ARANZADI

El diseño de perfiles algorítmicos para la gestión y protección de fronteras europeas: ¿una nueva forma de discriminación?.

BIB 2021\5369

Jonatán, Cruz Ángeles. Profesor ayudante doctor en el Área de Derecho internacional público y Relaciones internacionales. Universidad de Jaén

Publicación:

Revista Aranzadi de Derecho y Nuevas Tecnologías num.57/2021
Editorial Aranzadi, S.A.U.

Resumen
«Este estudio parte del análisis de los grandes sistemas IT o bases de datos, encargados de recopilar la información de los viajeros –regulares e irregulares– que entran o salen de la Unión Europea. Estos sistemas recogen cada vez más información y, aunque la normativa comunitaria establece cómo deben tratarse estos datos, todavía se plantean algunos riesgos de violación de principios jurídicos consolidados, tales como el de igualdad y no discriminación. De modo que, en este artículo, nos centraremos en cómo estos programas informáticos, cada vez más avanzados, perciben a los viajeros y en cómo, mediante el uso de la información recopilada y su tratamiento mediante algoritmos estadísticos, pueden clasificarlos como un posible riesgo para el orden, seguridad y salud pública.»
Abstract: «This study is based on the analysis of the large IT systems or databases, responsible for collecting information on travelers –regular and irregular– entering or leaving the European Union. These systems collect more and more information and, although EU regulation establish how this data should be treated, there are still some risks of violation of established legal principles, such as equality and non-discrimination. So in this paper, we will focus on how these increasingly advanced computer programs perceive travelers and how, through the use of the information collected and its treatment through statistical algorithms, they can classify them as a possible risk for order, safety and public health.»

Palabras clave
Protección, fronteras, Unión Europea, perfiles, algorítmicos.
Protection, borders, European Union, algorithmic, profiling.

SUMARIO

I. Introducción

En los últimos años, está aumentando el número de herramientas y aplicaciones que se sirven del análisis de datos como una nueva práctica de creación de conocimiento, con todo tipo de usos y utilidades en nuestra vida cotidiana[1] –desde las aparentemente más banales, como es el caso de las famosas *cookies* [2], que analizan nuestro rastro en internet, con el fin de elaborar perfiles para ofrecernos aquellos productos que pueden adaptarse a nuestros gustos, a los *software* más sofisticados de elaboración de perfiles de riesgo, que tratan de predecir posibles peligros en nuestras fronteras, y que analizaremos en este artículo–. Estas nuevas tecnologías, han permitido a la Unión Europea, reformular sus políticas de seguridad –diseñadas tras los atentados terroristas del 11 de septiembre de 2011–, perfeccionando la recopilación, el análisis y la minería predictiva de datos.

1 Para un estudio más detallado sobre aplicaciones basadas en análisis de datos y el uso de algoritmos para la creación de perfiles, que utilizamos en nuestra vida diaria, *vid.* GARCÍA ALLER, M.; *Lo imprevisible. Todo lo que la tecnología quiere y no puede controlar* , editorial Planeta, Barcelona, 2020, en la línea de GARCÍA ALLER, M.; *El fin del mundo tal y como lo conocemos. Las grandes innovaciones que van a cambiar tu vida* , editorial Planeta, Barcelona, 2017.

2 El anglicismo *cookie* , conocido también galleta o galleta informática, es un término que hace referencia a una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador. Sus principales funciones son: recordar accesos y conocer información sobre los hábitos de navegación, e intentos de spyware –programas espías–, principalmente por parte de agencias de publicidad. Esto puede causar problemas de privacidad y es una de las razones por las que las cookies tienen sus detractores.

Esta tendencia se vio plasmada en el Programa de Estocolmo[3], que establecía un plan de trabajo para la Unión Europea (UE) en el espacio de libertad, seguridad y justicia (ELSJ) para el periodo 2010-2014. Dicho programa planteaba como uno de sus objetivos "mejorar las herramientas de trabajo en términos de interoperabilidad de las bases de datos con el fin de permitir a los organismos encargados de hacer cumplir la ley hacer frente al terrorismo y a la delincuencia grave". La idea es sencilla. Se trata de conectar todas las bases de datos desarrolladas hasta la fecha en el ELSJ, con el fin de poder crear un portal común, desde el que poder gestionar toda la información de aquellas personas que cruzan las fronteras exteriores de la UE. A partir de la información extraída de estas grandes bases de datos (*big data*), utilizando la minería predictiva de datos (*data mining*), se desarrollan modelos predictivos para hacer estimaciones sobre pronósticos futuros. En este caso, se pretende desarrollar una serie de "perfiles de riesgo", que nos permitan predecir si una persona puede suponer una amenaza para la seguridad, la salud o el orden público.

