica de delitos se utilizan o se han utilizado en los cuatro países estudiados, Bélgica, Francia, Alemania y España, además de en otros países europeos, como Italia, Países Bajos, Suiza y Reino Unido.

Este estudio ha identificado dos tipos principales de sistemas centrados en la ubicación:

- predicción de «puntos críticos» de delincuencia que se basan en datos policiales históricos para prever futuros escenarios donde se cometerán delitos; y
- algoritmos de predicción de «riesgos» ambientales, que se basan en el supuesto de que los factores ambientales pueden determinar el lugar en el que se cometerá un delito, y, por tanto, predecir ubicaciones con mayor «riesgo».

Los métodos de predicción de «puntos críticos» de delincuencia utilizan las estadísticas históricas de delitos sobre el lugar y momento en el que ocurrió un delito para «predecir» futuros lugares en los que se cometerán delitos o «puntos críticos». Estas predicciones se basan en el análisis de datos estadísticos y tendencias de grandes cantidades de datos delictivos, a menudo procedentes de bases de datos policiales. Por norma general, los sistemas predictivos de «puntos críticos» ofrecen a la policía un «mapa de calor» para identificar las áreas o lugares en los que presuntamente existe un alto riesgo de que se cometa un delito.

Los sistemas de predicción de «puntos críticos» de delincuencia se utilizan para asignar los recursos policiales y determinar el momento y el lugar en el que deben patrullar sus agentes. Las medidas en las zonas con «puntos críticos» pueden incluir: vigilancia, recopilación de información, controles de identidad, interrogatorios, registros, órdenes de alejamiento, redadas en domicilios y detenciones. Este estudio pone de manifiesto que los puntos etiquetados como «puntos críticos» de delincuencia corresponden de manera desproporcionada a zonas o barrios en los que viven y trabajan comunidades de bajos ingresos y racializadas.

Los sistemas centrados en la ubicación tienen en cuenta datos ambientales y contextuales. Utilizan datos ambientales o contextuales para identificar las áreas o lugares más predispuestos presuntamente



a la delincuencia. Un algoritmo asigna un valor de vulnerabilidad a los lugares según factores espaciales, como por ejemplo:

- si el lugar está bien iluminado;
- estaciones de metro o autobús;
- terrazas de cafeterías;
- locales de comida rápida;
- baños públicos;
- farmacias, bares, algunos tipos de tiendas;
- árboles y bancos; y
- colegios y oficinas de correos.

Este método plantea una problemática similar en cuanto a sesgos y discriminación que los sistemas basados en datos de delincuencia.

Los sistemas de actuación policial «predictiva» centrados en las personas y los sistemas de «predicción» de delitos

Las herramientas de «predicción» de delitos centradas en las personas se diseñan para predecir la probabilidad o el «riesgo» que tiene una persona de cometer un delito. También se utilizan sistemas similares para evaluar las probabilidades que tiene una persona de ser víctima de un delito, como la violencia de género, o para la detección de supuestas denuncias falsas.

Las personas a las que se dirigen estos sistemas están sometidas a un análisis constante de los datos que las caracterizan, su pasado y presente, y sus relaciones. El objetivo es determinar y «predecir» su comportamiento, «riesgo» o supuesta «criminalidad». Esto puede conllevar graves consecuencias. Los resultados de estos sistemas pueden provocar la vigilancia o el control de las personas. Asimismo, puede conllevar más interpellaciones policiales, interrogatorios, registros, visitas al domicilio o lugar de trabajo, inhabilitación laboral, detenciones, deportaciones o arrestos.

Estas herramientas también se utilizan en el sistema jurídico-penal y pueden influir en la toma de decisiones del personal judicial, incluidas



las sentencias. De igual manera, pueden influir en la duración de las penas de cárcel de una persona y su puesta en libertad, así como en las condiciones de la detención.

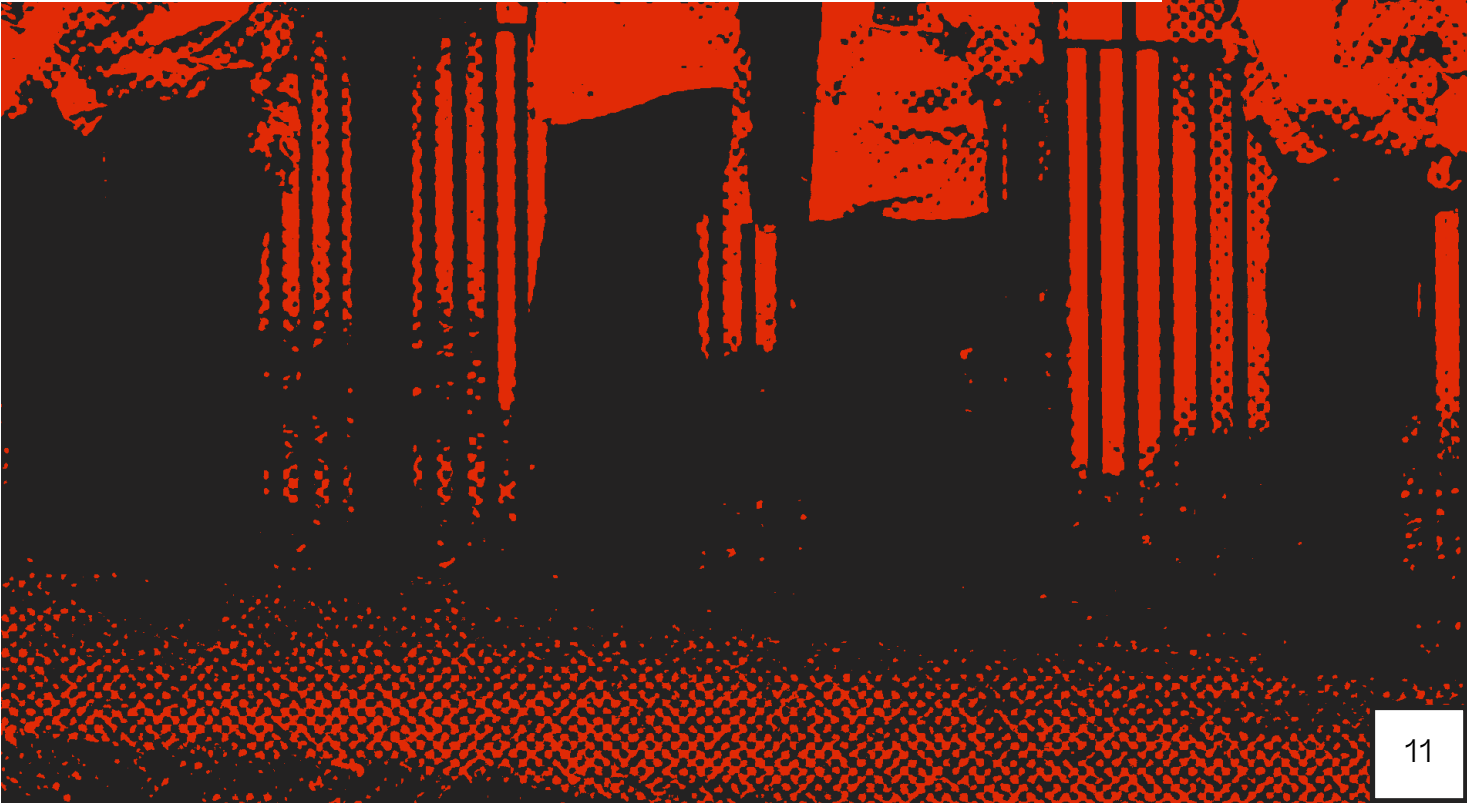
Conclusión

El uso de estos sistemas conlleva la elaboración de perfiles raciales y socio-económicos, su discriminación y criminalización. Se dirigen en particular a personas y comunidades marginadas, en concreto, a las personas negras y minorías étnicas, así como a personas de entornos desfavorecidos.

Su uso implica consecuencias injustas y discriminatorias: desde vigilancia, controles de identidad y registros, hasta acoso policial, redadas en domicilios, inhabilitación laboral, arresto, detención y deportación.

Estos sistemas se utilizan de forma secreta, es decir, la gente no es consciente de su uso. Como resultado, las personas a las que están dirigidas estas herramientas y las acciones derivadas de sus resultados no pueden oponerse a esos sistemas. Incluso si fueran conscientes de ello, no hay marco legal claro de responsabilidad.

La conclusión de todos los informes de las personas colaboradoras y de este informe es la misma: deberían prohibirse estos sistemas.





Introducción

En Europa, las autoridades policiales y jurídico-penales utilizan cada vez más sistemas digitales y basados en el análisis de datos. La introducción de estos nuevos sistemas se está produciendo a un ritmo vertiginoso, con poca transparencia sobre su implementación y sin un planteamiento previo de sus efectos y consecuencias.

Estos sistemas incluyen:

- vigilancia con reconocimiento facial;
- sistemas de reconocimiento de emociones;
- herramientas de extracción para teléfonos móviles;
- tobilleras y dispositivos de control electrónico; y
- sistemas «predictivos» y de elaboración de perfiles.

Lo que tienen en común todas estas prácticas es la recopilación y el tratamiento de cantidades masivas de datos (a menudo, datos personales de carácter sensible) para la toma de decisiones.

Este informe se centra en los sistemas automatizados de tomas de decisiones basados en el análisis de datos y algoritmos que utilizan los cuerpos de policía para «predecir» el lugar o el momento en el que se van a producir delitos o quién los va a cometer.

Quienes defienden estos enfoques supuestamente científicos y «predictivos» argumentan que permiten a la policía mejorar la eficacia de sus operaciones, además de reducir costes:

«Al utilizar una nueva estrategia llamada “actuaciones policiales basadas en la evidencia”, los gobiernos pueden trabajar con transparencia con la policía y la ciudadanía para invertir en tareas policiales rentables. Estas inversiones se pueden llevar a cabo simultáneamente con los recortes en los presupuestos destinados a la policía, lo que acabaría con tareas policiales costosas pero ineficaces».⁷

De hecho, el coordinador de IA de la Gendarmería Nacional francesa, el coronel Patrick Perrot, ha afirmado que los métodos basados en el análisis de datos permiten a la policía anticiparse a los delitos antes de que estos sucedan:

«... el enfoque científico nos permite desarrollar técnicas de modelización capaces de entender los futuros avances y prepararnos para ellos. Actualmente, la noción de anticipación es un factor determinante en el ámbito de los delitos».⁸

Como resultado, se ha producido un aumento en el escrutinio de los denominados sistemas de actuación policial «predictiva» por parte de organizaciones de la sociedad civil, activistas y organizaciones políticas, así como representantes del mundo académico de toda Europa.

Muchos grupos han planteado serias dudas sobre las posibles consecuencias de estos sistemas, por ejemplo, la vigilancia, el seguimiento, los interrogatorios, la interceptación y registro, las multas, las redadas domiciliarias, el uso de la fuerza, la deportación, la detención y arresto, así como la posible infracción de derechos individuales. Estos sistemas comprometen e infringen potencialmente el derecho a un juicio justo, a la privacidad, a la no discriminación, a la presunción de inocencia y el derecho a un resarcimiento efectivo.⁹

La investigación de este informe se suma a esta preocupación. El objetivo de esta investigación es apoyar campañas a nivel internacional, nacional, regional o local para solicitar la prohibición del uso de la IA y sus algoritmos por parte de las autoridades jurídico-penales. En aquellos casos en los que aún no se ha prohibido, es necesario contar con salvaguardas procesales, como por ejemplo rigurosas pruebas previas a la implementación, requisitos en cuanto a transparencia pública y oportunidades significativas de resarcimiento.



Resumen del informe

Este informe recopila y resume una exhaustiva investigación sobre los sistemas «predictivos» y las bases de datos en los sistemas policiales y jurídico-penales de Europa, basada en una investigación en cuatro países: Bélgica, Francia, Alemania y España.

Los principales motivos para elegir estos países han sido dos. Se sabía que los sistemas «predictivos» estaban siendo ampliamente utilizados por las fuerzas policiales y en el sistema jurídico-penal. Sin embargo, se contaba con pocos datos públicos sobre el desarrollo, uso e impacto de esos sistemas.

Los equipos de investigación llevaron a cabo esta investigación entre 2023 y 2024 junto con *AlgorithmWatch*, *La Quadrature du Net* y *Technopolice*. Las versiones originales están disponibles en Internet.¹⁰ Asimismo, *AlgoRace* ha llevado a cabo una investigación en España.

En cada país, los equipos de investigación trabajaron para estudiar los sistemas «predictivos» en uso, su funcionamiento, los resultados derivados de estos y su impacto en las personas, grupos y comunidades.

Esa investigación se combina en este informe para ofrecer una visión general del panorama, las tendencias y consecuencias de las actuaciones policiales «predictivas» en Bélgica, Francia, Alemania y España. También incluye otras investigaciones e informes sobre el uso de sistemas predictivos y de elaboración de perfiles en los sistemas policiales y jurídico-penales de Europa, incluidos los de Países Bajos, Italia, Suiza y Reino Unido.

En el informe, cuatro apartados examinan los sistemas «predictivos» basados en el análisis de datos que utilizan los cuerpos de policía: sistemas centrados en la ubicación, sistemas centrados en las personas, videovigilancia con IA y bases de datos. Al combinar algunos de los ejemplos más representativos de cada país, cada apartado abarca los fines, los datos utilizados y los resultados de estos sistemas.

El apartado final del informe analiza las principales preocupaciones y vulneraciones de derechos individuales, como la discriminación, criminalización, transparencia, responsabilidad e ilegitimidad.





Discriminación estructural e institucional

La mayor parte de los sistemas «predictivos» de delitos utilizan datos delictivos históricos. De esta manera, se refleja el racismo, la discriminación y los sesgos institucionales existentes en la policía y las instituciones jurídico-penales, así como en el resto de la sociedad.

Las prácticas discriminatorias de la policía de elaboración de perfiles raciales y étnicos llevan mucho tiempo recibiendo las críticas de las víctimas, asociaciones de víctimas, personas del ámbito académico, organizaciones de derechos humanos y organizaciones internacionales. Estas prácticas se traducen en intercepciones, controles de identidad y registros basados en características racializadas como el color de la piel o la (presunta) afiliación religiosa.

En 2017, un estudio realizado por la Agencia de los Derechos Fundamentales de la Unión Europea encuestó a personas de los entonces 28 Estados miembros de la UE y descubrió que casi la mitad de las personas encuestadas procedentes de una minoría étnica habían sido interceptadas por la policía. Esto incluía a personas «de origen subsahariano» en Luxemburgo y Finlandia, así como personas de «origen norteafricano» en Países Bajos y población de etnia gitana en Grecia y Portugal.¹¹

La mayoría de personas «de origen africano» interceptadas por la policía en la UE

percibieron que se debía a motivos de raza, de acuerdo con la Agencia de los Derechos Fundamentales de la Unión Europea (FRA).¹² En Francia, los hombres jóvenes percibidos como negros o árabes presentan 20 veces (un 2000 %) más posibilidades de que les intercepte la policía que el resto de la población, según el defensor del pueblo de derechos humanos del país.¹³

En Bélgica, no hay información oficial sobre la elaboración de perfiles étnicos, ya que históricamente no ha sido necesario que los equipos policiales documentasen las intercepciones y controles realizados. Sin embargo, Amnistía Internacional ha entrevistado a agentes de policía belgas que han admitido que la elaboración de perfiles raciales es una práctica existente en el cuerpo. Una persona de la policía afirmó: «Utilizo la elaboración de perfiles étnicos, pero no sé cómo podría hacer mi trabajo de otra manera. Tenemos que discriminar porque, de lo contrario, nunca atraparíamos a nadie».¹⁴

La policía española intercepta y registra de forma desproporcionada a las personas por su aspecto racial, étnico o religioso. Este hecho se ha documentado en varios estudios.¹⁵ Las personas del norte de África, el África subsahariana y los países del Este de Europa tienen más posibilidades de someterse a un control de identidad que las personas españolas.¹⁶

En Alemania, las personas de otras nacionalidades están sobrerrepresentadas entre las personas sospechosas de la policía, las condenadas por la justicia y las encarceladas.¹⁷ En Bélgica, un estudio descubrió que las personas en un proceso judicial cuyo nombre se percibía como musulmán tenían más posibilidades de ser condenadas que aquellas con un nombre belga, en igualdad de condiciones.¹⁸ En Francia, las personas extranjeras tienen tres veces más probabilidades de entrar en prisión preventiva, mientras que el 45 % de las personas en esta situación en Bélgica no son belgas.¹⁹

Pese a estas claras evidencias, la discriminación por parte de la policía, las fuerzas del orden y el sistema jurídico-penal sigue sin reconocerse aún como un problema estructural o institucional en muchos países europeos. Tal y como destacan los autores y autoras negros de Afrozensus 2020, una encuesta realizada a 6000 personas negras, africanas y afrodiaspóricas residentes en Alemania:

*«... el público general sigue preocupado de si realmente existe racismo institucional en los cuerpos de policía de Alemania o si estos son supuestamente casos aislados. Para las personas negras, africanas y afrodiaspóricas, no es solo una preocupación, sino una realidad».*²⁰

Estos datos, que representan la discriminación institucional y sistemática, se utilizan en los sistemas «predictivos», de elaboración de perfiles y evaluación de «riesgos» por parte de las autoridades policiales y jurídico-penales.

1.3. Implicación de las empresas

Las empresas privadas desempeñan un papel protagonista en la digitalización y automatización de la policía. Según los equipos de investigación de Bélgica, Francia y Alemania, son empresas de seguridad privada las que proporcionan estos sistemas a los cuerpos de policía, normalmente a través de licitaciones. Otros sistemas basados en el análisis de datos se desarrollan «internamente» o en colaboración con personal investigador del ámbito académico.

La empresa tecnológica más grande e importante que vende software policial «predictivo» en Europa es Palantir. De los 16 estados federales de Alemania, tres utilizan los sistemas de esta empresa.²¹ Los ingresos globales de Palantir en 2024 fueron de 2,87 mil millones de dólares.²² A nivel internacional, se le conoce por sus vínculos con servicios secretos, cuerpos militares y otros organismos gubernamentales.²³

Otras empresas importantes que proporcionan sistemas basados en el análisis de datos a las cuerpos policiales europeos son:

- Briefcam, una empresa israelí que ofrece videovigilancia con IA;²⁴
- ClearView, una empresa de reconocimiento facial estadounidense, proveedora de software principalmente para fuerzas del orden;²⁵
- Edicia, una empresa francesa que ha desarrollado un software de «seguridad urbana»;²⁶
- Simsi, que ha colaborado con la Universidad Rutgers de Nueva Jersey y es el proveedor comercial del modelado de riesgo territorial Risk Terrain Modelling;²⁷
- EuroCop en España, que en las últimas dos décadas ha firmado más de 100 contratos con las administraciones



públicas;²⁸

- Securitas, una empresa sueca que ofrece soluciones en materia de seguridad;²⁹ y
- SopraSteria, una empresa francesa que también tiene en vigor contratos con la UE para desarrollar uno de sus amplios sistemas de inmigración y actuación policial biométrica.³⁰

Además de Briefcam, otras empresas israelíes tienen contratos con las autoridades belgas, principalmente TA9/Rayzone y Interionet. El origen de TA9 es especialmente preocupante: su director ejecutivo antes era subdirector de la Unidad 8200, la unidad de inteligencia del ejército israelí supuestamente responsable del desarrollo de los sistemas de IA del ejército.³¹ La Unidad 8200 ha contado con varios funcionarios que posteriormente fundaron empresas de seguridad privada.³²

El sector tecnológico de vigilancia está actualmente en pleno auge.³³ Según una estimación, la tasa de crecimiento global anual es del 12,5 %, lo que se traduce en un sector con un valor de 186 mil millones de dólares en 2025.³⁴ Teniendo en cuenta lo lucrativo que es este sector, solo cabe esperar es que el número de sistemas «predictivos» y de empresas proveedoras aumenten en los próximos años.



1.4. La Ley de Inteligencia Artificial de la Unión Europea (Ley de IA de la UE)

La Ley de IA de la UE es un marco legal referente en todo el mundo para la regulación de la IA que se basa en sus posibles riesgos en cuanto a salud, seguridad y derechos fundamentales. Se aprobó en junio de 2024 tras unas negociaciones largas y complejas en el Parlamento Europeo. Los primeros elementos de la ley entraron en vigor en febrero de 2025.

La Ley de IA establece una serie de «prácticas prohibidas de la IA». Estas incluyen:

- la «actuación policial predictiva»;
- la identificación biométrica remota (como el reconocimiento facial en lugares públicos);
- la «puntuación ciudadana»; y
- el reconocimiento de las emociones.³⁵

La prohibición de la ley sobre los sistemas de «predicción» de delitos es vaga y poco clara, y contiene una gran exención que limitará considerablemente su impacto. Es posible que la ley no prohíba la gran mayoría, o incluso ninguno, de los sistemas contemplados en este informe y en su investigación subyacente.³⁶ Con respecto a los sistemas de actuación policial predictiva, prohíbe:

«... la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad».

Sin embargo, continúa diciendo:

*«... esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva».*³⁷

Al parecer, la ley prohíbe *algunos* sistemas de IA que realizan predicciones sobre personas basándose en «la elaboración de perfiles... rasgos o características de su personalidad». Sin embargo, esta prohibición no afecta a los sistemas de IA que «ayudan» al juicio humano. Esta última adición al texto provoca que la prohibición resulte inútil. Las fuerzas del orden pueden simplemente afirmar, tal y como lo hacen actualmente, que su uso de los sistemas de IA es para «ayudar» al juicio humano.

Además, el texto no hace referencia ni prohíbe claramente los sistemas de predicción de delitos centrado en la ubicación o criterios geográficos, que se utilizan de forma general en Europa. Las pautas de la Comisión Europea sobre las prácticas prohibidas en materia de IAd^e dejan claro que estas no se incluyen en el ámbito de aplicación de la prohibición.³⁸ Estas pautas son, sin embargo, no vinculantes. En caso de que haya alguna causa legal contra sistemas de este tipo, el Tribunal de Justicia de la Unión Europea (TJUE) tendrá la última palabra.

La prohibición se ha descrito como únicamente una prohibición parcial y es considerablemente más laxa que una versión original votada por el Parlamento Europeo en junio de 2023.³⁹ Los gobiernos de la UE y las grandes empresas tecnológicas han puesto un gran empeño en moderar las salvaguardas de la ley.⁴⁰

La Ley de IA contiene algunas medidas de transparencia muy básicas. Estipula que, en ciertos casos, allá donde los sistemas se clasifiquen como de «alto riesgo», habrá que informar a la ciudadanía del hecho de que se está utilizando un sistema con IA.⁴¹ Si una persona se ve afectada por una decisión basada en los resultados de un sistema de IA de alto riesgo que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener «explicaciones claras y significativas» acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones.⁴²

Sin embargo, hay una exención importante para aquellos sistemas utilizados para detectar, prevenir, investigar o enjuiciar delitos.⁴³ Esto se traduce en que no hay medidas eficaces de transparencia para los sistemas de actuación policial «predictiva» ni de «predicción» de delitos en la ley.

Además, no hay ningún mecanismo significativo que puedan utilizar las personas afectadas por una «práctica prohibida de IA» o un sistema de IA que incumpla la ley para oponerse a esos sistemas o buscar resarcimiento por los daños derivados del uso de los sistemas de IA.⁴⁴ Las personas afectadas pueden presentar una queja ante una autoridad nacional, pero la ley no obliga a dichas autoridades a ofrecer ningún tipo de compensación.⁴⁵

Existen normas en la legislación vigente sobre protección de datos, concretamente en el Reglamento General de Protección de Datos (RGPD) y la Directiva de Ámbito Penal (LED, Law Enforcement Directive). Esta última se aplica al uso de datos y sistemas automatizados de toma de decisiones por parte de las fuerzas del orden. La Directiva de Ámbito Penal prohíbe las decisiones basadas *únicamente* en el procesamiento automatizado. Por ello, al igual que lo indicado anteriormente, la prohibición podría perder su sentido. Las fuerzas del orden pueden simplemente indicar que las decisiones no se basaron únicamente en un procesamiento automatizado.



Metodología

La investigación que sirve de base para este informe la han realizado en Bélgica, Francia, Alemania y España equipos de investigación de esos países, para lo que han utilizado toda una serie de métodos con el apoyo de las personas que han editado este informe:

- **Entrevistas:** Los equipos de investigación realizaron entrevistas a personas expertas, académicas y otros/as investigadores, así como a las personas responsables del desarrollo de los sistemas automatizados de toma de decisiones y bases de datos. Asimismo, entrevistaron a agentes de policía y a otras personas funcionarias que utilizaban estos sistemas. Por último y más importante, entrevistaron y hablaron con personas y grupos afectados por estos sistemas y por la acción policial y del sistema jurídico penal en los que influían, además de con personas que trabajaban con esos grupos.
- **Solicitudes amparadas en la libertad de información:** los equipos de investigación se ampararon en las leyes de libertad de información para enviar solicitudes a cuerpos de policía nacionales y locales, a los departamentos gubernamentales y a las autoridades penitenciarias y de libertad condicional.
- **Investigación de fuente abierta:** los equipos de investigación se basaron en documentos públicos como contratos, registros financieros, informes y estudios de evaluación interna, evaluaciones de impacto, sitios web y folletos de empresas e información relacionada.
- **Revisión de la bibliografía académica:** los equipos de investigación revisaron y analizaron estudios e informes sobre estos sistemas, en concreto, estudios técnicos sobre su diseño, entrenamiento y funcionamiento.

Problemas de transparencia

Tras la investigación en todos estos países, queda claro que las autoridades policiales y jurídico-penales pretenden restringir y evitar la publicación de información sobre sistemas «predictivos», de elaboración de perfiles y evaluación de riesgos.

En todos los países, las solicitudes formales de los equipos de investigación a los departamentos gubernamentales, cuerpos de policía y autoridades locales fueron rechazadas o ignoradas (a menudo con la justificación del secreto comercial o de que suponían una amenaza para la seguridad nacional).⁴⁶ En aquellos casos en los que los departamentos gubernamentales respondieron, la información fue en general escasa y evasiva.⁴⁷ Por su parte, las empresas privadas proporcionan una amplia infraestructura y herramientas operativas a la policía. Sin embargo, no se acogen a las leyes de libertad de información.⁴⁸

En el mismo sentido, las solicitudes de entrevistas se rechazaron o ignoraron por norma general. En España, *AlgoRace* solicitó varias entrevistas a departamentos gubernamentales. Se rechazaron estas peticiones, a pesar de que estaban de acuerdo en hablar individualmente.

El nivel de transparencia en torno a estos sistemas es totalmente inaceptable, sobre todo si tenemos en cuenta las graves cuestiones técnicas, legales y políticas que plantean.





Sistemas «predictivos» centrados en la ubicación

Los métodos de actuación policial «predictiva» centrados en la ubicación se desarrollan para predecir dónde y, por lo general, cuándo se va a cometer un delito y poder asignar recursos policiales a esos lugares. Los equipos de investigación colaboradores descubrieron algoritmos de «predicción» de delitos en todos los países de estudio: Bélgica, Francia, Alemania y España.

Quienes defienden los sistemas de actuación policial «predictiva» centrados en la ubicación afirman que estos enfoques basados en el análisis de datos pueden mejorar la eficacia de la policía. Al identificar los lugares que suponen las mayores amenazas, la policía puede evitar que se cometan delitos. Este enfoque se ha resumido de la siguiente forma:

«Si la policía puede centrar sus recursos en estas personas, lugares y momentos peligrosos, serán más eficaces a la hora de reducir la criminalidad en sus jurisdicciones».⁴⁹

En Europa, los equipos de investigación han identificado dos tipos principales de sistemas centrados en la ubicación:

- algoritmos de predicción de «puntos críticos» de delincuencia que se basan en datos policiales históricos para prever futuros escenarios donde se cometerán delitos; y
- algoritmos de predicción de «riesgos», que se basan en la suposición de que los factores ambientales pueden determinar el lugar en el que se producirá un delito.

Ambos métodos suscitan preocupación por dirigirse y criminalizar de forma desproporcionada a las personas y comunidades de minorías raciales y de bajos ingresos.

Los ejemplos presentados en este informe demuestran que la actuación policial predictiva centrada en la ubicación puede conllevar graves consecuencias para las personas que viven y trabajan en zonas etiquetadas como de «alto riesgo». Pueden enfrentarse a una mayor vigilancia y seguimiento policial, controles de identidad y documentación de vehículos, registros, interrogatorios o, incluso, arrestos.

Pese a que la Ley de IA de la UE incluye una prohibición nominal de ciertos tipos de sistemas de actuación policial «predictiva», conforme a las directrices oficiales, no afecta a los sistemas «predictivos» centrados en la ubicación.⁵⁰ La investigación deja patente el potencial de estos sistemas para la discriminación y la elaboración de perfiles. Por ello, deben incluirse en cualquier prohibición significativa de las actuaciones policiales predictivas.

Este informe solo ofrece una visión general de los sistemas de «predicción» geográfica de delitos que utilizan las fuerzas policiales en Europa. Además de los sistemas de Francia, Bélgica, Alemania y España, también hay ejemplos similares en Italia, Suiza y Reino Unido (según una investigación anterior).

Predicción de «puntos críticos» de delitos

En Bélgica, Francia, Alemania y España, los sistemas centrados en la ubicación utilizan principalmente métodos de predicción de «puntos críticos» de delitos. Gracias a ellos, las estadísticas históricas de delitos que muestran cuándo y dónde se han producido delitos se utilizan para «predecir» futuros lugares o «puntos críticos» donde se van a cometer delitos.

Los equipos de investigación identificaron, al menos, nueve sistemas de predicción de «puntos críticos» diferentes. Muchos de estos sistemas se están implementando en varios cuerpos de policía de cada país.

En Alemania:

- la policía de Berlín está implementando una estrategia para clasificar los *kriminalitätsbelastete Orte* (kbOs) o «lugares afectados por delitos», en los que se

pueden ampliar las competencias policiales.⁵¹

- Tres estados federales alemanes están utilizando los sistemas de «puntos críticos» de delitos, frente a los seis estados que utilizaban cinco sistemas diferentes en 2018.⁵² Estos sistemas son:
 - SKALA (*System zur Kriminalitätsauswertung und Lageantizipation*, Sistema de análisis de delitos y anticipación de la situación) en Renania del Norte-Westfalia;
 - KrimPro (*Kriminalitätsprognose Wohnraumeinbruch*, Previsión criminal de robos con allanamiento) en Berlín; y
 - KLB-operativ (*Kriminalitätslagebild*, Concienciación sobre la situación criminal) en Hesse;⁵³ y
 - la policía de Baviera ha utilizado el Sistema de observación precriminal (PRECOBS).⁵⁴

En España, se utilizan los sistemas «predictivos» centrados en la ubicación de forma generalizada:

- a nivel nacional se utiliza el sistema «Predictive Police Patrolling» (P3-DSS) para asignar a las unidades policiales un área de patrulla;⁵⁵ y
- siete comunidades están utilizando un sistema de EuroCop, entre ellas, casi todos los cuerpos policiales de Madrid.⁵⁶

En Francia y Bélgica, los equipos de investigación encontraron menos ejemplos activos de métodos de actuación policial con «puntos críticos». En Francia, *La Quadrature du Net* identificó PredVol y PAVED, ambos utilizados por la Gendarmería Nacional pero que se han retirado desde entonces.⁵⁷

En Bélgica, *TechnoPolice* identificó un pequeño ensayo por parte de la policía de Westkust y el uso de un sistema de información geográfica producido por la empresa Orbit, en Flandes y Bruselas.⁵⁸ Según Orbit, su software se encuentra «implementado en casi 100 zonas policiales».⁵⁹

Los sistemas de predicción de «puntos críticos» de delitos han recibido críticas a nivel internacional tras el escrutinio del sistema PredPol en EE. UU. por reforzar y perpetuar los sesgos raciales.⁶⁰

Los sistemas incluidos en este informe, algunos de los cuales utilizan métodos muy similares a PredPol, también suscitan preocupación por la discriminación y criminalización que plantean. En los cuatro países, las zonas etiquetadas como de «alto riesgo» por los sistemas de «puntos críticos» de delitos suelen ser zonas en las que viven y trabajan las comunidades marginadas.

Objetivos

Según la policía, el cálculo estadístico de la predicción de los «puntos críticos» de delitos les permite reducir las tasas de criminalidad. Florian Gauthier, el científico de datos francés que diseñó PredVol, justifica la necesidad de los «puntos críticos» para predecir el robo de coches, señalando las discrepancias entre los lugares por los que patrulla la policía y los lugares en los que se producen los robos. Estas discrepancias, según él, se pueden reducir al utilizar datos de los delitos para guiar a las patrullas de agentes.⁶¹

Presuntamente, los métodos «basados en evidencias» como este permiten enviar a las patrullas policiales al lugar correcto en el momento correcto y así frustrar la actividad delictiva antes de que ocurra. En Alemania, la policía de Berlín afirma que la designación de un área como kbO aumenta la «sensación de seguridad», ya que permite a la policía «controlar la identidad de las personas relevantes, aumentar la posibilidad de detección y, por tanto, evitar delitos».⁶²

Muchos de los sistemas de actuación policial basados en «puntos críticos» son para presuntos robos o robos con allanamiento:

- en Francia, PredVol se utiliza para los presuntos robos de vehículos y PAVED⁶³ para robos de vehículos y robos con allanamiento;
- en Alemania, el sistema PRECOBS se centra en los presuntos robos de vehículos y robos con allanamiento, mientras que el sistema KbO se centra en los atracos, entre otros delitos;⁶⁴ los equipos de investigación han sugerido que los sistemas de «puntos críticos» para los hurtos se introdujeron en la década de 2010 como respuesta al miedo sembrado por los medios de comunicación por los robos con allanamiento;⁶⁵
- en Bélgica, los sistemas «predictivos» de la policía local de Westkust se centran en los robos con allanamiento y de vehículos,⁶⁶ y
- en España, el sistema EuroCop intenta «predecir» robos, entre otros delitos.⁶⁷

Datos utilizados

Los sistemas de predicción de «puntos críticos» de delitos se alimentan de datos y tendencias estadísticos de una gran cantidad de datos delictivos, normalmente de bases de datos de la policía, para prever donde se van a cometer futuros delitos.

En Alemania, el modelo de predicción de «delitos» centrado en la ubicación de los kbO (*Kriminalitätsbelastete Orte*, lugares afectados por delitos) utiliza una evaluación estadística que incluye datos sobre delitos y otros datos adicionales no especificados.⁶⁸

En Bélgica, el sistema de información geográfica de Orbit, que al parecer utilizan

más de 100 cuerpos de policía local, usa informes históricos de la policía sobre delitos para identificar futuros «puntos críticos» de delitos.⁶⁹ El sistema del cuerpo de policía local de Westkust también usa datos de la policía sobre presuntos delitos, matrículas, documentación de los tribunales o incluso el clima.⁷⁰

En Francia, el sistema PredVol se basa en datos sobre robos de vehículos procedentes de los sistemas informáticos utilizados para registrar todas las denuncias e informes, incluidos:

- coordenadas XY en las que se robó el vehículo;
- fecha; e
- información adicional sobre el modelo y color del vehículo.⁷¹

En España, el sistema EuroCop puede utilizar e integrar varias fuentes de información, incluidos datos y archivos de delitos de la policía, datos socioeconómicos y datos de videovigilancia. Estos datos se combinan en un modelo algorítmico para «predecir» delitos y generar «mapas de calor» y «rutas de patrulla» para la policía.⁷²

Preocupa seriamente que los datos históricos de la policía utilizados en los sistemas de «puntos críticos» de delitos provoquen una discriminación injusta. Tal y como se explicará más adelante, los datos históricos de delitos reflejan la sobrevigilancia y criminalización de las comunidades racializadas y de bajos ingresos. Los algoritmos de «puntos críticos» de delitos trasladan esta desproporcionalidad y discriminación a las futuras predicciones.

De hecho, el ministro de Interior belga reconoció en junio de 2020: «Las estadísticas policiales son, ante todo, un reflejo de la actividad del cuerpo. No reflejan la realidad de la delincuencia en una zona concreta».⁷³

Muchos sistemas de «puntos críticos» utilizan, además, datos sociodemográficos en sus datos de aprendizaje. El desarrollador de PredVol contó a *La Quadrature du Net*



que el sistema utilizaba 600 variables demográficas. Estas incluían la escolarización y las tasas de desempleo, el número de tiendas cercanas y la media de edad de la población. Las autoridades no facilitaron información más amplia.⁷⁴ Asimismo, descubrieron que PAVED, de las 15 variables sociodemográficas, se basaba en el sexo, la nacionalidad y los datos de inmigración, los ingresos familiares y el nivel de estudios.⁷⁵

El sistema de patrulla inteligente «Smart Patrolling» P3DSS del Cuerpo Nacional de Policía de España también utilizaba datos sobre la nacionalidad y dividía a las personas residentes en Madrid en los siguientes grupos: personas españolas, personas de otros países de la UE, personas de fuera de la UE y, de forma inusual, personas clasificadas por continente.⁷⁶ A continuación, el sistema calculaba para cada grupo de nacionalidad un «objetivo de contacto policial»: la cantidad de tiempo de patrulla que debía asignarse a cada grupo en función de su tamaño en relación con el territorio geográfico.⁷⁷ Estos grupos demográficos, pese a ser extremadamente generalizados, son básicamente sustitutos de los grupos raciales.

Los datos sobre nacionalidad, situación migratoria y género se consideran o pueden considerarse «categorías especiales» de datos.⁷⁸ Estas y otras variables sociodemográficas corren el riesgo de establecer correlaciones entre la criminalidad y la raza o dificultad económica. La ley de protección de datos de la UE lo deja claro:

*«La elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en datos personales que sean, por su naturaleza, especialmente sensibles en relación con los derechos fundamentales y libertades quedará prohibida».*⁷⁹

Conforme a estos datos introducidos, los sistemas de «puntos críticos» utilizan análisis estadísticos para predecir la probabilidad de futuros lugares donde se cometerán delitos. Las técnicas de modelización específicas para realizar estos análisis geográficos y temporales difieren según el sistema.