3 El Programa de Estocolmo es un plan estratégico quinquenal para incrementar y consolidar la seguridad –particularmente la seguridad ciudadana– en el interior del territorio de la Unión Europea. Fue presentado conjuntamente por la Presidencia sueca del Consejo y por la Comisión Europea, y adoptado por el Consejo Europeo, en 2009, y su ámbito de aplicación está diseñado entre 2010 y 2015.

Hasta la fecha (2021), estas grandes bases de datos se han venido utilizando en

distintos procesos relacionados con la migración, aunque trabajando de forma totalmente aislada, las unas de las otras. Por este motivo, la UE está trabajando para conseguir la "interoperabilidad" entre sus grandes bases de datos. Éstas pueden clasificarse en dos grandes categorías: (1) aquellas bases de datos capaces de identificar a una persona estableciendo correspondencias de datos alfanuméricos con información ya introducida en el sistema y (2) aquellos instrumentos, creados al amparo del Derecho de la Unión Europea, que contemplan el uso de estadísticas derivadas de sus datos para generar perfiles de riesgo.

En el marco del ELSJ, contamos con un total de seis grandes bases de datos, capaces de identificar a una persona cruzando su información y estableciendo correspondencias. En primer lugar, el Sistema de Información Schengen –mejorado– de segunda generación (SIS II)[4], que sirve para introducir y procesar alertas sobre personas buscadas, desaparecidas o de terceros países con el fin de proteger la seguridad y el orden público, así como también sirve para poder denegar la entrada o la estancia sujetas a una decisión de retorno. En segundo lugar, el Sistema de Información de Visados (VIS)[5], que facilita el intercambio de datos entre Estados miembros de Schengen sobre solicitudes de visados. En tercer lugar, el Sistema dactiloscópico europeo (Eurodac)[6]que determina el Estado miembro responsable de examinar una solicitud de protección internacional y ayudar a controlar la inmigración y los movimientos secundarios irregulares. En cuarto lugar, el Sistema de Entrada y Salida (SES)[7], que calcula y controla la duración de la estancia autorizada de inmigrantes y localiza a quienes la sobrepasan. En quinto lugar, el Sistema de Información Anticipada sobre los Pasajeros (API)[8], que recoge y trata los datos de pasajeros extracomunitarios, con fines de gestión de fronteras y acción policial. Y, en sexto lugar, el Sistema de Información de Antecedentes Penales para nacionales de terceros países (ECRIS-TCN)[9], que comparte información sobre condenas anteriores de ciudadanos extracomunitarios.

4 Sistema de Schengen de segunda generación (SIS II) regulado por la Decisión 2007/533/JAI y el Reglamento n.º 1987/2006. Ambas normas comparten una serie de elementos comunes que se completan con un conjunto de normas específicas que delimitan el uso del sistema en el ámbito concreto de competencias cada uno de los instrumentos.

5 Sistema de Información de Visados (VIS), regulado por el Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo de 9 de julio de 2008; modificado por: Reglamento (CE) n.º 810/2009 del Parlamento Europeo y del Consejo de 13 de julio de 2009; Reglamento (UE) n.º 610/2013 del Parlamento Europeo y del Consejo de 26 de junio de 2013; Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo de 30 de noviembre de 2017; y Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo de 20 de mayo de 2019. Corregido por: Rectificación, DO L 284, de 12 de noviembre de 2018, p. 39 (767/2008); Rectificación, DO L 284, de 12 de noviembre de 2018, p. 38 (810/2009); y por Rectificación DO L, de 3 de mayo de 2019, p. 14 (2017/2226).

6 Sistema dactiloscópico europeo (Eurodac), regulado por el Reglamento (UE) n.º 603/2013 relativo a Eurodac: la base de datos dactiloscópicos de los solicitantes de asilo de la Unión Europea para comparar sus impresiones dactilares; y Reglamento (UE) n.º 604/2013 –también conocido como Dublín III– por el que se establecen las normas de determinación del país de la UE responsable del examen de una solicitud de asilo.