PAVED y PredVol utilizan técnicas de aprendizaje automático, lo que significa que los sistemas «aprenden» automáticamente de otros datos, sin que haya que entrenarlos manualmente. La mayoría del resto de sistemas de «puntos críticos» identificados en Bélgica, Francia, Alemania y España utilizan métodos algorítmicos.

Resultados

Por norma general, los sistemas predictivos de «puntos críticos» ofrecen a la policía un «mapa de calor» para identificar las áreas o lugares en los que presuntamente existe un alto riesgo de que se produzca un delito. Por ejemplo, PRECOBS en Alemania muestra un mapa con zonas marcadas en distintos colores. Esos colores representan la supuesta probabilidad o niveles de riesgo de que se cometa un delito en esa zona (véase la figura 1).

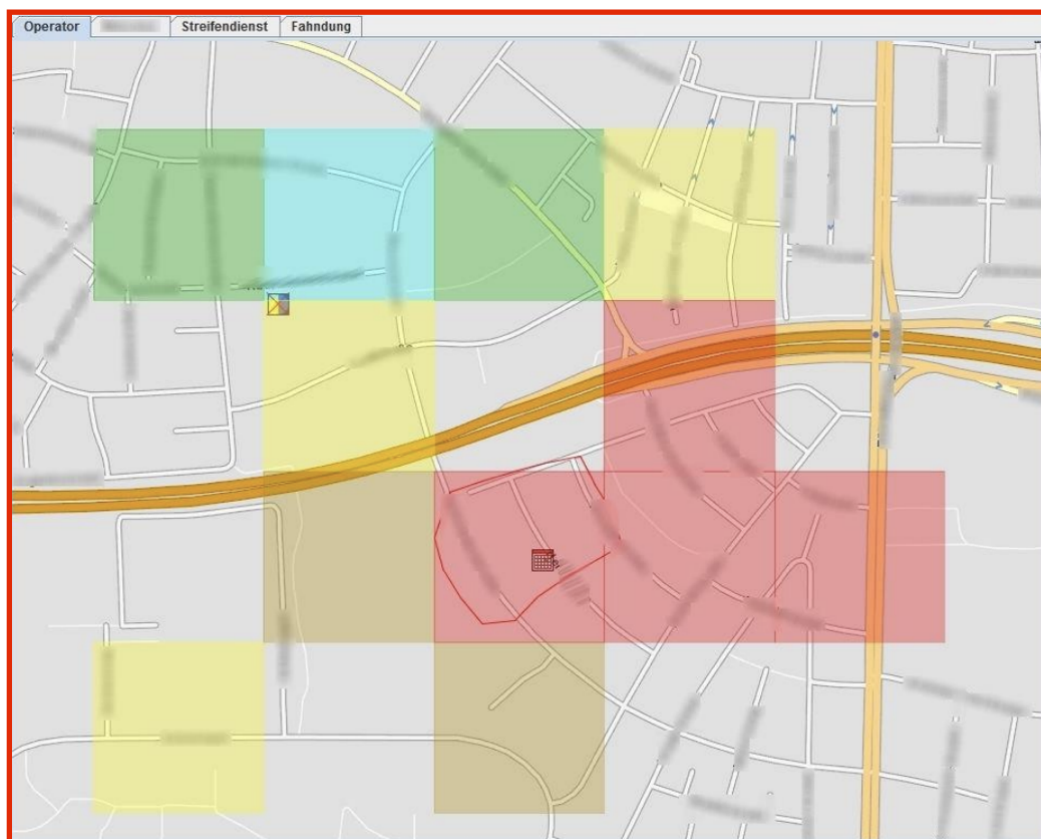


FIGURA 1: CAPTURA DE PANTALLA DEL MAPA DE COLORES DE PRECOBS DE UN LUGAR.
CRÉDITOS: SONJA PETERANDERL

Algunos sistemas, como PredVol en Francia, son accesibles «sobre el terreno» para que el personal policial pueda consultarlos en tabletas. A otros sistemas, como PAVED, solo puede acceder el personal de mando. Además de los «mapas de calor», PAVED también presenta al personal policial histogramas que muestran las variables sociodemográficas consideradas los indicadores más influyentes de la delincuencia (véase la figura 2).

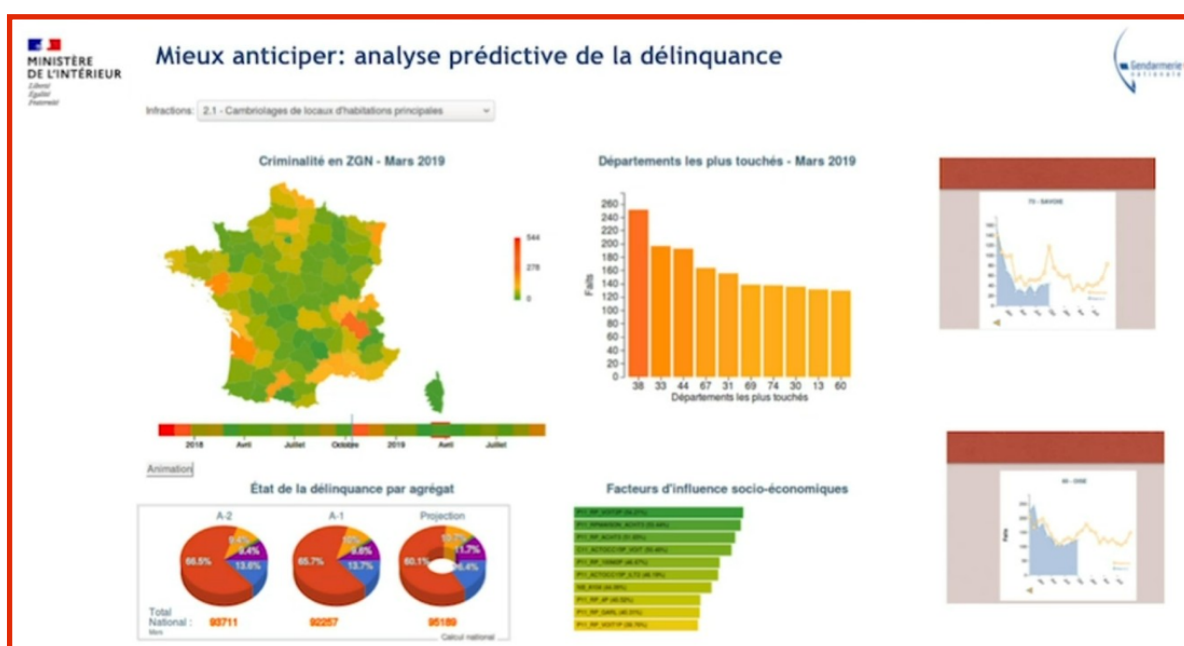


FIGURA 2: CAPTURA DE PANTALLA DE LA CHARLA QUE DIO EL CORONEL PATRICK PERROT, COLLOQUE DE L'INSTITUT DE DROIT PRIVÉ—UT CAPITOLE, EL 8 DE SEPTIEMBRE DE 2021 (FUENTE: «AI ET ENJEUX DE SÉCURITÉ» EN EL MINUTO 23 SEGUNDO 10).

Los sistemas de predicción de «puntos críticos» de delincuencia se utilizan para asignar los recursos policiales y determinar el momento y el lugar en el que deben patrullar sus agentes. Los resultados en las zonas de los «puntos críticos» pueden incluir:

- vigilancia;
- recopilación de información;
- controles de identidad;
- interrogatorios;
- registros;
- órdenes de alejamiento; o
- arrestos.⁸⁰

La designación de zonas de «puntos críticos» también podría ampliar las competencias de la policía en esos lugares. En Berlín, la policía tiene potestad legal para llevar a cabo controles de identidad o registros a personas u objetos en los denominados «kbOs», sin que sea necesaria una sospecha concreta, en lugar de «en función del comportamiento».⁸¹

Del mismo modo, *La Quadrature du Net* habló con una fuente que explicó que los «puntos críticos» generados por PAVED se utilizaban para persuadir a los fiscales a que autorizasen órdenes especiales para realizar controles de identidad y vehículos en esos lugares. De este modo, la policía administrativa podía utilizar los poderes de la policía judicial, lo que constituía una grave violación de las obligaciones de la policía administrativa.⁸²



Impacto

Los lugares calificados como «puntos críticos» de la delincuencia por los sistemas algorítmicos son en su mayoría zonas o barrios donde viven y trabajan comunidades de bajos ingresos y racializadas. La experta en derecho Lina Schmid destaca que los lugares clasificados como «kbOs» suelen estar frecuentados por una alta proporción de personas percibidas como migrantes.⁸³

Tras la introducción del sistema PRECOBS en Baviera, Matthias Monroy, redactor de la revista sobre derechos civiles alemana *Bürgerrechte & Polizei* (Derechos civiles y policía) dijo:

*«¿A quién para más a menudo la policía cuando cree que habrá un robo con allanamiento en las próximas horas o días? Yo diría que, lo más probable, es que sea a personas que lleven una vestimenta desaliñada, de distinto color de piel o que lleven capucha, patrones que ya se siguen en la policía actualmente».*⁸⁴

En Alemania, los controles por parte de la policía debido a la raza están prohibidos constitucionalmente (Artículo 3 del *Grundgesetz* o Ley Fundamental de la República Federal de Alemania). No obstante, Lina Schmid explica que designar ciertas zonas como «puntos críticos» permite a la policía saltarse esta prohibición:

*«La criminalización aquí (en lugar de a grupos racializados de personas, como suele suceder con la elaboración de perfiles raciales) afecta a lugares enteros y a las personas que los frecuentan. Esto abre la puerta a que la policía pueda elaborar perfiles raciales de forma soterrada porque, aunque se supone que todo el mundo es susceptible de estos controles, la realidad es que afecta principalmente a BIPoC (personas negras, indígenas y de color, por sus siglas en inglés)».*⁸⁵

Según la iniciativa vecinal *Wrangelkiez United*, los controles realizados en los kbO de Görlitzer Park/Wrangelkiez afectan casi exclusivamente a personas negras y de minorías raciales, «independientemente de lo que estén haciendo o adónde se dirijan».⁸⁶ Se somete a controles al alumnado de una escuela de idiomas del barrio cuando van a clase, y los hombres negros también suelen ser sometidos a controles en el parque, tal y como se denuncia en las entrevistas en vídeo con *Wrangelkiez United*:

*«Cuando está la policía (...), la gente de piel oscura como yo tiene que someterse a controles sin motivo real, no es que hayamos cometido ningún delito. Es solo por nuestro aspecto».*⁸⁷

Predicción de «riesgos»

En Europa, los sistemas centrados en la ubicación también incluyen sistemas de predicción de «riesgos» que utilizan datos ambientales o contextuales para identificar lugares supuestamente más propensos a la delincuencia.

Estos sistemas de predicción de «riesgos» con carácter medioambiental se basan en la teoría criminológica de las «ventanas rotas». Esta teoría argumenta que el entorno físico es un factor determinante a la hora de cometer un delito. La propusieron James Wilson y George Kelling en EE. UU. en 1982.⁸⁸ La teoría formula hipótesis en torno a los factores ambientales (como las ventanas rotas) como indicadores o efectos disuasorios de la criminalidad.

Las actuaciones policiales basadas en el principio de las «ventanas rotas» se introdujo posteriormente en EE. UU. Un ejemplo que se suele citar mucho es el de los cambios introducidos por el anterior comisario del Departamento de Policía de Nueva York, William Bratton.⁸⁹ Este modelo ha servido de inspiración para el diseño y desarrollo de métodos de actuación policial basados en el análisis de datos, pese a contar con el descrédito general de profesionales de la criminología y de la sociología.⁹⁰

Al igual que sucede con los algoritmos basados en los «puntos críticos» de delincuencia, los algoritmos de «riesgos» ambientales pueden dirigir a la policía a zonas en las ciudades cuya población presenta dificultades económicas y, con más probabilidad, habitadas y frecuentadas por comunidades racializadas.

Objetivos

Los cuerpos de policía de Bélgica y Francia están utilizando un modelo algorítmico llamado «Risk Terrain Modelling» (modelado de riesgo territorial) para predecir delitos o el nivel de criminalidad, lo que incluye evaluar los «riesgos» ambientales. Se conocen otros usos por parte de la policía en el Reino Unido⁹¹

La metodología de modelado de riesgo territorial (RTM, por sus siglas en inglés) la desarrollaron Joel Caplan y Leslie Kennedy, dos investigadores de la Universidad Rutgers de Nueva Jersey, EE. UU. Presuntamente, se ha probado en más de 45 países en seis continentes. Su sitio web, que anuncia el software producido por la empresa Simsi, declara:

«Lo que hace el modelado de riesgo territorial (RTM) es identificar los riesgos procedentes de las características de un entorno y modelar cómo se combinan para crear entornos de comportamiento únicos para cometer un delito.

Probablemente, te vendrá a la cabeza el cliché de un callejón oscuro al pensar en un posible escenario de un delito. En este caso, estás teniendo en cuenta

*al menos dos atributos del entorno: (1) un callejón y (2) una mala iluminación. Se considera que el riesgo de que se produzca un delito en entornos en los que estas características concretas coexistan es extremadamente alto».*⁹²

El sitio web distingue el modelado de riesgo territorial de los métodos de predicción de «puntos críticos» de delitos de la siguiente forma:

*«Los puntos críticos te indican dónde se concentra la delincuencia, pero no necesariamente los motivos para ello. Con demasiada frecuencia, la gente se centra en los puntos críticos sin tener en cuenta las características especiales que hacen que estos lugares sean propicios en primer lugar... Los puntos críticos no son más que los síntomas de los lugares que son muy favorables para la delincuencia. El modelado de riesgo territorial lleva este análisis más allá con el diagnóstico espacial».*⁹³

Actualmente, este sistema se utiliza en Zennevallei (Bélgica) y París (Francia). La *Direction de la Sécurité de Proximité de l'Agglomération Parisienne* (DSPAP o División de Seguridad Local del Área de París) comenzó a utilizar el algoritmo con un geoestadístico del antiguo *Observatoire National de la Délinquance et des Réponses Pénales* (ONDRP u Observatorio Nacional de Criminalidad y Respuestas Penales),⁹⁴ que había trabajado varios años con la Universidad de Rutgers y que afirmaba:

*«Llevo utilizando el algoritmo del RTM (modelado de riesgo territorial) más de ocho años... Ahora es una aplicación web, mucho más potente que antes, pero se basa en el mismo principio: va en consonancia con la prevención situacional de delitos, lo que significa que identificamos los elementos contextuales y ambientales que provocan la comisión de delitos... Así que al analizar un entorno e identificar los factores que agravan el riesgo, podemos predecir lo que podrá suceder en un entorno similar».*⁹⁵

En Zennevallei, se utiliza para fines similares. Aquí, el programa lo lidera Anneleen Rummen, una estudiante de doctorado de la Universidad de Gante, bajo la supervisión del profesor de criminología Wim Hardyns.⁹⁶

Existen otros sistemas de predicción de «riesgos» ambientales que no utilizan el algoritmo del RTM. Por ejemplo, MapRevelation y el «módulo predictivo» del sistema Smart Police de Francia. MapRevelation fue uno de los primeros sistemas de actuación policial «predictiva» implementados en Francia. Comercializado por la empresa Sûreté Globale,⁹⁷ lo utilizan las autoridades locales y cuerpos de policía local de Montpellier, Lyon, Lille, Villeurbanne, Montauban, Angers, Colombes y Melun Val de Seine.⁹⁸

Datos utilizados

El sistema RTM utiliza varios «factores de ponderación» que alimentan al modelo final. Estos factores pueden ajustarse al caso de uso concreto del modelo. El algoritmo asigna un valor de vulnerabilidad a los lugares según factores espaciales, como por ejemplo:

- si el lugar está bien iluminado;
- estaciones de metro o autobús;
- terrazas de cafeterías;
- locales de comida rápida;
- baños públicos;
- farmacias;
- tiendas de comestibles;
- bares;
- árboles y bancos;
- algunos tipos de comercios;
- colegios;
- oficinas de correos.

En el sitio web del modelado de riesgo territorial (Risk Terrain Modelling), algunos ejemplos de otros factores incluyen: «drogas», «edificios vacíos» y «bandas».⁹⁹

En París, el sistema RTM se alimenta de datos del software de redacción de procesos de la Policía Nacional (LRPPN o *Logiciel de Rédaction des Procédures de la Police Nationale*). Deduce las correlaciones entre delitos y los denominados factores ambientales. En 2018, Jean-Luc Besson, responsable del Departamento Geoestadístico del ONDRP, definió los factores que podrían utilizarse en el modelo parisino:

«Si observamos los atracos que tienen lugar cerca de cajeros automáticos, nos preguntaremos: ¿los cajeros más afectados abren las 24 horas? ¿Están cerca de un cruce o una estación de tren, etc.?»,¹⁰⁰



Los equipos de investigación no pudieron obtener información precisa sobre todas las variables utilizadas en los sistemas de modelado de riesgo territorial de París y Zennevallei. Sin embargo, se sabe que el modelo de Zennevallei utiliza factores como las condiciones meteorológicas durante eventos específicos.¹⁰¹

En Francia, supuestamente MapRevelation se ha entrenado con una base de datos de «terrorismo» con el objetivo de «predecir» ataques.¹⁰² También se ha alimentado de datos de los cuerpos de policía local que usan el sistema.

El «módulo predictivo» de Smart Police, desarrollado por la empresa francesa Edicia, utiliza técnicas de aprendizaje automático. Se alimenta tanto con datos operativos de la policía (por ejemplo, expedientes, infracciones, situación del personal policial y vehículos) y datos urbanos (por ejemplo, datos ambientales y climatológicos, eventos locales y nacionales, datos sociodemográficos y electorales).

El módulo «predictivo» de Smart Police obtiene también, supuestamente, información de redes sociales y otros colaboradores. Estos colaboradores incluyen personal de dirección de un colegio y personas arrendadoras de vivienda pública, así como información de primera mano de agentes de policía.¹⁰³ Con ello, se corre el riesgo evidente de codificar rumores, habladurías y opiniones no verificadas en sistemas algorítmicos, disfrazándolos con un velo de objetividad técnica.

Resultados

Resulta complicado encontrar información conclusiva sobre los resultados de los sistemas de predicción de «riesgos» ambientales utilizados en Bélgica y Francia debido al secretismo que rodea a los cuerpos de policía y organismos gubernamentales.

Conforme a una fuente contactada por *La Quadrature du Net*, no hay pruebas conclusivas de que el sistema de modelado RTM reduzca las tasas de criminalidad en Francia. Esta fuente también afirmó que esta metodología permite a las instituciones que la utilizan evadir el debate sobre las causas estructurales del delito.¹⁰⁴ Surge un problema similar con otros sistemas de predicción de «puntos críticos» de delitos.

Otros sistemas de «predicción» de delitos centrados en la ubicación que se utilizan en Europa

Además de los sistemas detallados anteriormente en Bélgica, Francia, Alemania y España, otros cuerpos de policía de Europa también están utilizando sistemas de actuación policial «predictiva» centrados en la ubicación.

En Reino Unido, *Amnesty International UK*, la filial de Amnistía Internacional en Reino Unido, detectó que casi tres cuartas partes de los cuerpos de policía utilizaban sistemas de actuación policial «predictiva», de los cuales 32 de 46 utilizaban sistemas de «predicción» de delitos centrados en la ubicación.¹⁰⁵ *Aministía* investigó el uso por parte de los cuerpos de policía de Reino Unido del RTM y descubrió que su utilización por parte de la Policía Metropolitana de Londres «contribuye y refuerza la elaboración de perfiles raciales y las actuaciones policiales discriminatorias».¹⁰⁶ El análisis demográfico de las zonas señaladas como de «alto riesgo» por el algoritmo del RTM muestra que:

*«... aquellas zonas en las que el sistema de modelado de riesgo territorial (Risk Terrain Modelling) predijo que iban a producirse episodios graves de violencia se corresponden significativamente con las zonas en las que hay mayor población de residentes con dificultades económicas de raza negra procedentes de África, de raza negra procedentes del Caribe, asiáticos de Bangladesh y de Pakistán».*¹⁰⁷

El Dr. Adam Elliott-Cooper, investigador y autor de *Black Resistance to British Policing* (Resistencia negra a la actuación policial británica), al reflexionar sobre el uso de los factores de «riesgo» ambientales para «predecir» delitos, afirmó:

*«No deberíamos sorprendernos de que el tipo de edificios al que va a ir la policía no van a ser chalés adosados con una valla blanca de madera. Serán los barrios de protección oficial, las zonas urbanas del interior de las ciudades en las que haya más presencia policial, no en las prósperas zonas de las afueras, ¿verdad? Así que veremos cómo este enfoque supuestamente geográfico y, por tanto, enfoque de actuación policial supuestamente más científica y objetiva, en realidad simplemente está reproduciendo estos problemas existentes».*¹⁰⁸

En Países Bajos, la policía ha estado utilizando el «Sistema de anticipación de delitos». Este sistema de predicción de «puntos críticos» originalmente se alimentaba de puntos de datos, como por ejemplo, cuántas personas «no occidentales» con al menos un progenitor extranjero vivían en una zona. Aunque estos puntos de datos se eliminaron posteriormente, el sistema siguió utilizando datos delictivos históricos e indicadores sobre raza y clase, como los datos de ingresos y renta.¹⁰⁹

La policía italiana antes utilizaba «Delia», un sistema desarrollado por una empresa llamada KeyCrime. Este sistema cuenta con funciones de «predicción» de delitos con criterios geográficos e individuales. Supuestamente, es uno de los primeros ejemplos del mundo de software de actuación policial «predictiva» disponible comercialmente. Su andadura comenzó en 2008.¹¹⁰ Sin embargo, KeyCrime ha entrado en proceso de quiebra, lo que achacan a la incertidumbre financiera provocada por la llegada de la Ley de IA de la UE y la posibilidad de que el sistema se pueda prohibir en un futuro.¹¹¹

No obstante, en Italia sigue utilizándose un sistema llamado XLAW.¹¹² XLAW es un sistema de predicción de «riesgos» con criterios ambientales (similar a los sistemas de modelado de riesgo territorial utilizados en Francia, Bélgica y Reino Unido). Los factores de predicción espacio-temporales del sistema incluyen: grandes espacios, lugares de pagos de prestaciones a final de mes, hora de cierre de las tiendas, llegadas de trenes y barcos, y variaciones climatológicas.¹¹³

En algunos cantones suizos, la policía ha estado utilizando PRECOBS (el mismo sistema que se utiliza en Alemania).¹¹⁴





Sistemas de elaboración de perfiles y «predictivos» de delitos centrados en las personas

Las herramientas de «predicción» de delitos centrados en las personas se diseñan para predecir la probabilidad o el «riesgo» que tiene una persona de cometer ciertas acciones, en concreto aquellas definidas por la ley como delitos. En lugar de centrarse en una ubicación específica, lo hacen en personas específicas.

La autoridades policiales y del sistema jurídico-penal utilizan estos sistemas para intentar elaborar un perfil, «predecir» o evaluar el «riesgo» de que una persona cometa un delito o lleve a cabo una conducta delictiva. Otros sistemas intentan evaluar las probabilidades de que alguien pueda ser víctima de un delito, por ejemplo, en el caso de la violencia de género. También se han utilizado para detectar denuncias de delitos presuntamente falsas.

Las personas a las que se dirigen estos sistemas están sometidas al análisis de los datos que las caracterizan, su pasado y presente, y sus relaciones. El objetivo es determinar y «predecir» su comportamiento, «riesgo» o supuesta «criminalidad».

Las consecuencias pueden ser graves. Estos sistemas pueden provocar la vigilancia

o el control de las personas, que podrían enfrentarse a más intercepciones de la policía, interrogatorios, registros o visitas en el domicilio o en el lugar de trabajo. El uso de estos sistemas puede conllevar la detención, el arresto o la deportación.

Estas herramientas también se utilizan en el sistema jurídico-penal. Pueden influir al personal judicial a la hora de tomar decisiones, por ejemplo, con las sentencias. Asimismo, pueden influir en la duración de las penas de cárcel de una persona y su puesta en libertad, así como en las condiciones en las que se encuentran.

Objetivo

Los sistemas «predictivos», de elaboración de perfiles y de evaluación de «riesgos» centrados en las personas se utilizan con fines muy diversos. Algunos cuerpos utilizan programas informáticos de extracción y análisis de datos para recopilar y cotejar datos, evaluar patrones y utilizarlos para «predecir» futuros patrones.

En Alemania, tres estados federales disponían de licencias de programas de análisis y extracción de «macrodatos» basados en el software Gotham desarrollado por la empresa tecnológica de EE. UU. Palantir. Como muchas otras empresas que desarrollan y venden tecnología a la policía, Palantir mantiene un gran secretismo sobre su tecnología y los contratos que firma.

La policía del estado de Hesse en Alemania utiliza un sistema con la tecnología de Palantir llamado *hessenDATA* para crear amplios perfiles individuales de las personas. El sistema muestra un registro de información conocida sobre una persona, que incluye; cuándo y dónde ha sido interceptada por la policía, registro de detenciones, si alguna vez se le han incautado drogas y su domicilio.

En Bélgica, un sistema utilizado por la Policía Nacional belga llamado «i-Police» ofrece múltiples funciones, entre ellas:

- análisis y «predicción» de patrones;
- predicción de futuros delitos con fines «preventivos»;
- posibilitar el seguimiento y vigilancia;
- la asignación de patrullas policiales, intercepciones y registros;
- y otras formas de intervención y aplicación de la ley.¹¹⁵

La policía belga también ha elaborado perfiles de personas y grupos y los ha incluido en bases de datos específicas, un asunto tratado con más profundidad más adelante. Esto incluye el uso de estas bases de datos para las llamadas «bandas urbanas», un término

plagado de racismo.¹¹⁶ Las personas perfiladas como supuestas integrantes de «bandas» han sido objeto de seguimiento, vigilancia y un mayor número de intercepciones y registros.¹¹⁷

Las herramientas de evaluación de «riesgos», elaboración de perfiles y «predicción» de delitos de las personas se han introducido en Alemania para evaluar el supuesto futuro riesgo que suponen las personas denominadas terroristas islámicos¹¹⁸ o defensoras del terrorismo. La Oficina de la Policía Criminal Federal ha desarrollado dos herramientas de evaluación de «riesgos» individuales llamadas RADAR (Análisis basado en las reglas de delincuentes potencialmente peligrosos para la evaluación de riesgos graves).

Una de las versiones, RADAR-iTE, es una herramienta que se utiliza para analizar y elaborar perfiles de las personas denominadas «islamistas». La Policía Federal belga también ha afirmado que utiliza una herramienta similar a RADAR-iTE.¹¹⁹ La otra herramienta, RADAR-rechts, la utiliza la Oficina de la Policía Criminal Federal de Alemania para elaborar perfiles de personas con ideas de extrema derecha que se consideran una amenaza violenta. Esta autoridad también está desarrollando otra herramienta, RADAR-Haft («RADAR-detención») para evaluar lo propensa que es una persona encarcelada a la violencia antes de su puesta en libertad.

El objetivo de RADAR-iTE y RADAR-rechts consiste en evaluar principalmente el riesgo de aquellas personas identificadas previamente como «Gefährder» (peligrosas). Se trata de una clasificación de las amenazas desarrollada por las fuerzas del orden alemanas que se ha exportado al resto de la UE.¹²⁰ El término es confuso y está abierto a interpretaciones subjetivas. Los sistemas también se utilizan para evaluar a las «personas relevantes», otra categoría poco clara y subjetiva. La elaboración de perfiles de riesgo se usa para evaluar y priorizar a las personas de «alto riesgo» para luego intervenir y aplicar la ley.¹²¹

En España, VioGén es uno de los sistemas de evaluación de riesgos individuales más reconocidos. Su objetivo es evaluar el riesgo de violencia de género de una persona que haya denunciado un incidente. Esta evaluación determina la actuación de la policía.¹²²

La policía española también ha utilizado un tipo de sistema «predictivo» menos habitual. VeriPol es un sistema algorítmico que utiliza la Policía Nacional española para detectar presuntas denuncias falsas. Utiliza las técnicas de procesamiento de lenguaje natural para analizar los textos de denuncias de atracos, robos de carteristas y tirones de bolsos. Supone un eficaz detector de mentiras. Se creó para prevenir denuncias falsas fraudulentas. El objetivo principal es ofrecer a la policía una rápida evaluación sobre si una denuncia es potencialmente falsa.¹²³ En marzo de 2025, se anunció que la Policía Nacional había dejado de utilizar VeriPol. El Ministerio del Interior de España aclaró que se debía a que el sistema carecía de validez en los procesos legales.¹²⁴

Las autoridades en materia de seguridad de todo el mundo, incluidas las de Europa,

cada vez están analizando más los «registros de nombres de los pasajeros» (PNR, por sus siglas en inglés). Se trata de datos personales recopilados por las aerolíneas con fines comerciales cuando una persona reserva un vuelo.¹²⁵ Los datos de los PNR se cruzan con las bases de datos de la policía y otros organismos públicos. Los algoritmos se utilizan sistemáticamente en busca de patrones en estos datos conforme a criterios predeterminados.¹²⁶ Los sistemas de este tipo acaban con la presunción de inocencia y convierten a cualquier persona usuaria del transporte aéreo en sospechosa.¹²⁷ La UE está planeando ampliar su uso a otros métodos de transporte, en primer lugar al transporte marítimo.¹²⁸

En las cárceles españolas, se utiliza un sistema llamado DRAVY para intentar identificar a las personas presas que presuntamente están viviendo un proceso de la denominada radicalización «yihadista».¹²⁹ Como el objetivo principal de DRAVY es evaluar la radicalización «yihadista», resulta discriminatorio, ya que se centra casi exclusivamente en personas musulmanas y con raíces musulmanas. El sistema está configurado para centrarse en el «yihadismo», un término que, por sí solo, se basa en estereotipos occidentales discriminatorios.

En las cárceles españolas, también se usa una herramienta similar, RisCanvi, para «predecir» el riesgo de reincidencia. Se utiliza para tomar decisiones con respecto a la libertad condicional, los permisos penitenciarios y la categorización de las personas presas.¹³⁰

Datos utilizados

Estos sistemas funcionan, se entrenan y desarrollan con datos de la policía, las fuerzas del orden y los sistemas jurídico-penales.

Estas autoridades suelen recopilar estos datos o acceder a ellos en diversas fuentes. En Alemania, los sistemas Palantir utilizan datos de las bases de datos de la policía y otras fuentes, incluidas las redes sociales. En los últimos años, se han interpuesto varios recursos jurídicos contra estos sistemas, así como contra las leyes de análisis de datos en las que se ampara su uso.¹³¹ Cuando se consiguió restringir el alcance de los análisis y fuentes de datos gracias a un recurso jurídico, una fuente de la policía alemana afirmó: «Cuando llegó el veredicto hubo quejas y los compañeros se dieron cuenta de que ya no se les permitiría actuar tanto».¹³²

El sistema belga i-Police pretende incluir los datos de todas las bases de datos y las grabaciones de las cámaras de videovigilancia de la policía belga. También utiliza «inteligencia» de código abierto, como información de las redes sociales o de prensa. Para conseguir desempeñar estas funciones, i-Police utiliza tecnologías digitales de una serie de subcontratistas, entre ellos varias empresas israelíes como Interionet y TA9/Rayzone. El director ejecutivo de esta última fue subdirector de la Unidad 8200, la unidad de inteligencia del ejército israelí, responsable del desarrollo e implementación de «Gospel», un sistema de IA para generar de forma automática objetivos de bombardeos en Gaza, como parte del actual

genocidio y matanza masiva del pueblo palestino por parte de Israel.¹³³

Los datos que utilizan estos sistemas están sesgados. En toda Europa, la policía se centra de forma desproporcionada en personas de minorías étnicas. Por ejemplo, la policía española intercepta y registra de forma desproporcionada a las personas por su aspecto racial, étnico o religioso.¹³⁴ En Alemania, las personas que no tienen la ciudadanía están sobrerrepresentadas entre las sospechosas fichadas por la policía, las condenadas por los tribunales y las encarceladas.¹³⁵ El sistema jurídico-penal belga ha sido condenado en varias ocasiones por sus prácticas racistas, especialmente en cuanto a la elaboración de perfiles étnicos.¹³⁶ El Comité de la ONU para la Eliminación de la Discriminación Racial (CERD) ha compartido su preocupación por el hecho de que las personas de origen extranjero estén sobrerrepresentadas en el sistema jurídico-penal belga, especialmente en prisión.¹³⁷

Los datos del sistema policial y jurídico-penal que se utilizan en estos sistemas digitales están plagados de sesgos estructurales e institucionales, sobrerrepresentaciones y discriminación. Y sin embargo se utilizan para crear, desarrollar y explotar sistemas de «predicción», elaboración de perfiles y «evaluación de riesgos» basados en datos. El resultado es una mayor focalización en los mismos grupos y comunidades marginados. Después, los resultados de estas operaciones alimentarán estos sistemas, lo que aumentará la probabilidad de que las personas de estos grupos se perciban como de «alto riesgo» en el futuro. De esta forma, estos algoritmos producen una profecía autocumplida o ciclo de retroalimentación. Existen claros ejemplos sobre cómo estos datos discriminatorios influyen en los resultados de estos sistemas.

No se conoce la lista completa de los datos utilizados por el sistema de elaboración de perfiles alemán RADAR-iTE. Sin embargo, se basa en una evaluación remota sin contacto directo con la persona que se está evaluando.¹³⁸ La evaluación incluye temas como «violencia contra otras personas», «interacción con las autoridades y otras instituciones» y «vínculos



con el ejército y viajes». Otras preguntas son: «¿Cómo es su vida privada? ¿Es más una persona solitaria o actúa en grupo? ¿Tiene contactos fuera del panorama islamista? ¿Tiene trabajo?». ¹³⁹

Este tipo de elementos para la elaboración del perfil implica que a alguien que venga de una zona de conflicto o que utilice determinadas rutas para hacer turismo o visitar a la familia, se le podría catalogar como persona sospechosa o de «riesgo». Los elementos de datos como las personas colaboradoras, personas de contacto o los patrones de viaje pueden conllevar una clara discriminación. ¹⁴⁰ Asimismo, la evaluación de RADAR-iTE también contiene otros elementos preocupantes y potencialmente discriminatorios sobre los problemas de salud mental y tendencias suicidas. ¹⁴¹

Tampoco han estado exentos de problemas los datos utilizados para entrenar al sistema que antes utilizaba la policía española, VeriPol, para detectar denuncias falsas. VeriPol se entrenaba con denuncias presentadas a la policía que alguien del personal policial catalogaba manualmente como falsa o verdadera. Sin embargo, no todos esos casos se han resuelto, por lo que no había hallazgos objetivos o conclusivos sobre la veracidad o falsedad de dichas denuncias. Por tanto, el modelo se basaba completamente en las conjeturas del personal policial que catalogó las denuncias. ¹⁴² Resulta llamativo que las autoridades españolas tardaran siete años en reconocer los problemas relacionados con su uso y dejar de utilizarlo.

En España, el sistema VioGén presuntamente predice si una mujer va a sufrir violencia de género. Sin embargo, el sistema no utilizaba los testimonios reales de las mujeres que denunciaron casos de violencia de género, sino las versiones del personal policial presente en esas denuncias. Por tanto, la puntuación de riesgo resultante depende totalmente de la valoración del personal policial. ¹⁴³ Además, el sistema solo puede procesar datos de denuncias presentadas.

Sin embargo, muchos casos de violencia de género no se denuncian, especialmente si hablamos de mujeres migrantes, de entornos marginados y con dificultades económicas y mujeres con menores a su cargo. Junto con las personas del colectivo LGBTQIA+ y personas con discapacidad, estos grupos son los más afectados por las dificultades estructurales a la hora de denunciar a sus agresores. Por lo tanto, el sistema no tenía en cuenta del todo las experiencias de los grupos más marginados de la sociedad. ¹⁴⁴

Los conceptos en los que se basan estos sistemas «predictivos», de elaboración de perfiles y evaluación de «riesgos» están básicamente sesgados. Este problema emana de una falta de claridad que lleva a la subjetividad o de términos culturalmente específicos con trasfondos racializados.

En Alemania, términos vagos como «Gefährder» (persona peligrosa) y «relevante Person» (personas que pueden desempeñar un papel importante) se utilizan para categorizar a personas sospechosas de cometer o ser cómplices de un delito. Se han

convertido en términos habituales entre las fuerzas de seguridad y la policía, y se utilizan en los sistemas RADAR. No se han definido legalmente y resultan vagos y nada científicos. Esto significa que se elaborarán perfiles de las personas de forma subjetiva, a discreción de las autoridades y de forma incoherente. De este modo se vulnera toda la legitimidad del sistema.

Estos problemas se revelan por el uso práctico de los términos. Los cuerpos de policía alemanes han tenido muchas más reservas a la hora de categorizar a las personas extremistas de extrema derecha como personas peligrosas que a aquellas personas denominadas «islamistas». Por ejemplo, cuando se destapó la organización neonazi NSU (National Socialist Underground) en 2011, solo cuatro personas del grupo se categorizaron como «Gefährder».¹⁴⁵

Los datos utilizados en estos sistemas plantean otros problemas. El sistema belga i-Police combinará datos de varias fuentes de la policía, incluida información «no validada». Esto incluye información sin corroborar de informes policiales, que se suelen conocer o describir como «inteligencia» policial, que incluyen información sobre personas que no han sido condenadas o acusadas de un delito. El director de la autoridad en materia de protección de datos que supervisa a la policía belga, el COC, ha planteado tener serias dudas sobre el uso de estos datos en el sistema i-Police.¹⁴⁶

Los sistemas que evalúan posibles delitos, futuros delitos o el «riesgo» de que estos se cometan, suponen un cambio conceptual, pasando de las evaluaciones basadas



en pruebas reales de una acción o de la implicación en una acción, a un riesgo abstracto e indeterminado que *podría* desarrollarse en el futuro, a menudo estimado únicamente sobre la base de pruebas circunstanciales. Lo mismo ocurre con todos los sistemas centrados en el individuo o la persona.