7 Sistema de Entrada y Salida (SES), regulado por el Reglamento (UE) n.º 2017/2226 del Parlamento

Europeo y del Consejo, de 30 de noviembre de 2017, sobre el establecimiento de un sistema de entrada/salida (SES) para registrar los datos de entrada y salida y los datos de denegación de entrada de los nacionales de terceros países que cruzan las fronteras exteriores de los Estados miembros y la determinación de las condiciones de acceso al SES con fines policiales, y la modificación del Convenio de aplicación del Acuerdo y los Reglamentos de Schengen (CE) n.º 767/2008 y (UE) n.º 1077/2011 . Modificado por: Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo de 13 de septiembre de 2018; Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019. Corregido por: Rectificación, DO L 258, de 15 de octubre de 2018, p. 5 (2017/2226); y Rectificación DO L 117, de 3 de mayo de 2019, p. 14 (2017/2226).

8 Sistema de Información Anticipada sobre los Pasajeros (API), regulado por: Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

9 Sistema de Información de Antecedentes Penales para nacionales de terceros países (ECRIS-TCN) regulado por: Reglamento (UE) 2019/816 por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas.

En el presente artículo, más allá del estudio de la interoperabilidad de las bases de datos enumeradas anteriormente que, sin duda, puede servir para dotar al agente o guarda de fronteras de una información más completa –que ya de por sí pueden generar una serie de riegos para la protección de los derechos fundamentales[10] –, nos centraremos en el análisis del funcionamiento de dos grandes sistemas que son capaces de aplicar estadísticas derivadas de los datos almacenados para generar perfiles de riesgo. Éstas sí permiten la detección de "sospechosos", al contener una funcionalidad de elaboración algorítmica de perfiles que identifica a personas que pueden ser de interés para las autoridades policiales y de gestión de fronteras. En primer lugar, el Sistema Europeo de Información y Autorización de Viajes (SEIAV)[11], que evalúa si un ciudadano extracomunitario exento de visado entraña un riesgo para la seguridad, la migración irregular o la salud pública. Adoptado en 2018, este sistema compara automáticamente la información facilitada por los viajeros durante el proceso de solicitud con las bases de datos pertinentes de la Unión Europea y de ámbito internacional, sirviéndose de un conjunto "indicadores de riesgo" contenidos en el propio sistema. Un algoritmo desarrollado por Frontex compara el perfil individual del viajero –basado en indicadores como la edad, el sexo, la nacionalidad, el lugar de residencia, el nivel académico y la profesión– con estos indicadores de riesgo para determinar si la solicitud debe remitirse a una revisión manual –realizado por un agente o guarda de fronteras competente–. En segundo lugar, el Registro de Nombres de los Pasajeros (RNP o PNR)[12], que recoge, trata e intercambia datos de pasajeros de vuelos extracomunitarios. Estos datos son recogidos por empresas de transporte aéreo, a partir de información facilitada por los propios pasajeros, como fechas e itinerarios de viaje, datos de contacto y de pago, información sobre equipajes, así como otro tipo de observaciones generales, tales como las preferencias dietéticas. Además de detectar los movimientos transfronterizos de personas determinadas, estos datos pueden utilizarse para identificar amenazas todavía desconocidas, tratando los datos de los pasajeros con arreglo a los indicadores de riesgo específicos. Estos criterios se establecen por parte de las unidades de intervención policial y se

actualizan de acuerdo con los nuevos datos y patrones disponibles en el sistema.

10 A tal efecto, para más información, véase, CRUZ ÁNGELES, J.; "Procesamiento informático de datos y protección de derechos fundamentales en las fronteras exteriores de la Unión Europea", *Revista Freedom, Security & Justice: European Legal Studies*, n.º 1, 2020, pp. 94-122.

11 Sistema Europeo de información y Autorización de Viajes (SEIAV) regulado por: Reglamento (UE) 2018/1240, del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226; y por el Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con objeto de establecer el Sistema Europeo de información y Autorización de Viajes (SEIAV).