Resultados e impacto

Estos sistemas «predictivos», de elaboración de perfiles y evaluación de «riesgos» se utilizan para influir en una serie de decisiones y resultados policiales y de las fuerzas del orden: desde la vigilancia y el seguimiento, a las intercepciones e interrogatorios, registros, redadas en domicilios e, incluso, arrestos.

El sistema de la policía del estado alemán de Hesse, hessenDATA, facilita una vigilancia enormemente invasiva. Pese a que se supone que se utiliza para delitos «graves», «organizados» o de «seguridad estatal», se ha estado utilizando cada vez más para delitos no violentos. En 2022, se denunció que la policía categorizó unas 12 000 de las 14 000 consultas a hessenDATA al año como «medidas preventivas» contra la comisión de delitos.¹⁴⁷

Los resultados de estos sistemas suelen asignar una puntuación de «riesgo» a las personas: bajo, medio o alto, o variaciones en dichas categorías. Estas puntuaciones supuestamente indican las probabilidades que tienen de cometer un delito o presentar un comportamiento delictivo.

Según la Oficina de la Policía Criminal Federal de Alemania, RADAR-iTE ha evaluado a unas 800 personas del espectro «islamista» desde 2017.¹⁴⁸ Con fecha de noviembre de 2023, 487 personas habían sido clasificadas como peligrosas (*Gefährder*) con respecto a delitos con «motivación política» motivados por la ideología religiosa. Por el contrario, el número de personas de extrema derecha categorizadas como «*Gefährder*» o «personas relevantes» sigue siendo relativamente bajo, al igual que el número de evaluaciones de RADAR-rechts.¹⁴⁹

El sistema VioGén que utiliza la policía española se usa para asignar puntuaciones de riesgo, pero para víctimas, no para delincuentes. Una puntuación baja significa que la policía comprobará que la víctima está bien mediante llamadas telefónicas; por ejemplo, cuando haya una puntuación de riesgo extremo, la policía podría vigilar la casa de la víctima o asignarle una patrulla para garantizar su seguridad.¹⁵⁰ En el 95 % de los casos, la policía aplica lo que le indica la puntuación de riesgo VioGén.¹⁵¹

Como resultado de la elaboración de perfiles a partir de los Registros de nombres de los pasajeros (PNR), la Oficina de la Policía Criminal Federal de Alemania ha calificado las rutas entre Turquía y Alemania como rutas potencialmente sospechosas. Presuntamente, las suelen utilizar las personas integrantes de grupos terroristas islámicos «ya que son rutas populares de turismo y, por tanto, ofrecen precios baratos y facilidad para pasar

desapercibido».¹⁵²

El sistema DRAVY utilizado en las cárceles españolas predice incorrectamente un alto nivel de riesgo a casi la mitad de las personas a las que evalúa.¹⁵³ Esto se traduce en que estas personas reciben un tratamiento más estricto y unas condiciones de vida más duras mientras están encarceladas. A las personas extranjeras esto les afecta de forma desproporcionada.¹⁵⁴ El sistema RisCanvi, que también se utiliza en España, es conocido por discriminar conforme al estatus socio-económico o por la relación con otras personas. Otorga una mayor puntuación a las personas con un historial de empleo y situación económica «inestables», aquellas sin red familiar o personas con familiares o progenitores con antecedentes penales.¹⁵⁵

La cantidad de personas afectadas por esta herramienta y sus consecuencias es considerable.



Con fecha de septiembre de 2023, el sistema VioGén había evaluado unos 770 000 casos.¹⁵⁶ Los sistemas de Registro de nombres de los pasajeros (PNR) permiten elaborar perfiles de millones de personas que utilizan el transporte aéreo. En 2022, 156 aerolíneas alemanas transmitieron alrededor de 424 millones de registros de datos PNR a la policía, que afectaban a unos 121 millones de personas que utilizaron el transporte aéreo. En 2023, se generaron unos 385 millones de registros PNR hasta el 31 de octubre, correspondientes a 107 millones de personas usuarias del transporte aéreo.

Además, más allá de vulnerar la privacidad de decenas de millones de personas usuarias del transporte aéreo, los sistemas PNR han provocado que un gran número de personas tengan que hacer frente a intervenciones policiales. En 2023, la policía alemana realizó más de 10 000 intervenciones por los perfiles elaborados con el sistema PNR. Casi una quinta parte de los casos resultaron ser falsos positivos (coincidencia incorrecta).¹⁵⁷ En los 8284 casos de positivos reales (coincidencias correctas), se implementaron las siguientes medidas:

- 2178 investigaciones sobre la residencia;
- 2394 seguimientos de la policía/controles de la policía secreta;
- 1236 arrestos, 2303 controles específicos (abiertos); y
- 173 denegaciones/rechazos de entrada.¹⁵⁸

Por tanto, se analizan millones de registros de datos de personas usuarias del transporte aéreo para llevar a cabo miles de investigaciones sobre estatus de inmigración o posibles delito, por lo que la base evidencial objetivo de estas no existe o es muy vaga.

Los casos individuales destacados en el informe de Alemania demuestran las consecuencias extremas de ser etiquetado (incorrectamente) como «*Gefährder*». El sesgo antimusulmán lleva a la policía y a las autoridades a tratar a las personas jóvenes musulmanas de forma distinta a las personas jóvenes blancas con un comportamiento problemático similar, porque se les considera antes una amenaza.¹⁵⁹

Las consecuencias de ser objeto de un perfil del sistema RADAR-iTE incluyen:

- estar bajo vigilancia y seguimiento;¹⁶⁰
- «prisión preventiva» cuya duración puede pasar de varios días a meses;¹⁶¹
- detención antes de la deportación y,¹⁶² después, la deportación.¹⁶³

Las personas sometidas a perfiles también pueden ver sus solicitudes de asilo paralizadas.¹⁶⁴

Otros sistemas de «predicción» de delitos centrados en la persona que se utilizan en Europa

Además de los ejemplos presentados anteriormente, las autoridades de los sistemas policiales y jurídico-penales de otros países europeos también están utilizando herramientas para la elaboración de perfiles y «predicción» de delitos centradas en la persona. Otras investigaciones anteriores encontraron pruebas del uso de sistemas similares en cuerpos de policía y cárceles de Reino Unido, Italia y Países Bajos.

Amnesty International UK reveló que 11 cuerpos de policía estaban utilizando herramientas de elaboración de perfiles y «predicción» de delitos centrados en las

personas en el Reino Unido.¹⁶⁵ Estas herramientas incluyen:

- la herramienta de la Policía Metropolitana de Londres, Violence Harm Assessment (Evaluación del daño violento), que elabora perfiles de personas de todo Londres según su riesgo de comportamiento violento. Con fecha de agosto de 2024, el 66 % de las personas de las que el sistema elaboró un perfil eran negras, frente al 22 % de personas blancas.
- El sistema Integrated Offender Management (IOM, Gestión de delincuentes integrada) de la Policía de West Midlands se utiliza para «predecir» el potencial de una persona de comportamiento delictivo en el futuro. El análisis interno del cuerpo mostró que las personas negras tienen un 2,4 más de probabilidades de aparecer en el grupo de alto riesgo «previsto» que una persona del norte de Europa (blanca).

En Inglaterra y Gales, los servicios penitenciarios y de libertad condicional están utilizando el sistema Offender Assessment System (OASys, Sistema de evaluación de delincuentes) para «predecir» el riesgo de reincidir de toda persona que se introduzca en el sistema jurídico-penal. Este sistema ha recibido muchas críticas por la elaboración de perfiles raciales, amenazas a la privacidad y la falta de oportunidades para rendir cuentas o reparar el daño que sufren las víctimas.¹⁶⁶

En Países Bajos, la policía ha utilizado un sistema llamado ProKid, cuyo objetivo es «predecir» el riesgo de reincidir de menores y jóvenes.¹⁶⁷ En Ámsterdam, la policía ha utilizado dos herramientas para la elaboración de perfiles llamadas Top400 y Top600, que pretenden clasificar a los 600 y 400 jóvenes que presuntamente tienen más posibilidades de cometer distintos tipos de delitos.¹⁶⁸

Diana Sardjoe, una madre cuyos hijos se incluyeron en la elaboración de perfiles de Top400 y Top600, ha declarado que la consecuencia es que sus hijos estén sometidos a un continuo seguimiento y al acoso de las instituciones, y ha solicitado la prohibición de estos sistemas de actuación policial «predictiva».¹⁶⁹

En Italia, la policía antes utilizaba un sistema de elaboración de perfiles llamado Delia, que incluía datos étnicos para elaborar perfiles personales.¹⁷⁰





Sistemas de videovigilancia con IA

Cada vez con más frecuencia, los cuerpos de policía de toda Europa están utilizando sistemas de videovigilancia con IA. Estos sistemas utilizan métodos basados en la IA para realizar búsquedas en las grabaciones de vídeo, como las de las cámaras CCTV (circuitos cerrados de televisión) y bases de datos de la policía, para identificar a personas y objetos o detectar comportamientos «sospechosos».

La investigación en la que se basa este informe incluye varios ejemplos de sistemas de videovigilancia con IA que utiliza la policía en Bélgica y España. La *Quadrature du Net* ha llevado a cabo por separado una amplia investigación sobre los usos policiales de la videovigilancia con IA en Francia.¹⁷¹ En Alemania, *AlgorithmWatch* ha identificado dos proyectos piloto de sistemas de videovigilancia con IA en cárceles para «prevenir el suicidio». Además, hay pruebas de que la policía de Italia también utiliza este sistema.

El uso de la videovigilancia con IA por parte de las fuerzas del orden suscita importantes

preocupaciones, ya que puede vulnerar derechos fundamentales, como el derecho a la intimidad y a la no discriminación.

Actuación policial

En España, varias localidades de la Comunidad de Madrid utilizan sistemas de videovigilancia que incluyen métodos de IA para el reconocimiento de imágenes. Los sistemas, proporcionados por Bosch Security a través de la empresa con sede en EE. UU. Intelligent Security Services, tienen dos fines: reconocimiento automático de matrículas y la identificación de personas sospechosas de delitos.¹⁷² El sistema también puede utilizarse para la búsqueda de personas conforme a criterios como el color de pelo, la ropa, los rasgos faciales y la edad. No hay pruebas concretas que demuestren que este sistema disminuye la tasa de criminalidad.¹⁷³ En Madrid, con fecha de enero de 2025, había al menos 83 cámaras de vigilancia con IA operadas por la Policía Municipal, que planea instalar 38 más.¹⁷⁴

En Bélgica, los cuerpos de policía local y la policía federal utilizan varios sistemas de videovigilancia con IA. Entre estos sistemas se incluye un software fabricado por BriefCam, una empresa israelí, para el análisis retrospectivo de imágenes a través de la creación de sinopsis de los vídeos.¹⁷⁵ Al igual que el sistema de Bosch en España, este sistema permite a la policía categorizar a las personas conforme a criterios como el color de la ropa, el género o sus pertenencias.

Esta última función podría ser ilegal. El marco legal belga en cuanto a no discriminación permite la investigación selectiva basada en criterios objetivos, pero prohíbe la clasificación masiva de personas. Conforme a estos ejemplos y otros, el informe belga pide que se eliminen los futuros planes de videovigilancia con IA incluidos en el gran proyecto i-Police.

En 2023, Francia se convirtió en el primer país europeo en legalizar la vigilancia biométrica, a través de cámaras de videovigilancia algorítmicas, en virtud de una ley sobre la organización de los Juegos Olímpicos de París 2024.¹⁷⁶ El sistema se implementó en Saint-Denis, un barrio con una población mayormente de minorías étnicas y clase trabajadora al norte de París, donde se celebraron la mayor parte de los Juegos Olímpicos.¹⁷⁷ El sistema se legisló originalmente para tener una vigencia hasta finales de 2024, pero en cuanto terminaron las Olimpiadas, las autoridades intentaron ampliar su periodo de uso.¹⁷⁸

En otro lugar de Francia, *La Quadrature du Net* ha interpuesto un recurso judicial de tres años contra la implementación del software de videovigilancia basado en IA Briefcam en Moirans, en la región de Isère. El 30 de enero de 2025, un tribunal falló que el uso de este sistema era ilegal: incumplía varias normas de protección de la privacidad en virtud de la Ley de Protección de Datos de la UE y el Código de Seguridad Interno francés.¹⁷⁹

Este fallo invalida los marcos legales que anteriormente permitían el uso de los

sistemas de videovigilancia automatizados, incluidos aquellos introducidos mediante autorizaciones temporales experimentales para los Juegos Olímpicos de París de 2024. El fallo también marca un importante precedente legal para otras causas abiertas actualmente frente a los sistemas algorítmicos que utiliza la policía en Francia.¹⁸⁰

Cárceles

En Alemania, *AlgorithmWatch* ha identificado dos proyectos piloto de sistemas de videovigilancia con IA para «prevenir el suicidio» en las cárceles. Estos distópicos sistemas de vigilancia aumentarían la videovigilancia ya existente en las celdas con algoritmos de aprendizaje automático para intentar detectar signos iniciales de intentos de suicidio.

En Renania del Norte-Westfalia, el Ministerio de Justicia alemán y la empresa informática alemana FusionSystems querían desarrollar un algoritmo de aprendizaje automático basado en grabaciones de aprendizaje interpretadas por actores. El algoritmo se entrenó para detectar objetos (por ejemplo, cuchillos, tijeras, cuerdas, mecheros) y comportamientos que pudiesen indicar intenciones suicidas. Esto podría incluir, por ejemplo, hacer un lazo con un cinturón, atar una cuerda o un lazo a la reja de una ventana, sacar un cuchillo o jugar con un cuchillo de gran tamaño. Asimismo, se entrenó al algoritmo con grabaciones de comportamientos que no llamaban la atención, como sentarse en cuclillas, leer o ver la televisión. Supuestamente, así se enseñaba al sistema a distinguir entre situaciones inofensivas e indicaciones de riesgo de suicidio.¹⁸¹ Presuntamente, el sistema también incluía un mecanismo de control esquelético, que utilizaba sensores y técnicas de aprendizaje automático para controlar los movimientos corporales y articulares de una persona.¹⁸²

Estos factores se utilizarían para asignar un «nivel de peligro» a la situación en la celda, que se calcularía continuamente. Se informaría al funcionamiento de prisiones sobre la situación actual con un sistema de alarma de «semáforo». Además, en caso de «niveles de peligro» alto, sonaría una alarma acústica para poder intervenir rápidamente.

En Baja Sajonia, el Centro de Investigación para la Tecnología de Innovación FZI y la empresa de seguridad de TI VOMATEC Innovations pretenden desarrollar un sistema similar. El objetivo es crear un «software operativo como prototipo» que, probablemente, se implemente por primera vez en una cárcel de Oldemburgo.¹⁸³

En un primer momento, el proyecto buscaba utilizar la tecnología de vigilancia con IA en zonas comunes, como zonas de exterior o espacios de ocio. La intención era identificar, supuestamente, «el traspaso de objetos prohibidos entre las personas encarceladas».¹⁸⁴ Sin embargo, esto dió lugar a fuertes críticas por parte de las autoridades en materia de protección de datos de Baja Sajonia.¹⁸⁵ A diferencia del sistema de Renania del Norte-Westfalia, que se había entrenado con grabaciones de actores, el sistema de Baja

Sajonia se había entrenado con grabaciones reales de intentos de suicidio y escenas violentas en las cárceles.¹⁸⁶

Resulta muy preocupante el uso de sistemas de análisis de movimientos corporales o emociones basados en la IA. Este tipo de tecnología no solo no tiene fundamento científico,¹⁸⁷ también es propensa al sesgo racial o étnico. Por ejemplo, la tecnología de la cámara puede calibrarse solo para tonos de piel más claros. Hay más posibilidades de que se interpreten como «agresivas» las expresiones faciales de los hombres negros que las de los blancos.¹⁸⁸ Los sesgos culturales pueden influir en el entendimiento normativo del lenguaje corporal o la expresión facial. Otros factores que pueden influir en esta tecnología son una mala iluminación o las caras oscurecidas o alteradas por la presencia de gafas o pañuelos para la cabeza.

Debido a que los falsos negativos pueden tener consecuencias que potencialmente ponen en riesgo la vida, el uso prospectivo de estos sistemas resulta extremadamente preocupante. Incluso aún cuando funcionan según su uso previsto, con unos niveles de precisión adecuados, son enormemente invasivos¹⁸⁹ e interfieren de forma considerable en la privacidad de las personas encarceladas. Un antiguo preso entrevistado por *AlgorithmWatch* afirmó que para prevenir realmente de forma eficaz los suicidios en las cárceles, sería necesario abolir el sistema penitenciario:

*«La cárcel no es un lugar terapéutico, no es un sitio para rehabilitarse, su función es el castigo. Por lo que la gente que lo necesita no recibe ayuda, es muy deprimente y veo que la gente no aguanta mucho... Hay otras formas de prevenir el suicidio: la terapia y la empatía, contar con el apoyo de la comunidad, ayudar a la gente a encontrar un objetivo en su vida».*¹⁹⁰

En 2023 en España, el Departamento de Justicia de la Generalitat puso en marcha un proyecto piloto en la cárcel Mas d'Enric cercana a Tarragona de «cámaras de reconocimiento facial y análisis de vídeo» para la «detección en tiempo real de expresiones no verbales y actitudes que indiquen un comportamiento ilícito». Financiado en parte por la Unión Europea, estaba previsto ampliar su uso a otras cárceles de la región. Sin embargo, el gobierno de la Generalitat de Catalunya anunció en enero de 2024 que, en virtud de la recién aprobada Ley de IA, no se iba a continuar con el proyecto.¹⁹¹



Bases de datos

Las bases de datos suelen proporcionar los datos utilizados en los sistemas «predictivos», de elaboración de perfiles y evaluación de «riesgos» utilizados por las autoridades policiales y jurídico-penales. También pueden servir de justificación o supuesta base evidencial para actuaciones policiales y de las fuerzas del orden. Incluyen a una gran variedad de grupos de población y pueden contener una gran cantidad de datos sensibles, desde datos biográficos hasta huellas dactilares, fotos y antecedentes penales, entre muchas otras opciones.

En Bélgica, la policía y las fuerzas del orden utilizan varias categorías distintas de bases de datos:

- la Base de datos nacional general se utiliza para investigaciones policiales;
- las bases de datos «básicas» se componen de notas de campo de la policía y apuntes de «inteligencia»;
- las bases de datos especiales las crea la policía para fines específicos, como por ejemplo para las llamadas «bandas urbanas»;
- las bases de datos comunes comparten datos entre la policía y las agencias de inteligencia para supuestos fines terroristas; y
- las bases de datos técnicas contienen datos recopilados automáticamente, como los procedentes de las cámaras de reconocimiento automático de número de matrículas.¹⁹²

La Policía Nacional y Gendarmería francesas utilizan una base de datos llamada TAJ («Tratamiento de registros penales») para las actividades del día a día de las fuerzas del orden, que las autoridades francesas han intentado interconectar con varias bases de datos más.¹⁹³ Incluye información diversa sobre aquellas personas sospechosas de haber cometido un delito grave, así como de las víctimas.¹⁹⁴ Entre los cuerpos municipales de la policía francesa, la recopilación de datos de forma ilegal resulta una práctica común.¹⁹⁵

La Policía Nacional y Gendarmería tienen autorización para utilizar la TAJ para el reconocimiento facial *post facto* en el contexto de las investigaciones judiciales. Esto significa que pueden hacerse, por ejemplo, con grabaciones de circuitos cerrados de televisión o fotos de las personas sospechosas y utilizarlas para buscar en la base de datos registros que coincidan. La función de comparación facial cada vez se utiliza más para los controles de identidad administrativos. De media, el sistema se utiliza para este fin más de 1600 veces al día.¹⁹⁶

La base de datos de la Policía Nacional española sobre personas extranjeras, ADEXTTRA, contiene una gran cantidad de información. Estos datos incluyen:

- nacionalidad;
- estado civil;
- profesión y actividad laboral;
- posesión de bienes;
- ingresos y beneficios;
- información sobre cohabitación;
- registros de conducta, detenciones y detenciones extrajudiciales, así como antecedentes penales;
- fotografías y otras imágenes;
- huellas dactilares; y
- muestras de voz.¹⁹⁷



Las bases de datos que utilizan la policía y las fuerzas del orden europeas contienen una cantidad inmensa de datos. La Base de datos general nacional belga contiene información sobre tres millones de personas (un cuarto de la población belga).

En Francia, la base de datos TAJ contiene registros de casi 20 millones de personas, y

unos 10 millones de fotografías faciales.¹⁹⁸ La base de datos de *Titres électroniques sécurisés* (TES o documentos electrónicos protegidos), creada en 2016 por el Ministerio del Interior, alberga información de todas las personas solicitantes de documentos de identidad y pasaportes.¹⁹⁹ Con el tiempo, el Ministerio del Interior francés podrá acceder a la imagen facial de cualquier persona que se encuentre en territorio francés.²⁰⁰ Esto encaja a la perfección con los planes de la UE de recopilar «datos de identidad» de cada persona extranjera presente en el territorio de la UE y ponerlos a disposición de la policía y las autoridades de inmigración.²⁰¹

Cientos de cuerpos de policía municipal franceses cuentan con el software «Smart Police», una plataforma y aplicación digital que les permite redactar informes «sobre la marcha», hacer fotos y describir sucesos, todo lo cual puede añadirse a las bases de datos centrales pertinentes. Smart Police incluye un elemento «predictivo», que recopila información de diversas fuentes, combinando datos policiales sobre delincuencia y datos sobre la ubicación de agentes con datos socioeconómicos de la población, previsiones meteorológicas y «rumores» de la dirección de los colegios y de responsables de arrendamientos, e incluso de las redes sociales, para intentar «predecir» el riesgo de que se produzcan actos delictivos.²⁰²

Los datos de estas bases de datos y la forma en la que se utilizan pueden tener consecuencias serias e importantes. Contienen una inmensa cantidad de información incorrecta, así como de información sin corroborar presentada como datos de «inteligencia».

Pese a que los datos imprecisos pueden parecer inofensivos, sus consecuencias pueden ser graves. Por ejemplo, si se mantiene información desactualizada sobre una persona en una base de datos, se le podría arrestar por error. En España, se ha detenido por error a migrantes porque los registros en las bases de datos no se habían actualizado correctamente.²⁰³

Junto con información fácticamente correcta, la denominada inteligencia policial puede utilizarse en los sistemas «predictivos» y de elaboración de perfiles. Esto influye en los resultados del sistema, lo que a su vez influye en las decisiones de la policía y las fuerzas del orden. Así, la información no corroborada pasa a ser un hecho que luego se utiliza contra las personas.

Las bases de datos preocupan también por su discriminación ilegal. Pueden ser discriminatorias por sí mismas, por el origen y los tipos de datos que contienen. Su uso también puede conllevar prácticas discriminatorias.²⁰⁴ En las bases de datos de los sistemas policiales y jurídico-penales están considerablemente sobrerrepresentadas las personas, grupos y comunidades marginadas que históricamente han sido perseguidas, controladas y castigadas por las autoridades estatales. Esto incluye a las personas y comunidades negras y racializadas, a migrantes y personas de clase trabajadora y de entornos desfavorecidos socio-económicamente, personas del colectivo LGTBQ+ y personas con problemas de salud mental.²⁰⁵ Varios estados federales alemanes han mantenido bases de datos que incluían etiquetas como «yonqui», «vagabundo/a», «gitano/a» y «contagioso/a», esta última en relación con personas

con VIH.²⁰⁶

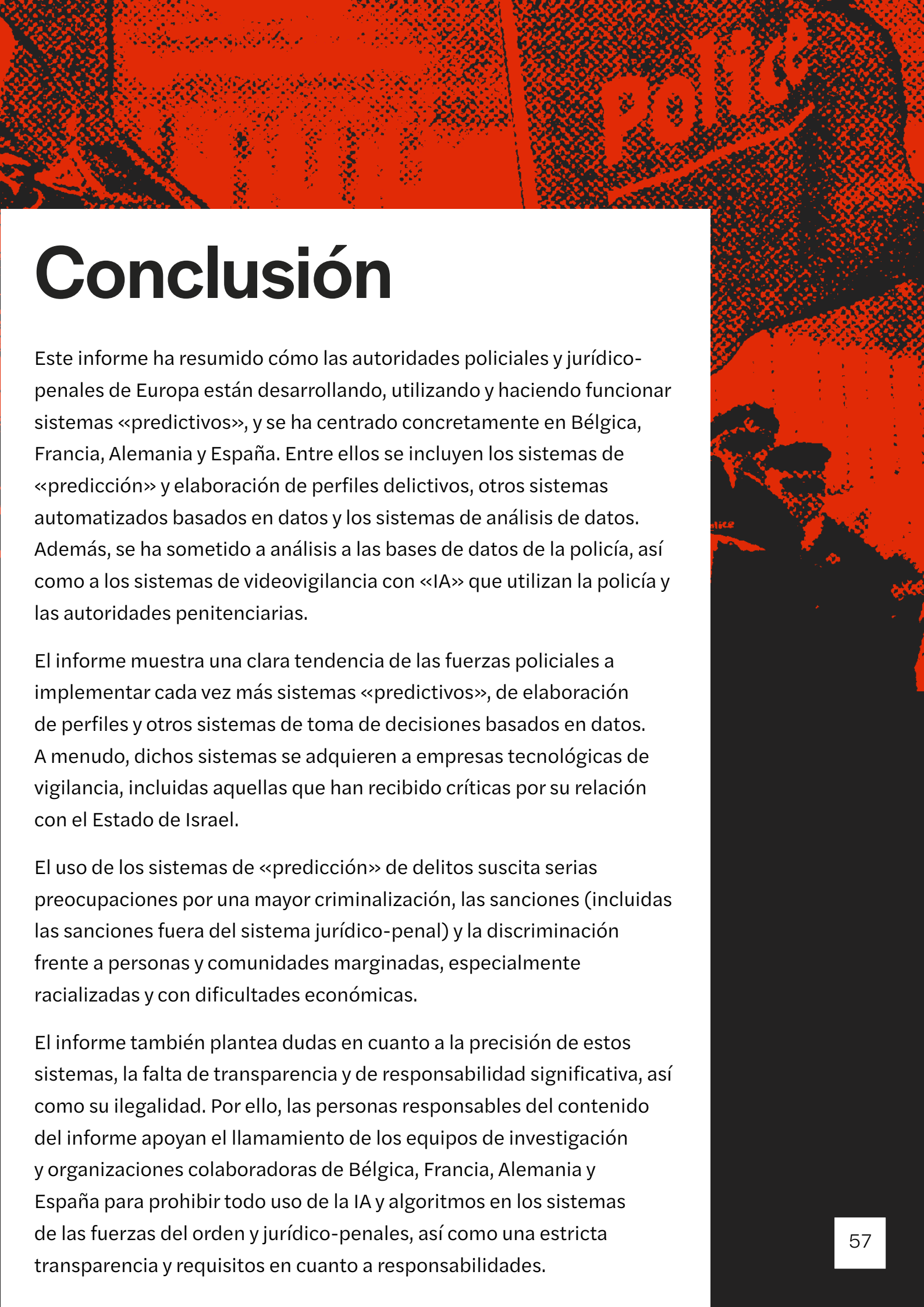
Cada vez más empleadores y autoridades utilizan las bases de datos de la policía belga para realizar pruebas de seguridad. Las personas de origen norteafricano y belga-marroquí están sobrerrepresentadas entre aquellas que no superan estas pruebas. El informe de Bélgica también se hace eco de la historia de un joven musulmán que no pudo acceder a un empleo por la información errónea que aparecía en una base de datos de la policía.²⁰⁷

Los cuerpos de policía local de Bélgica crean asimismo bases de datos para perseguir a las denominadas «bandas urbanas», un término con una gran carga de racismo para los hombres jóvenes. La concepción de estos grupos como «urbanos» y «bandas» se debe a su origen étnico, y los parámetros para incluirlos en estas bases de datos resultan vagos. Las personas incluidas en dichas bases de datos, se vieron sometidas al control, vigilancia y a un mayor número de intercepciones y registros.²⁰⁸

La policía local de Bélgica también cuenta con una base de datos sobre personas que ejercen el trabajo sexual. Aunque aparentemente se utiliza para «regular» el sector, con ella pueden seguir y controlar a las personas que ejercen este tipo de trabajos. Como el registro de personas que ejercen trabajos sexuales es obligatorio, esto sirve para excluir a personas con un estatus migratorio irregular o precario y las aleja de redes de apoyo y seguridad.²⁰⁹

La base de datos española ADEXTTRA se utiliza para identificar a las personas migrantes y comprobar su situación en el país. Facilita a la policía la realización de controles de identidad de aquellas personas percibidas como «extranjeras». Se ha demostrado sobradamente que la policía española utiliza técnicas de elaboración de perfiles raciales.²¹⁰

Las restricciones y salvaguardas en torno al uso policial de las bases de datos y la información que contienen son frágiles, así como la aplicación de la ley al respecto. Normalmente, no se castiga ni denuncia a integrantes de la policía que acceden de forma ilegal a los datos o infringen los requisitos o directrices.²¹¹ Además, se suelen sobrepasar los periodos de conservación de datos, lo que en la práctica supone el almacenamiento indefinido de datos personales y potencialmente sensibles sin eliminarlos.²¹² La policía no elimina los datos que está obligada a eliminar por ley, y los mecanismos de aplicación o las sanciones son escasos o inexistentes cuando esto ocurre.²¹³



Conclusión

Este informe ha resumido cómo las autoridades policiales y jurídico-penales de Europa están desarrollando, utilizando y haciendo funcionar sistemas «predictivos», y se ha centrado concretamente en Bélgica, Francia, Alemania y España. Entre ellos se incluyen los sistemas de «predicción» y elaboración de perfiles delictivos, otros sistemas automatizados basados en datos y los sistemas de análisis de datos. Además, se ha sometido a análisis a las bases de datos de la policía, así como a los sistemas de videovigilancia con «IA» que utilizan la policía y las autoridades penitenciarias.

El informe muestra una clara tendencia de las fuerzas policiales a implementar cada vez más sistemas «predictivos», de elaboración de perfiles y otros sistemas de toma de decisiones basados en datos. A menudo, dichos sistemas se adquieren a empresas tecnológicas de vigilancia, incluidas aquellas que han recibido críticas por su relación con el Estado de Israel.

El uso de los sistemas de «predicción» de delitos suscita serias preocupaciones por una mayor criminalización, las sanciones (incluidas las sanciones fuera del sistema jurídico-penal) y la discriminación frente a personas y comunidades marginadas, especialmente racializadas y con dificultades económicas.

El informe también plantea dudas en cuanto a la precisión de estos sistemas, la falta de transparencia y de responsabilidad significativa, así como su ilegalidad. Por ello, las personas responsables del contenido del informe apoyan el llamamiento de los equipos de investigación y organizaciones colaboradoras de Bélgica, Francia, Alemania y España para prohibir todo uso de la IA y algoritmos en los sistemas de las fuerzas del orden y jurídico-penales, así como una estricta transparencia y requisitos en cuanto a responsabilidades.

Discriminación

Los sistemas «predictivos» centrados en la ubicación no contienen datos sobre personas concretas. Sin embargo, las personas racializadas y procedentes de los entornos más desfavorecidos son las que más sufren las intercepciones y controles de la policía, así como sus posibles consecuencias, en las zonas en las que se «predicen» los delitos.

Las predicciones conllevan un aumento del control policial de esas zonas y de las personas y comunidades que las habitan. Esto conlleva la elaboración de perfiles raciales, las intercepciones, controles y registros de las personas de estas zonas, y, por tanto, su criminalización. De esta forma, las herramientas de «predicción» de delitos ofrecen la justificación de la selección racista de algunas zonas y las personas que las habitan. También eluden las supuestas protecciones jurídicas frente a la elaboración de perfiles étnicos.

Estos controles, intervenciones e incidentes de las fuerzas del orden se registran posteriormente en las bases de datos que alimentan a los sistemas «predictivos». El uso de los datos para las «predicciones» futuras crea un ciclo de retroalimentación en el que se seleccionan las mismas zonas y perfiles una y otra vez.

El mismo problema de los datos sesgados que provocan unos resultados sesgados y perpetúan los ciclos de retroalimentación se da con los sistemas predictivos centrados en personas. El sistema español DRAVY también muestra una discriminación básica en su diseño: se centra en el concepto occidental de la denominada radicalización «yihadista» y, por tanto, se centra casi exclusivamente en musulmanes y personas de origen musulmán. También presenta una considerable tasa de falsos positivos. De forma similar, el sistema RADAR-iTE en Alemania se basa en la islamofobia y una concepción sesgada de quién constituye una potencial «amenaza». Esto se traduce en un considerable sesgo antimusulmán en sus resultados y en aquellas personas afectadas por su uso.



Criminalización

Al amparo de los sistemas de «predicción» de delitos centrados en la ubicación, barrios enteros se categorizan como delictivos y la «previsión» de que se cometan delitos aquí es muy alta. Esto conlleva una mayor presencia policial e intervenciones de patrullas, intercepciones y registro, así como otras operaciones. También justifica las intercepciones, controles de identidad y registros «sin indicios de sospecha», ya que la «predicción» proporciona tanto la justificación como la sospecha. Esto aumenta la probabilidad de criminalizar a las personas y comunidades que viven y trabajan en estas zonas, y puede darse sin que haya pruebas objetivas de delito.

Los sistemas centrados en las personas elaboran perfiles de estas en función de su origen, para lo que las categoriza directamente como delincuente o indirectamente como posible delincuente, lo que supone un estigma. Estas personas se consideran y tratan como culpables hasta que se demuestre su inocencia. También hay personas que se han visto vinculadas a otras con un perfil delictivo por los sistemas de elaboración de perfiles. Esto crea una red increíblemente amplia de criminalización.

Las «predicciones» o perfiles individuales pueden conllevar consecuencias y sanciones graves tanto penales como de otra índole. Tal y como se ha resumido en este informe, las consecuencias conocidas incluyen la vigilancia y seguimiento de la policía y fuerzas del orden, visitas al domicilio o al lugar de trabajo, redadas, inhabilitación laboral, interrogatorios o incluso arrestos o detenciones «preventivas». Algunas personas se han visto sometidas a investigaciones por su situación de residencia. Se han enfrentado a controles fronterizos e interrogatorios, se les ha denegado la entrada, han visto cómo pausaban o detenían sus expedientes de asilo o, incluso, han sido deportadas. Todo esto puede darse sin que haya pruebas objetivas de delito: solo basándose en una sospecha generada algorítmicamente basada en el análisis de datos.



Transparencia y responsabilidades

La falta de transparencia en relación con el desarrollo, formación y uso operativo de estos sistemas «predictivos», de elaboración de perfiles y evaluación de riesgos es una traba fundamental para la justicia y la exigencia de responsabilidades.

Las personas blanco de la policía o de las fuerzas del orden por el resultado de la actuación policial «predictiva» o de un sistema de «predicción» de delitos, a menudo no son conscientes de ello. Las autoridades que utilizan estos sistemas no suelen facilitar información sobre estos sistemas o cómo los usan. Tampoco notifican a las personas que se han sometido a la elaboración de perfiles o un sistema de predicción o evaluación de riesgos, ni de que las acciones acometidas contra ellas se deben a esta causa. Esto plantea serias dudas sobre lo injustos e imparciales que son estos sistemas y los procesos en los que influyen.

En toda Europa, los marcos jurídicos no exigen un nivel de transparencia considerable a estos sistemas. La próxima Ley de IA de la UE no exige requisitos considerables en materia de transparencia en este contexto. Incluye muchas exenciones para aquellos sistemas utilizados para detectar, prevenir, investigar o enjuiciar delitos.

Esto tiene que cambiar. Las autoridades policiales y jurídico-penales deben publicar la información de todos los sistemas automatizados, basados en el análisis de datos o algoritmos que utilicen en un sitio web o base de datos de acceso público, donde se incluyan los detalles del sistema o software y su funcionamiento, los datos utilizados, la forma en la que el sistema realiza los análisis o crea resultados y para qué se utilizan, así como las posibles consecuencias.

Si una persona o grupo experimenta alguna consecuencia policial o jurídico-penal debido al resultado de un sistema automatizado de toma de decisiones o basado en análisis de datos, deberá saberlo. La autoridad policial o jurídico-penal deberá informar a la persona y ofrecerle la información necesaria para que pueda oponerse a esta decisión o resultado. Esta información debe facilitarse en un formato y forma que resulte entendible para una persona lego en estos sistemas.



Las personas y grupos deben contar con rutas claras para oponerse a los resultados o consecuencias de este tipo de sistema automatizado de toma de decisiones, así como la posibilidad de un resarcimiento significativo.

Sin base legal y uso ilegal

Muchos de estos controvertidos sistemas se desarrollan, prueban o utilizan sin que exista una base legal suficiente en la que ampararse. En muchos casos, operan sin una base legal e incluso, a veces, de forma ilegal, como sucede en Alemania. La recogida de datos en que se basan estos sistemas también se ha considerado ilegal, como en Francia.

Imprecisión

En muchos casos, estos sistemas son, básicamente, imprecisos. Ofrecen imprecisiones graves o falsos positivos, lo que puede implicar a personas inocentes. En muchos casos, la policía, las fuerzas del orden o las autoridades jurídico-penales no evalúan correctamente ni significativamente su precisión antes de implementar estas herramientas. Incluso una vez realizadas estas pruebas, a veces siguen utilizando sistemas con un bajo nivel de precisión.

La precisión, no obstante, tampoco es la panacea. Un sistema «preciso» podría simplemente servir para mantener y reproducir la discriminación inherente en los datos que utiliza.

Prohibición

Tal y como se demuestra en este informe, los sistemas «predictivos», de elaboración de perfiles y evaluación de «riesgos» centrados en la ubicación y en las personas conllevan la elaboración de perfiles raciales y socioeconómicos, la discriminación y la criminalización.

Su uso conlleva consecuencias injustas y discriminatorias, desde la vigilancia hasta la detención y registro, desde el acoso y la violencia policial hasta el arresto, desde la detención hasta la deportación.

La conclusión de este informe y aquellos en los que se basa es la misma: estos sistemas deben prohibirse.