12 Registro de Nombres de los Pasajeros (RNP o PNR) regulado por: Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

A principios de 2020, la propia Comisión Europea reconoció en el preámbulo de su Libro Blanco sobre Inteligencia Artificial (IA)[13], que el uso de este tipo de tecnología conlleva una serie de riesgos potenciales, incluida la "discriminación". En esta línea de trabajo, nos planteamos cómo se regula la elaboración de perfiles de riesgo y cómo podemos combatir posibles casos de discriminación –menos visibles y trazables–; así como qué garantías jurídicas ofrece el sistema europeo a una persona o a un colectivo que puede sentirse discriminado por este tipo de perfiles, y que no alcanza a comprender, realmente, su funcionamiento –debido a una posible falta de transparencia por parte de las Administración Pública[14]–.

13 La Inteligencia Artificial (IA) es la inteligencia llevada a cabo por máquinas. En ciencias de la computación, una máquina "inteligente" ideal es un agente flexible que percibe su entorno y lleva a cabo acciones que maximicen sus posibilidades de éxito en algún objetivo o tarea. Coloquialmente, el término inteligencia artificial se aplica cuando una máquina imita las funciones "cognitivas" que los humanos asocian con otras mentes humanas, como por ejemplo, percibir, razonar, aprender y resolver problemas.

14 Desde su creación (2011-12), la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA) contribuye a la aplicación de las políticas de justicia y asuntos de interior de la UE mediante la gestión de sistemas informáticos de gran magnitud. A tal efecto, gestiona los sistemas informáticos integrados de gran magnitud que: (1) mantienen la seguridad interior en los países Schengen; (2) permite a los países Schengen intercambiar datos sobre visados; y (3) determinan qué país de la UE es responsable de examinar una determinada solicitud de asilo.

II. El análisis de datos en la elaboración de perfiles: metodología inductiva (criminales) y deductiva (de riesgo)

En los últimos siglos, la medición de la peligrosidad es una cuestión que ha preocupado a científicos de diversas áreas de conocimiento: no sólo a psiquiatras, psicólogos y criminólogos, sino también a penalistas y operadores jurídicos, que han mantenido un elevado interés en los instrumentos para su medición, de cara a individualizar las medidas de seguridad a imponer o, incluso, algunas penas. En este contexto, la perfilación criminal se presenta como una técnica de investigación

derivada del análisis que se realiza a los diferentes patrones conductuales en los agresores conocidos, para con ello definir y crear tipologías –perfilación criminal inductiva– y así auxiliar en la resolución de crímenes en los casos donde se desconoce al responsable, a partir de los indicios físicos y psicológicos encontrados en la escena del crimen –perfilación criminal deductiva–.

El desarrollo de la herramienta del *offender profiling* –perfil del delincuente– se atribuye a los agentes del FBI en el centro de entrenamiento de Quantico –Virginia Oeste– en la década de los años '70 –del pasado Siglo XX–. Originalmente, esta técnica de investigación se plantea para describir el comportamiento y características probables del autor desconocido de un crimen. No obstante, en las últimas décadas se cuestiona si el uso de perfiles psicológicos en crímenes puede ayudar a determinar el tipo de personalidad del criminal y sus características conductuales desde un análisis de los crímenes ya cometidos; de ser así, la técnica del *profiling* permitiría realizar un perfil del posible agresor –tenga o no antecedentes–. Esta definición está relacionada con la que utiliza actualmente el FBI, que considera el perfil criminal como una herramienta que ayuda a obtener información específica del delincuente agilizando la investigación, además de brindar información a los agentes sobre la forma más adecuada de interrogar a posibles sospechosos.

Esta construcción de la tipificación delincuencial encuentra sus primeros antecedentes en la obra del criminólogo y médico italiano, Ezechia Marco LOMBROSO (1835-1909), en su Teoría del Criminal Nato[15], establecía que las causas de la criminalidad están relacionadas con la forma y las causas físicas/biológicas del autor de los hechos. Creía en el determinismo biológico, basado en que todos los delincuentes comparten particularidades fisonómicas, atributos o deformidades. Este autor, desarrolla un listado de características comunes a los delincuentes: (1) psicológicas –impulsividad, inestabilidad emocional, capacidad de manipulación, narcisismo–; (2) cognitivas –cómo procesan la información, pensamientos respecto a su entorno, capacidad de comprensión, carecen de flexibilidad cognitiva, de ponerse en lugar del otro, etc.–; y (3) conductuales –agresividad y tendencia a la actuación–. Asimismo, entre los rasgos cognitivos estudiados para la elaboración de perfiles criminales podemos destacar: cognición impersonal, impulsividad, razonamiento concreto, rigidez cognitiva, baja capacidad de fantasía, ausencia de metas y valores estables, locus de control externo, baja autoestima, percepción social inadecuada, tendencia al egocentrismo y pobres habilidades sociales –resolución de conflictos interpersonales–. En sus estudios, LOMBROSO concluye que la mayoría de las personas que recurren a la violencia, lo hacen simple y llanamente por regresiones evolutivas –y por tanto, los criminales forman parte de nuestra sociedad, porque hay un porcentaje de individuos que nacen con la predisposición fisionómica para la conducta criminal–.

15 Para un estudio más detallado *vid.* LOMBROSO, C.; *Le più recenti scoperte ed applicazioni della psichiatria ed antropologia criminale* , Fratelli Bocca, Torino, 1893; en la línea de LOMBROSO, C.; El delito: Sus causas y remedios, Victoriano Suárez, Madrid, 1902.

En pleno Siglo XXI, la elaboración de perfiles ha evolucionado significativamente. Actualmente, la elaboración de perfiles sigue implicando la clasificación de personas de acuerdo con sus características personales. No obstante, éstas pueden clasificarse como "invariables" –como la edad o la altura– o "variables" –como las prendas utilizadas, los hábitos, las preferencias y otros elementos del comportamiento–. Los perfiles de riesgo se elaboran, de forma automática, mediante una técnica de minería de datos, que clasifica a las personas en virtud de algunas de sus características observables con el fin de deducir, con un cierto margen de error, otras que no son observables. Estas prácticas de elaboración de perfiles tienen como objeto la creación de conocimiento, mediante el análisis de los datos existentes para formular premisas en relación con una persona o un grupo –se utilizan registros de experiencias anteriores y análisis estadísticos para establecer correlaciones entre determinadas características y determinados resultados o conductas–; así como para facilitar procesos decisorios, utilizando dichas correlaciones para tomar decisiones sobre las medidas que deben adoptarse. Esto convierte a la elaboración de perfiles en una herramienta poderosa a disposición de los policías y agentes de fronteras. No obstante, esta herramienta también entraña una serie de riesgos importantes, tales como: el establecimiento de correlaciones genéricas que pueden no ser correctas para todas las personas; generar correlaciones incorrectas, tanto para ciertas personas como para determinados grupo; crear estereotipos nocivos y provocar discriminación; o resultar problemáticos si se trata a una persona como a un miembro de un grupo, en lugar de como a un individuo.

Más específicamente, en el ámbito de la acción policial y de la gestión de fronteras, se entiende por elaboración de perfiles a "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la ubicación o los movimientos de dicha persona física" [16]. Los resultados de este tratamiento de datos se utilizan para orientar la acción policial y de gestión de fronteras, en varios ámbitos, entre los que podemos destacar: actuaciones de identificación y registro; operaciones de detención; denegación de acceso a ciertas zonas; o la realización de una "inspección de segunda línea" [17] en frontera de carácter más exhaustivo. El diseño de este tipo de inspecciones ponen de manifiesto cómo el uso de estas bases de datos no puede sustituir la labor de los policías y agentes de fronteras, sino que debe complementarla.

16 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/911/JAI del Consejo, DO L 119 (Directiva sobre la policía), artículo 3, apartado 4.

17 Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que

se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen). Artículo 2. Definiciones. (...) 13. "Inspección de segunda línea: una nueva inspección que puede efectuarse en un lugar especial aparte de aquel en que se inspecciona a todas las personas (primera línea). Artículo 8. Inspecciones fronterizas de personas". (...) 4. (...) "Los nacionales de terceros países sujetos a una inspección minuciosa de segunda línea recibirán información por escrito, en una lengua que comprendan o cuya comprensión sea razonable suponerles o de otra forma eficaz, con respecto al propósito y al procedimiento de dicha inspección. La citada información existirá en todas las lenguas oficiales de la Unión y en la lengua o lenguas del país o los países fronterizos del Estado miembro de que se trate e indicará que el nacional del tercer país puede pedir que se le facilite el nombre y el número de identificación de servicio de los guardias de fronteras que lleven a cabo la inspección minuciosa de segunda línea así como el nombre del paso fronterizo y la fecha en que se ha cruzado la frontera".