Los órganos legislativos nacionales en los que se están utilizando estos sistemas deberían aprobar una prohibición de su uso. Igualmente, los



órganos legislativos locales o municipios en los que se están utilizando, como por ejemplo, los ayuntamientos, también deberían prohibirlos en su jurisdicción.²¹⁴

Existen varias campañas, algunas más recientes y otras con más tiempo a sus espaldas, contra el uso de estos sistemas en Europa y otros lugares, como la campaña para prohibir los sistemas de actuación policial predictiva en la Ley de IA de la UE,²¹⁵ las campañas de *Technopolice* en Francia²¹⁶ y Bélgica,²¹⁷ la coalición de *Safety Not Surveillance* en Reino Unido²¹⁸ y *Stop LAPD Spying* en EE. UU.²¹⁹ El apoyo a estas campañas y otras similares resulta crucial, ya que los gobiernos, cuerpos de policía, autoridades jurídico-penales y empresas pretenden ampliar el uso de los sistemas algorítmicos, automatizados y de inteligencia artificial.



“

The authors of this report support the calls of the researchers and partner organisations in Belgium, France, Germany and Spain for a prohibition on all uses of AI and algorithms in law enforcement and criminal legal settings, as well as strict transparency and accountability requirements.



Créditos de las imágenes

Portada: ["Politie doet handboeien om"](#) by Shirley de Jong

Página 6: ["Brussels police \(1\)"](#) by Eoghan OLionnain

Página 7: ["we won't pay for your greed #2"](#) by Alisdare Hickson

Páginas 8-11: ["Britain's MOD sprayed blood red to highlight the UK's complicity in Israel's war crimes in Gaza #6"](#) by Alisdare Hickson

Página 12: ["sscs1014sbab10903"](#) by Santa Cruz Sentinel

Página 13: ["Fight Police Racism !"](#) by Alisdare Hickson

Página 14: ["Police - Paris, June 1992"](#) by Ian Abbott

Página 15: ["Politie overmeestert man"](#) by Shirley de Jong

Página 17: ["Palantir pavilion, World Economic Forum, Davos, Switzerland"](#) by Cory Doctorow

Página 18: ["manifest contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 \(1\)"](#) by Jeanne Menjoulet

Página 21: ["Gendarmerie"](#) by Eddy Meulemans

Página 22: ["Spanish Police Colibrí"](#) by José Luis Celada Euba

Página 23: ["IMG_4601"](#) by Public Collectors

Página 27: ["Greater Manchester Police - BMW R1200RTs"](#) by Autumn

Página 30: ["Salt City 21"](#) by Office of Public Affairs

Página 34: ["manifest contre la «Loi Sécurité](#)

[globale» à Paris le 28 novembre 2020 \(2\)"](#) by Jeanne Menjoulet

Página 37: ["VIDEO Überwachungsanlage"](#) by Christophe Stoll

Página 38: ["Torrevieja police vans ~ repeating patterns dailyshoot"](#) by Les Haines

Página 42: ["Protest against doublethink - a peace dove is a paraglider while genocide is self defence"](#) by Alisdare Hickson

Página 44: ["Brussels police \(2\)"](#) by Eoghan OLionnain

Página 46: ["#BlackLivesMatter protest in Stockholm, Sweden"](#) by Teemu Paananen

Página 48: ["IMG_0297"](#) by Steve Eason

Página 49: ["Police surveillance"](#) by York GreenParty

Página 53: ["_S9A0303"](#) ****by Steve Eason

Página 54: ["manifest contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 \(3\)"](#) by Jeanne Menjoulet

Página 56: ["Belgique - 21 juillet 2013 - Police - Politie - Polizei \(1\)"](#) by Antonio Ponte

Página 57: ["Belgique - 21 juillet 2013 - Police - Politie - Polizei \(2\)"](#) by Antonio Ponte

Páginas 58-61: ["Belgique - 21 juillet 2013 - Police - Politie - Polizei \(3\)"](#) by Antonio Ponte

Página 62: ["manifest contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 \(4\)"](#) Jeanne Menjoulet

Página 63: ["Fight Racism !"](#) by Alisdare Hickson

Notas

1 Article 3(1), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_3

2 To give just one example, the definition in the Act is substantially different from the one included in the initial proposal. See: ‘Proposal for a Regulation laying down harmonised rules on artificial intelligence’, 21 April 2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

3 Cabinet Office et al, ‘Ethics, Transparency and Accountability Framework for Automated Decision-Making’, 2021, <https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making/ethics-transparency-and-accountability-framework-for-automated-decision-making>

4 Cambridge Dictionary, ‘Machine learning’, <https://dictionary.cambridge.org/dictionary/english/machine-learning>

5 Amnesty International, ‘We Sense Trouble: automated discrimination and mass surveillance in predictive policing in the Netherlands’, 2020, <https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR3529712020ENGLISH.pdf>

6 Links to all the reports are available at: <https://statewatch.org/predictivepolicing>

7 Lawrence Sherman, ‘The Cost-Effectiveness of Evidence-Based Policing’, 2010, https://eso.expertgrupp.se/wp-content/uploads/2010/07/2010_3-Sherman.pdf

8 Patrick Perrot, ‘L’analyse du risque criminel : l’émergence d’une nouvelle approche’, *Revue de l’Électricité*

et de l’Électronique, REE 2014-5 SEE, 2014, https://www.researchgate.net/publication/274071556_L'analyse_du_risque_criminel_l'emergence_d'une_nouvelle_approche.

9 EDRI, ‘Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act’, 2022, <https://edri.org/our-work/civil-society-calls-on-the-eu-to-ban-predictive-ai-systems-in-policing-and-criminal-justice-in-the-ai-act/>

10 Links to all the reports are available at: <https://statewatch.org/predictivepolicing>

11 European Union Agency for Fundamental Rights, ‘Second European Union Minorities and Discrimination Survey - Main results’, 2017, page 26, 29, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-eu-midis-ii-main-results_en.pdf

12 European Union Agency for Fundamental Rights, ‘Being Black in the EU — Experiences of people of African descent’, 2023, <https://fra.europa.eu/en/publication/2023/being-black-eu>

13 France 24, ‘Police violence: How can France tackle racial profiling without first addressing race?’, 9 July 2023, <https://www.france24.com/en/americas/20230709-france-s-police-dilemma-how-to-combat-racial-profiling-without-talking-about-race>

14 Amnesty International, ‘YOU NEVER KNOW WITH PEOPLE LIKE YOU’: POLICE POLICIES TO PREVENT ETHNIC PROFILING IN BELGIUM’, May 2018, https://www.amnesty-international.be/sites/default/files/bijlagen/ethnic_profiling_executive_summary_en.pdf

15 Rights International Spain and Open Society Justice Initiative, ‘Under Suspicion: The Impact of Discriminatory Policing in Spain’, 2019, Report: <https://>

www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf; Video:

<https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain>

16 Arenas-García L and García-España E, 'Police stop and search in Spain: an overview of its use, impacts and challenges', March 2022, <https://indret.com/wp-content/uploads/2022/07/1715.pdf>

17 Bundeszentrale für Politische Bildung, 'Migration und Kriminalität – Erfahrungen und neuere Entwicklungen', 25 September 2020, <https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/301624/migration-und-kriminalitaet-erfahrungen-und-neuere-entwicklungen/#footnote-target-14>

18 Samantha Bielen, Peter Grajzl and Wim Marneffe, 'Blame Based on One's Name? Extralegal Disparities in Criminal Conviction and Sentencing', European Journal of Law and Economics, June 2021. DOI:[10.1007/s10657-020-09670-6](https://doi.org/10.1007/s10657-020-09670-6)

19 Dieter Burssens, Carrol Tange, and Eric Maes, 'A la recherche de determinants du recours a la detention preventive et de sa duree', Institut National de Criminalistique et de Criminologie, 2015

20 Each One Teach One (EOTO), Citizens For Europe (CFE), 'Afrozensus 2020, Perspektiven, Anti-Schwarze Rassismuserfahrungen und Engagement Schwarzer, afrikanischer und afrodiasporischer Menschen in Deutschland', 2021, <https://afrozensus.de/reports/2020/Afrozensus-2020.pdf> (translated from German)

21 Germany report

22 Palantir, 'Palantir reports Q4 2024 Revenue Growth', 2025, <https://investors.palantir.com/news-details/2025/Palantir-Reports-Q4-2024-Revenue-Growth-of-36-YY-U.S.-Revenue-Growth-of-52-YY-Issues-FY-2025-Revenue-Guidance-of-31-YY-Growth->

[Eviscerating-Consensus-Estimates/](#)

23 With early funding stemming from In-Q-Tel, the venture capital arm of the CIA, Palantir's customers include: the CIA, NSA, FBI, ICE and army in the US, as well as the NHS in Britain.

24 See here for more information on the company's involvement in the Israeli occupation of Palestine: <https://dimse.info/briefcam/>

25 See here for information on the use of ClearView software by US police: <https://www.bbc.co.uk/news/technology-65057011>

26 Edicia, <https://www.edicia.fr/fr/>

27 Risk Terrain Modelling, <https://www.riskterrainmodeling.com/about.html>

28 Eurocop, <https://www.eurocop.com/>. El Salto (2021), 'El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos'. 4 February 2021. <https://www.elsaltodiario.com/tecnologia/estado-policial-espanol-2.0-empresas-privadas--vigilar-ciudadanos>

29 Securitas, <https://www.securitas.com/en/>

30 See here for more information on SopraSteria's contract with the EU for the 'Shared Biometric Matching System' (sBMS): [https://www.soprasteria.com/newsroom/press-releases/details/idemia-and-sopra-steria-chosen-by-eu-lisa-to-build-the-new-shared-biometric-matching-system-\(sbms\)-for-border-protection-of-the-schengen-area](https://www.soprasteria.com/newsroom/press-releases/details/idemia-and-sopra-steria-chosen-by-eu-lisa-to-build-the-new-shared-biometric-matching-system-(sbms)-for-border-protection-of-the-schengen-area)

31 James Bamford, 'How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza', *The Nation*, 12 April 2024; 'Questions and Answers: Israeli Military's Use of Digital Tools in Gaza', *Human Rights Watch*, 10 September 2024, <https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza>

32 Forbes, 'Meet The Ex-NSA And Ex-Unit 8200 Spies Cashing In On Security Fears', 10 September 2014, <https://www.forbes.com/sites/>

[kashmirhill/2014/09/10/meet-the-ex-nsa-and-ex-unit-8200-spies-cashing-in-on-security-fears/](https://kashmirhill.com/2014/09/10/meet-the-ex-nsa-and-ex-unit-8200-spies-cashing-in-on-security-fears/)

33 One definition of surveillance tech includes the following wide range of technologies: video surveillance (CCTV systems, IP cameras, video analytics software), big data (data analytics tools for surveillance data, predictive analytics for crime prevention), police body cameras (wearable cameras for law enforcement, recording and storage solutions), biometrics (fingerprint recognition technology, voice recognition systems), domestic drones (aerial surveillance drones for personal use, drones equipped with cameras and sensors), face recognition technology, Radio Frequency Identification tagging, and Stingray tracking devices (for mobile devices and intercepting cellular communications), see: The Business Research Company, 'Surveillance Technology Market Report', 2025. <https://www.thebusinessresearchcompany.com/report/surveillance-technology-global-market-report>. According to this definition, this report covers only predictive analytics for crime 'prediction', and AI video surveillance.

34 Ibid.

35 Article 5, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_5

36 <https://statewatch.org/predictivepolicing>

37 Chapter II, Article 5(d), Article 3(1), AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_3

38 EU Commission, 'Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act', 4 February 2025, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>

39 Fair Trials, 'EU Parliament approves landmark AI law', 16 June 2023, <https://www.fairtrials.org/articles/news/eu-parliament-approves-landmark-ai-law/>

40 Investigate Europe 'France spearheads member state campaign to dilute European AI regulation', 22 January 2025 <https://www.investigate-europe.eu/posts/france-spearheads-member-state-campaign-dilute-european-artificial-intelligence-regulation>; TIME, 'Big Tech Is Already Lobbying to Water Down Europe's AI Rules', 21 April 2023, <https://time.com/6273694/ai-regulation-europe/>

41 European Digital Rights (EDRI), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptikon Foundation, and PICUM, 'Artificial Intelligence Act Amendments - Ensure meaningful transparency of AI systems for affected people', November 2021, https://panoptikon.org/sites/default/files/meaningful_transparency_for_people_affected_by_ai_art_52_aia_without_amendment_text.pdf

42 Article 86, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_86

43 Article 50, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_50

44 European Digital Rights (EDRI), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptikon Foundation, and PICUM 'Artificial Intelligence Act Amendments - Ensure rights and redress for people impacted by AI systems', November 2021, <https://edri.org/wp-content/uploads/2022/05/Rights-and-Redress-AIA-Amendments-for-online.pdf>

45 Article 85, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_85

46 Germany report; Belgium report, France report. France in particular has weak freedom of information laws and performs poorly in the global 'freedom of information' index.

47 Spain report

- 48 Germany report
- 49 Braga, Anthony A., Barao, Lisa, ‘Targeted Policing for Crime Reduction’, Handbook on Crime and Deviance, Handbooks of Sociology and Social Research, Springer, 2019, https://doi.org/10.1007/978-3-030-20779-3_17
- 50 EU Commission, ‘Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act’, 4 February 2025, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>
- 51 Germany report
- 52 Knobloch, Tobias, ‘Vor die Lage kommen: Predictive Policing in Deutschland’, Stiftung Neue Verantwortung, 29 August 2018, https://www.stiftung-nv.de/sites/default/files/predictive_policing.pdf
- 53 Germany report
- 54 Germany report
- 55 Camacho-Collados, M., & Liberatore, F, ‘A decision support system for predictive police patrolling’. *Decision support systems*, 75, 25-37, 2015, <https://www.sciencedirect.com/science/article/abs/pii/S0167923615000834>
- 56 El Salto, ‘El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos’, 4 February 2021, **Error! Hyperlink reference not valid.**
- 57 France report
- 58 Belgium report
- 59 Orbit GIS, ‘Zones de police’, <https://www.orbitgis.com/fr/zone-de-police>
- 60 *The Markup*, ‘Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them’, 2021, <https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them>
- 61 Florian Gauthier, ‘Prédire les vols de voitures ?’, *Etalab blog*, 2018, <https://www.etalab.gouv.fr/predire-les-vols-de-voitures>
- 62 Abgeordnetenhaus Berlin, ‘Bericht des Senats gemäß § 21 Absatz 4 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) für das Jahr 2021’, 22 July 2022, <https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/DruckSachen/d19-0444.pdf> (translated from German)
- 63 France report
- 64 Germany report
- 65 Germany report, interview with Egbert, Simon, Postdoctoral Researcher ‘The Future of Prediction’, University of Bielefeld, 04 October 2023
- 66 Haco. ‘Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit’, *De Standaard*. 17 May 2016, https://standaard.be/cnt/dmf20160517_02292901
- 67 El Salto, ‘El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos’, 4 February 2021, **Error! Hyperlink reference not valid.**
- 68 Polizei Berlin, ‘Kriminalitätsbelastete Orte’, **Error! Hyperlink reference not valid.**
- 69 Orbit gis. ‘Zones de police’, <https://web.archive.org/web/20230930192819/https://www.orbitgis.com/fr/zone-de-police>; Orbit gis, ‘Zones de police – Stratégie’, https://www.orbitgis.com/fr/zone-de-police/zp_strategie
- 70 Haco. ‘Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit’. *De Standaard*. 17 May 2016, https://standaard.be/cnt/dmf20160517_02292901
- 71 France report
- 72 Eurocop, ‘Analysis and prediction of crime’, <https://www.eurocop.com/sistemas-de-eurocop/analisis-y-prediccion-del-delito/>
- 73 Minister of Interior’s answer of 09/07/2020 to written question n°7-591. *Belgian Senate*,

<https://senate.be/www/?Mlval=/Vragen/SVPrintNLFR&LEG=7&NR=591>

74 France report

75 France report

76 Quijano-Sánchez, L, 'Applications of AI and Data Science in Policing: 7 years of collaborations with the Spanish Police'. Lara Quijano-Sánchez, Ph.D by the Politechnic School of the Universidad Autónoma de Madrid. 25 January 2022, <https://www.youtube.com/watch?v=z8uBNNPtUmE>; Liberatore, F., Camacho-Collados, M., & Quijano-Sánchez, L, 'Towards social fairness in smart policing: Leveraging territorial, racial, and workload fairness in the police districting problem', *Socio-Economic Planning Sciences*, 87, 101556, 2023, <https://www.sciencedirect.com/science/article/pii/S0038012123000563#sec5>

77 Ibid.

78 Article 10, Law Enforcement Directive, <https://eur-lex.europa.eu/eli/dir/2016/680/oj>

79 Recital 38 and Article 11, Law Enforcement Directive, <https://eur-lex.europa.eu/eli/dir/2016/680/oj>

80 German report, France report, Belgium report.

81 Polizei Berlin, 'Kriminalitätsbelastete Orte', <https://www.berlin.de/polizei/polizeimeldungen/fakten-hintergruende/artikel.1078268.php>, (translated from German)

82 France report

83 Lina Schmid, 'Grundrechte in Gefahr(engebieten). Verfassungsrechtliche Beurteilung der polizeilichen Praxis "kriminilitätsbelasteter Orte", 2023, in *Mythos Generalverdacht. Wie mit dem Mythos Clankriminalität Politik gemacht wird*, Nautilus Flugschrift, p.167, translated from German.

84 Süddeutsche Zeitung, 'Unbeteiligte geraten ins Kontrollraster', 12 Sept 2014, <https://www.sueddeutsche.de/wirtschaft/ueberwachung-mit-predictive->

[policing-unbeteiligte-geraten-ins-kontrollraster-1.2115126](#) (translated from German)

85 Lina Schmid, 'Grundrechte in Gefahr(engebieten). Verfassungsrechtliche Beurteilung der polizeilichen Praxis "kriminilitätsbelasteter Orte", 2023, in *Mythos Generalverdacht. Wie mit dem Mythos Clankriminalität Politik gemacht wird*, Nautilus Flugschrift, p.167, translated from German

86 Wrangelkiez United, 'Perspektiven: Realitäten von Geflüchteten', Video, <https://wrangelkiezunited.noblogs.org/home/>, translated from German

87 Ibid

88 George L. Kelling and James Q. Wilson, *The Atlantic*, 'Broken Windows: The Police and Neighbourhood Safety', 1982, <https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/>

89 Donna Ladd, 'Inside William Bratton's NYPD: broken windows policing is here to stay', *The Guardian*, 2015, <https://www.theguardian.com/us-news/2015/jun/08/inside-william-bratton-nypd-broken-windows>

90 'Northeastern University researchers find little evidence for 'broken windows theory', say neighborhood disorder doesn't cause crime', *Northeastern Global News*, 15 May 2019, <https://news.northeastern.edu/2019/05/15/northeastern-university-researchers-find-little-evidence-for-broken-windows-theory-say-neighborhood-disorder-doesnt-cause-crime/>

91 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025, <https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf>

92 Risk Terrain Modelling, 'Spatial dynamics of crime', <https://www.riskterrainmodeling.com/overview.html>

93 Ibid.

- 94 Following its closure in 2020, part of the *Observatoire*'s activities have been transferred to the French Ministry of the Interior's *Service Statistique Ministériel de la Sécurité Intérieure* (SSMSI, part of the *Institut des hautes études du ministère de l'Intérieur* or IHEMI, created in September 2020).
- 95 Camille Gosselin, 'La police prédictive : enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique', Paris: IAU Île-de-France, 2019, https://www.institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf
- 96 Belgium report
- 97 Sûreté Globale website, <https://web.archive.org/web/20230610153444/https://www.sureteglobale.org>
- 98 France report
- 99 Risk Terrain Modelling, 'Spatial dynamics of crime', <https://www.riskterrainmodeling.com/overview.html>
- 100 Thibault Sardier, 'Cartographie criminelle : surveiller et prédire', *lemonde.fr*, 5 January 2018, https://www.lemonde.fr/idees/article/2018/01/05/cartographie-criminelle-surveiller-et-predire_5237723_3232.html
- 101 Anneleen Rummens & Wim Hardyns, 'Comparison of near-Repeat, Machine Learning and Risk Terrain Modeling for Making Spatiotemporal Predictions of Crime'. *Applied Spatial Analysis and Policy*, 2021, Vol. 13, no. 4, pp. 1035–1053. DOI: 10.1007/s12061-020-09339-2
- 102 International terrorism database, <https://www.start.umd.edu/gtd/access/>. It shows that France only has 20 entries from 2016 to 2019, which leaves one wondering about the relevance of this dataset.
- 103 France report
- 104 France report
- 105 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025, <https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf>
- 106 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025, <https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf> p.69
- 107 Ibid.
- 108 Ibid.
- 109 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 09 September 2021, **Error! Hyperlink reference not valid.;**
- 110 Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, *Justice, Power and Resistance*, 5(3), 227-248, <https://doi.org/10.1332/UBQA2752>
- 111 AlgorithmWatch, 'The Rise and Fall of a Predictive Policing Pioneer', 7 November 2024, <https://algorithmwatch.org/en/predictive-policing-pioneer-keycrime/>; Wired, 'Perché la più avanzata startup italiana di polizia predittiva è sull'orlo del baratro', 31 January 2024, <https://www.wired.it/article/polizia-predittiva-keycrime-startup-ai-act/>
- 112 Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, *Justice, Power and Resistance*, 5(3), 227-248, <https://doi.org/10.1332/UBQA2752>
- 113 Ibid.
- 114 AlgorithmWatch, 'Automating Society Report 2020 — Swiss Edition', January 2021, <https://automatingsociety.algorithmwatch.org/report2020/switzerland/>
- 115 Belgium report

- 116 Williams, P, 'Criminalising the Other: challenging the race-gang nexus', *Race & Class*, 2014, 6(3), 18-35. <https://doi.org/10.1177/0306396814556221>
- 117 Belgium report
- 118 The terms 'terrorist', 'terrorism', 'Islamist', 'extremism', 'extremist' and 'radicalisation' are ill-defined, imprecise and easily misused. As they routinely appear in laws, policies, government statements and academic research, however, they are used in this report for ease of reference. This does not imply that their use or definition by government institutions is endorsed. Per Amnesty UK, 'This Is The Thought Police: The Prevent duty and its chilling effect on human rights', November 2023, <https://www.amnesty.org.uk/files/2023-11/Amnesty%20UK%20Prevent%20report%20%281%29.pdf>
- 119 Belgium report
- 120 'EU: Definition of "potential terrorists" opens door to broad information-sharing', *Statewatch*, 2 October 2024, <https://www.statewatch.org/news/2024/october/eu-definition-of-potential-terrorists-opens-door-to-broad-information-sharing/>
- 121 Bundeskriminalamt, 'RADAR (Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos)', https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/Radar/radar_node.html
- 122 Eticas Research, 'The external audit of the VioGen system', 8 March 2022; Bayona, J. Z. (2014). *Violencia contra la mujer: marco histórico evolutivo y predicción del nivel de riesgo* (Doctoral dissertation, Universidad Autónoma de Madrid), <https://dialnet.unirioja.es/servlet/tesis?codigo=43479>
- 123 Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M, 'Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police', *Knowledge-Based Systems*, 2018, 149, 155-168, <https://www.sciencedirect.com/science/article/abs/pii/S095070511830128X?via%3Dihub>; Nature, 'Police use a computer to expose false testimony', 30 May 2018, <https://www.nature.com/articles/d41586-018-05285-9>
- 124 Civio, 'Spanish National Police stop using Veripol, its star AI for detecting false reports', 25 March 2025 <https://civio.es/transparencia/2025/03/25/national-police-stop-using-veripol-its-star-ai-for-detecting-false-reports/>
- 125 Germany report; 'PNR for all: UN Security Council mandates worldwide air travel surveillance and profiling, biometric collection, terrorist watchlists', *Statewatch*, 8 January 2018, <https://www.statewatch.org/news/2018/january/un-pnr-for-all-un-security-council-mandates-worldwide-air-travel-surveillance-and-profiling-biometric-collection-terrorist-watchlists/>
- 126 Germany report.
- 127 Tony Bunyan, 'EU: The surveillance of travel where everyone is a suspect', *Statewatch*, August 2008, <https://www.statewatch.org/media/documents/analyses/no-70-eu-travel-surveillance.pdf>
- 128 European Commission, 'ProtectEU: a European Internal Security Strategy', COM(2025) 148 final, 1 April 2025, https://home-affairs.ec.europa.eu/document/download/48218e1a-9e03-4be1-b19c-d04c323c1117_en?filename=ProtectEU-European-Internal-Security-Strategy_en.pdf
- 129 Senate, 'Orden de servicio 3/2018', February 2018, <https://www.senado.es/web/expedientappendixblobervlet?legis=12&id1=119003&id2=1>
- 130 Andrés Pueyo, A., Arbach Lucioni, K., & Redondo, S., 'The RisCanvi: a new tool for assessing risk for violence in prison and recidivism', *Handbook of recidivism risk/needs assessment tools*, 2018, 255-268, <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119184256.ch13>; AlgorithmWatch (2021), 'In Catalonia,

the RisCanvi algorithm helps decide whether inmates are paroled', 25 May 2021, <https://algorithmwatch.org/en/riscanvi/>

131 Justizportal Nordrhein-Westfalen, § 25a HSOG Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) Landesrecht Hessen, https://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?xid=169564,130; Gesellschaft für Freiheitsrechte, 'NRW Assembly Act: Threat to freedom of assembly and civil-society', <https://freiheitsrechte.org/en/themen/demokratie/vb-versammlungsrecht-nrw>

132 Germany report

133 Harry Davies, Bethan McKernan, Dan Sabbagh. 'The Gospel': how Israel uses AI to select bombing targets in Gaza', *The Guardian*, 1 December 2023, www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets

134 Rights International Spain and Open Society Justice Initiative, 'Under Suspicion: The Impact of Discriminatory Policing in Spain', 2019. Report: <https://www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf>; Video:

<https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain>; Arenas-García L and García-España E, 'Police stop and search in Spain: an overview of its use, impacts and challenges', March 2022, <https://indret.com/wp-content/uploads/2022/07/1715.pdf>

135 Bundeszentrale für Politische Bildung, 'Migration und Kriminalität – Erfahrungen und neuere Entwicklungen', 25 September 2020, <https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/301624/migration-und-kriminalitaet-erfahrungen-und-neuere-entwicklungen/#footnote-target-14>

136 Jérémiah Vervoort, 'I-Police ou l'art de prédire la discrimination', Travail de fin d'études, Brussels: Université libre de Bruxelles, 2021

137 CERD, 'Concluding observations on the sixteenth to nineteenth periodic reports of Belgium', *United Nations Committee on the Elimination of Racial Discrimination*. cerd/c/bel/co/16-19, 2014, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%2F16-19

138 Germany report

139 Welt, 'So funktioniert das Radar für radikale Islamisten', 12 June 2017, <https://www.welt.de/politik/deutschland/plus165451390/So-funktioniert-das-Radar-fuer-radikale-Islamisten.html>

140 Germany report

141 Germany report

142 Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M. (2018), 'Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police', *Knowledge-Based Systems*, 149, 155-168, <https://www.sciencedirect.com/science/article/abs/pii/S095070511830128X?via%3Dihub>

143 Eticas Research, 'The external audit of the VioGen system', 8 March 2022.

144 Eticas Research, 'The external audit of the VioGen system', 8 March 2022.

145 Tagesschau, 'Immer mehr rechte Gefährder', 26 June 2022, <https://www.tagesschau.de/inland/rechte-gefaehrder-103.html>

146 Belgium report

147 Germany report

148 Germany report

149 Germany report

150 Secretary of State for Security, 'Instruction nº 7/2016', 8 July 2016, <https://violenciagenero.igualdad.gob.es>

151 Bayona, J. Z, *Violencia contra la mujer: marco histórico evolutivo y predicción del nivel de riesgo* (Doctoral dissertation, Universidad Autónoma de Madrid), 2014, <https://dialnet.unirioja.es/servlet/tesis?codigo=43479>

152 Kanzlei Redecker Sellner Dahs, 'Stellungnahme an das Verwaltungsgericht Wiesbaden', 09 September 2021

153 Secretary General of Penitentiary Institutions, Ministry of Interior, 'Construcción y validación de una herramienta de clasificación y de valoración del riesgo de radicalismo violento en el ámbito penitenciario', 2021 https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/instituciones-penitenciarias/Construccion-y-validacion-de-una-herramienta-de-clasificacion-y-de-valoracion-del-riesgo-de-radicalismo-violento-en-el-ambito-penitenciario_126210405.pdf

154 *Ibid*

155 Karimi-Haghighi, M., & Castillo, C., 'Efficiency and fairness in recurring data-driven risk assessments of violent recidivism', In *Proceedings of the 36th Annual ACM Symposium on Applied Computing* (pp. 994-1002), March 2021 https://chato.cl/papers/karimi_haghighi_castillo_2021_efficiency_fairness_temporal_recurring.pdf

156 Ministry of Interior, 'Statistical data Viogen', September 2023, <https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/violencia-contra-la-mujer/estadisticas/2023/Estadistica-Septiembre-2023.pdf>

157 Germany report

158 Germany report

159 Germany report

160 MDR, 'Sachsen-Anhalt will Polizei-Gewahrsam bei Terrorverdacht verlängern', 17 December 2023 <https://www.mdr.de/nachrichten/sachsen-anhalt/>

161 *Ibid*

162 Tagesspiegel, 'Neue Plätze für 40 Straftäter – im Abschiebeknast', 31 January 2024, <https://www.tagesspiegel.de/berlin/losung-fur-berliner-massregelvollzug-neue-platze-fur-40-straftater-im-abschiebeknast-11137660.html>

163 Tagesschau, 'Warum die Abschiebepläne kaum einzuhalten sind', 04 October 2022, <https://www.tagesschau.de/investigativ/ndr-wdr/koalition-abschiebungen-gefahrder-101.htm>

164 Deutscher Bundestag, 'Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökyay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE, Drucksache 19/5202, Personenpotentiale islamistischer „Gefährder“', 9 November 2018, <https://dserver.bundestag.de/btd/19/056/1905648.pdf> (translated from German)

165 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025 <https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf?VersionId=JqCcTODw37yAXyINmAY6uAzrKEWucFF7>

166 The Conversation, 'A black box' AI system has been influencing criminal justice decisions for over two decades — it's time to open it up', 26 July 2023, <https://theconversation.com/a-black-box-ai-system-has-been-influencing-criminal-justice-decisions-for-over-two-decades-its-time-to-open-it-up-200594>; 'UK: Over 1,300 people profiled daily by Ministry of Justice AI system to 'predict' re-offending risk', *Statewatch*, 9 April 2025, <https://www.statewatch.org/news/2025/april/uk-over-1-300-people-profiled-daily-by-ministry-of-justice-ai-system-to-predict-re-offending-risk/>

167 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 09 September 2021, **Error! Hyperlink reference not valid.**

168 Ibid.

169 Fair Trials, 'My sons were profiled by a racist predictive policing system — the AI Act must prohibit these systems', 28 September 2022, <https://medium.com/@FairTrials/my-sons-were-profiled-by-a-racist-predictive-policing-system-the-ai-act-must-prohibit-these-b2ea66a9a763>

170 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 9 September 2021, <https://www.fairtrials.org/articles/publications/automating-injustice/>; Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, *Justice, Power and Resistance*, 5(3), 227-248, <https://doi.org/10.1332/UBQA2752>

171 La Quadrature du Net, 'Non à la vidéosurveillance algorithmique, refusons l'article 7 de la loi olympique!', 18 January 2023, <https://www.laquadrature.net/2023/01/18/non-a-la-videosurveillance-algorithmique-refusons-larticle-7-de-la-loi-olympique/>

172 See the 'Law Enforcement and Corrections' webpage on the ISS website: <https://issivs.com/served-verticals/law-enforcement-and-corrections/>

173 El País, 'Marbella, el mayor laboratorio de videovigilancia de España', 22 November 2019, https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html

174 La Vanguardia, 'Madrid has 83 cameras on the streets with artificial intelligence Surveillance', 9 January 2025 <https://www.lavanguardia.com/mediterranean/20250109/10268393/madrid-83-cameras-street-artificial-intelligence-surveillance-install-mayor-martinez-almeida-spain-city-council-police-technology.html>

175 Nicolas Bocquet, 'The Brussels Smart City: how "intelligence" can be synonymous with video surveillance'. *Brussels Studies*, 2021, journals.openedition.org/brussels/5678

176 La Quadrature du Net, 'France becomes the first European country to legalize biometric surveillance' 29 March 2023, <https://www.laquadrature.net/en/2023/03/29/france-becomes-the-first-european-country-to-legalize-biometric-surveillance/>

177 Jacobin, 'Emmanuel Macron Is Using the 2024 Olympics to Make France a Surveillance State', 21 March 2023 <https://jacobin.com/2023/03/emmanuel-macron-2024-olympics-surveillance-state-ai-biometric-system>

178 Jacobin, 'France Wants to Make Olympics-Style Surveillance Permanent', 23 October 2024 <https://jacobin.com/2024/10/france-olympics-surveillance-ai-policing>

179 ID Tech Editorial Team, 'French Court Rules Briefcam's AI Surveillance System Unlawful', 31 January 2025, <https://idtechwire.com/french-court-rules-briefcams-ai-surveillance-system-illegal/>

180 Ibid.

181 Ministerium der Justiz des Landes Nordrhein-Westfalen, 'Bericht zum TOP „Todesfälle und Suizide im Strafvollzug. 84. Sitzung des Rechtsausschusses des Landtags Nordrhein-Westfalen am 27.10.2021', 25 October 2021. www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-5871.pdf

182 Ibid.

183 Germany report

184 Niedersächsischer Landtag, 'Antrag, Einsatz künstlicher Intelligenz zur Suizidprävention und Verbesserung der Sicherheit in niedersächsischen Justizvollzugsanstalten', Drucksache 18/8729, 09 March 2021, <https://www.landtag-niedersachsen.de/Drucksachen/>

[Drucksachen_18_10000/08501-09000/18-08729.pdf](#), translated from German

185 Landesbeauftragte für den Datenschutz Niedersachsen, '27. Tätigkeitsbericht 2021', 2021, <https://www.lfd.niedersachsen.de/startseite/infothek/tatigkeitsberichte/2021/barbara-thiel-stellt-tatigkeitsbericht-2021-vor-212174.html>, translated from German

186 Germany report

187 Barrett, L. F. et al., 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements', *Psychological Science in the Public Interest*, 20(1), 1-68, 2019. <https://journals.sagepub.com/doi/10.1177/1529100619832930>

188 Rhue, Lauren, 'Racial Influence on Automated Perceptions of Emotions', 9 November 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765

189 Article 19, 'Emotional Entanglement: China's emotion recognition market and its implications for human rights', 19 November 2020

190 Germany report

191 AlgorithmWatch, 'Spanish Inmates Not to Be Automatically Monitored in Fear of AI Act', 28 March 2024 <https://algorithmwatch.org/en/spanish-inmates-not-monitored-in-fear-of-ai-act/>

192 Belgium report

193 Statewatch, 'France: Green light for police surveillance of political opinions, trade union membership and religious beliefs', 13 January 2021, <https://www.statewatch.org/news/2021/january/france-green-light-for-police-surveillance-of-political-opinions-trade-union-membership-and-religious-beliefs/>

194 France report

195 France report

196 Camille Gosselin, 'La police prédictive : enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique', (Paris: IAU Île-de-France, 2019), [https://www.](https://www.institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf)

[institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf](https://www.institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf)

197 Ibid

198 Didier Paris and Pierre Morel-À-L'Huissier, 'Rapport sur les fichiers mis à la disposition des forces de sécurité', Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République (Paris: Assemblée Nationale, Commission des Lois), October 2018, <http://www.assemblee-nationale.fr/15/rap-info/i1335.asp>

199 La Quadrature du Net, 'La reconnaissance faciale des manifestants est déjà autorisée', 18 November 2019, <https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/>

200 France report

201 Statewatch/Platform for International Cooperation on Undocumented Migrants, 'Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status', 18 November 2019, <https://www.statewatch.org/publications/reports-and-books/data-protection-immigration-enforcement-and-fundamental-rights-what-the-eu-s-regulations-on-interoperability-mean-for-people-with-irregular-status/>

202 France report

203 Sainz de la Maza Quintanal, E, "'Ultima ratio": el proceso de expulsión de inmigrantes en situación irregular en España', 2015, <https://docta.ucm.es/entities/publication/769b2a6c-8db4-4e2f-8f8e-623cb7c9ce6c>

204 Valdivia, A., & Tazzioli, M, 'Datafication Genealogies beyond Algorithmic Fairness: Making Up Racialised Subjects', in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (pp. 840-850), June 2023, <https://doi.org/10.1145/3593013.3594047>

205 Belgium report, Germany report, France report

- 206 Matthias Monroy, ‘Suspicion files: German police databases on political activists’, *Statewatch*, 10 April 2018, <https://www.statewatch.org/analyses/2018/suspicion-files-german-police-databases-on-political-activists/>
- 207 Belgium report
- 208 Belgium report
- 209 Belgium report
- 210 Rights International Spain and Open Society Justice Initiative, ‘Under Suspicion: The Impact of Discriminatory Policing in Spain’, 2019. Report: <https://www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf>; Video: <https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain>
- 211 Belgium report, France report
- 212 Belgium report
- 213 Belgium report, France report
- 214 Reuters, ‘In a U.S. first, California city set to ban predictive policing’, 19 June 2020, <https://www.reuters.com/article/us-usa-police-tech-trfn/in-a-us-first-california-city-set-to-ban-predictive-policing-idUSKBN23O31A/>
- 215 EDRI, ‘Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act’, 1 March 2022, <https://edri.org/our-work/civil-society-calls-on-the-eu-to-ban-predictive-ai-systems-in-policing-and-criminal-justice-in-the-ai-act/>
- 216 <https://technopolice.fr/>
- 217 <https://technopolice.be/>
- 218 <https://www.openrightsgroup.org/campaign/safety-not-surveillance/>
- 219 <https://stoplapdspying.org/>