La elaboración contemporánea de perfiles tiene dos usos principales: (1) identificar a personas físicas en función de información de inteligencia específica –se utiliza un perfil que recoge las características de determinados sospechosos, basadas en pruebas recogidas acerca de un hecho concreto– y (2) como método predictivo para identificar a personas "desconocidas" que puedan ser de interés para las autoridades policiales y de gestión de fronteras. Podemos observar cómo esta herramienta conserva la esencia de la teoría de LOMBROSO, es decir, se basa en el análisis de datos y en premisas basadas en la experiencia –con la ventaja de que la base de datos puede realizar miles, o incluso millones de experimentos y cruzar la información de forma automática–. No obstante, lo ideal es que estos nuevos modelos predictivos estén enfocados en el comportamiento. O de lo contrario, pueden plantearse problemas cuando, en la práctica, éstos se convierten en perfiles ilícitos, al enfocarse, única o principalmente, en características físicas o en aspectos inmutables o inherentes a una persona o a un grupo determinado –categorías prohibidas de discriminación–, lo que genera la creación de estereotipos, que discriminan a una persona o un grupo determinado.

III. La protección de datos en la elaboración de perfiles: estudio de la normativa europea

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

La creación de algoritmos con fines predictivos es un proceso complejo que requiere la toma de múltiples decisiones por diversas personas implicadas en el proceso. En este sentido, no sólo se refiere a los patrones que sigue un ordenador, sino también al proceso de recogida, preparación y análisis de datos. Se trata de un proceso humano que comprende varias fases, en las que desarrolladores y responsables deben tomar decisiones. En cada una de estas fases del proceso de elaboración algorítmica de perfiles, se puede introducir un sesgo algorítmico[18]. Para evitar este tipo de sesgos discriminatorios y violaciones de los derechos a la

protección de datos y a la intimidad, tanto las personas que diseñen los algoritmos como los agentes de policía y de gestión de fronteras que recojan e interpreten los datos deberán tener un conocimiento claro de los derechos fundamentales y su aplicación en este contexto.

18 El fenómeno del "sesgo algorítmico" se produce cuando un sistema informático refleja los valores de los humanos que están implicados en la codificación y recolección de datos usados para entrenar el algoritmo. El sesgo algorítmico se puede encontrar en todo tipo de bases de datos, desde redes sociales a grandes bases de datos para gestionar fronteras, pudiendo tener un gran impacto en la privacidad de los usuarios o agravar sesgos sociales como los existentes respecto a razas, género, sexualidad o etnias. A medida que los algoritmos expanden su capacidad para organizar la sociedad, la política, las instituciones y el comportamiento, hemos comenzado a preocuparnos por la forma en que los resultados no previstos y la manipulación de los datos puede impactar en el mundo físico –o analógico–. Los sesgos pueden repercutir en los algoritmos teniendo como origen influencias culturales, sociales, o institucionales; debido a limitaciones técnicas de su diseño; o por ser utilizado en contextos no esperados en un principio o por usuarios que no se habían considerado en el diseño inicial del software.

En una primera fase preparatoria, se diseña y desarrolla el algoritmo –especificando el objetivo de análisis: predicción; descripción; o explicación–. Los datos se recogen o se seleccionan datos con fines productivos –estos datos pueden producir sesgos si no son representativos de la realidad o reflejan prejuicios ya existentes–. Los datos son recogidos por las autoridades fronterizas y por otros organismos públicos. E incluso, en algunos casos, se pueden comprar datos a empresas privadas (*Data Brokers*)[19]. Estos datos se conservan en almacenes y se preparan para análisis –es posible introducir sesgos durante dicha etapa de preparación de datos a la hora de seleccionar los atributos que deseamos que el algoritmo tenga en cuenta–. A continuación, a través de la minería de datos, se analizan para establecer patrones y correlaciones, adecuándose los modelos estadísticos con el fin de realizar predicciones –esto es lo que suele denominarse "arte" del aprendizaje profundo: elegir qué atributos considerar o ignorar puede influir significativamente en la precisión de la predicción del modelo–. Y, finalmente, tras la interpretación de los datos o la aplicación del modelo predictivo, el resultado de análisis se utiliza para establecer patrones conductuales de determinados grupos de personas. Sobre la base de estos perfiles o predicciones, se pueden tomar decisiones en el ámbito de la actuación policial y la gestión de fronteras.

19 Los *Data Brokers* o vendedores de datos son empresas que se dedican a recoger información de los consumidores, ya sea con o sin su permiso, y que venden a un tercero que esté interesado en obtener dicha información. Éstos recopilan datos y a través del Big Data (o ciencia de datos) analizan las tendencias de los usuarios en áreas tan diversas como: finanzas, intereses políticos, religión u orientación sexual, entre otras.

A medida que la inteligencia artificial penetra en la sociedad y se usa para tomar decisiones que afectan a las personas, aumenta el problema de los algoritmos sesgados. En este sentido, conviene señalar que la gran mayoría de aplicaciones de Inteligencia Artificial se basan en una categoría conocida como aprendizaje profundo (o *deep learning*)[20], cuyos algoritmos están especializados en encontrar patrones en los datos. A pesar de la enorme utilidad de este enfoque, también presenta una serie de desafíos. A continuación, destacamos los cuatro retos principales.

20 El aprendizaje profundo (o *deep learning*), compuesto por algoritmos de aprendizaje automático, ideados para el aprendizaje automático. Éstos pueden usar una cascada de capas con unidades de procesamiento no lineal para extraer y transformar variables –utilizando aprendizaje supervisado o no supervisado, incluyendo aplicaciones de modelización de datos y reconocimiento de patrones–; estar basados en el aprendizaje de múltiples niveles de características o representaciones de datos –las características de más alto nivel se derivan de las características de nivel inferior para formar una representación jerárquica–; o aprender múltiples niveles de representación que corresponden con diferentes niveles de abstracción –formando una jerarquía de conceptos–. Todas estas formas tienen en común: múltiples capas de procesamiento no lineal; y el aprendizaje supervisado o no supervisados de representaciones de características en cada etapa. Las capas forman una jerarquía de características desde un nivel de abstracción más bajo a uno más alto.

En primer lugar, la introducción inconsciente de sesgos. La introducción del sesgo no siempre resulta obvia durante la construcción del modelo porque es posible que el diseñador no sea consciente de éste, hasta que se aprecien los posibles impactos derivado del tratamiento de los datos y las decisiones. En segundo lugar, procesos mal diseñados. Muchas de las prácticas comunes en el aprendizaje profundo no están diseñadas para tener en cuenta la detección de sesgos. El rendimiento de los modelos de aprendizaje profundo se prueba antes de su implementación, lo que parece una oportunidad perfecta para identificar sesgos. Pero, en la práctica, los informáticos dividen sus datos al azar y utilizan uno de los grupos para entrenar el algoritmo. El otro se reserva para validar su eficacia posteriormente. Eso significa que los datos de control para probar el rendimiento del modelo tienen los mismos sesgos que los datos de entrenamiento. Por tanto, es imposible detectar los resultados sesgados. En tercer lugar, la falta de contexto social. La forma en que se enseña a los informáticos a abordar los problemas, a menudo, puede no encajar con la mejor forma de pensar en dichos problemas –de ahí, la importancia de contar con asesoramiento para la creación de algoritmos–. Y, en cuarto lugar, las distintas acepciones del término “equidad”. Esto no ocurre sólo en Ciencias Sociales y Jurídicas, es una cuestión ampliamente debatida en Ciencias de la Computación[21]. La diferencia es que en informática el concepto de equidad debe definirse en términos matemáticos, como equilibrar las tasas de falso positivo y falso negativo en un sistema de predicción. Los falsos positivos se refieren a casos en que una persona es señalada e investigada a causa de una predicción errónea de que dicha persona puede constituir de peligro; así como los falsos negativos se refieren a personas que entrañan un verdadero riesgo en el contexto de las operaciones policiales y de gestión de fronteras, pero a las que el sistema no ha identificado como tales. Entonces, el problema principal que se suscita es que el algoritmo es capaz de procesar una cantidad ingente de datos, pero no es capaz de razonar en términos epistemológicos. Es decir, un algoritmo no sabe qué es justo o injusto, quién es bueno o malo, sino que simplemente extrae de todas las experiencias almacenadas posibles parámetros que nos ayudan a identificar posibles perfiles de riesgo. En este contexto, la gestión de estas grandes bases de datos requiere de una serie de garantías mínimas para el usuario, tales como: el respeto de su vida privada; el deber de información sobre la lógica aplicada y las consecuencias previstas; así como una correcta gestión y conservación de los datos –contando con evaluaciones de impacto del tratamiento automatizado–. A continuación,

analizaremos las luces y sombras de la normativa europea en materia de protección de datos, en relación con la técnica de la elaboración algorítmica de perfiles.

21 Para un estudio más detallado vid. LEESE, M.; "The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union", *Security Dialogue* , vol. 45 (5), 2014, pp. 494-511.

1. Seguridad versus derecho a la vida privada

Con arreglo al ordenamiento jurídico de la Unión Europea, el respeto a la vida privada (artículo 7[22]) y la protección de los datos personales (artículo 8 de la Carta[23]) son derechos distintos, aunque estrechamente relacionados. El derecho a la vida privada (o derecho a la intimidad) es un derecho más general, que prohíbe cualquier injerencia en la vida privada de una persona física. El concepto de vida privada no incluye simplemente lo que una persona desea mantener como confidencial, sino también los medios a través de los cuales expresa su personalidad, por ejemplo, al elegir con quién interactúa[24] o cómo se viste. La protección de los datos personales se limita a la evaluación del carácter lícito del tratamiento de datos personales. Estos derechos no son absolutos y pueden limitarse en circunstancias concretas (véase artículo 8 del Convenio Europeo[25] de Derechos Humanos y el artículo 52 de la Carta[26]).

22 Carta de los Derechos Fundamentales de la Unión Europea . Artículo 7. Respeto de la vida privada y familiar. "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

23 Carta de los Derechos Fundamentales de la Unión Europea. Artículo 8. Protección de datos de carácter personal. "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El resto de estas normas quedará sujeto al control de una autoridad independiente".

24 Para un estudio más detallado sobre el concepto de derecho a la vida privada *vid.* CRUZ ÁNGELES, J.; Derechos humanos y nuevos modelos de familia. Estudio en el marco de los sistemas europeo e interamericano de protección de derechos humanos, editorial Thomson Reuters Aranzadi, Pamplona, 2018, *passim.*

25 Convenio Europeo de Derechos Humanos. Artículo 8. Derecho a la vida privada y familiar. "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

26 Carta de Derechos Fundamentales. Artículo 52. Alcance de los derechos garantizados. "1. Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás. 2. Los derechos reconocidos por la presente Carta que tienen su fundamento en los Tratados comunitarios o en el Tratado de la Unión Europea se ejercerán en las

condiciones y dentro de los límites determinados por éstos. 3. En la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán igual a los que les confiere dicho Convenio. Esta disposición no impide que el Derecho de la Unión conceda una protección más extensa".

El Derecho derivado de la Unión profundiza en los derechos a la intimidad y la protección de los datos personales. Dos instrumentos legislativos especifican cómo se pueden recoger y tratar los datos personales. El Reglamento 2016/679 o Reglamento General de Protección de Datos (RGPD)[27] establece los principios generales y las garantías que se aplican al tratamiento de los datos personales. Más concretamente, la Directiva 2016/680 [28], establece las normas que se aplican al tratamiento de datos personales en el contexto de las operaciones policiales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.

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

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

En cuanto a la jurisprudencia europea en la materia, podemos observar cómo el Tribunal de Justicia de la Unión Europea (TJUE), en el asunto Heinz Huber contra *Bundesrepublik Deutschland* [29], evaluó la legitimidad de un Registro Central de Extranjeros (Auslanderzentralregister, AZR), que contiene ciertos datos personales relativos a nacionales extranjeros –tanto ciudadanos de la UE como de países terceros– que han residido en Alemania durante más de tres meses. En este caso, el TJUE concluyó que los datos recogidos para un fin concreto no pueden utilizarse para un fin distinto al que se le atribuyó inicialmente –sin el consentimiento expreso de los usuarios–. En este sentido, el Tribunal determinó que el AZR es un instrumento legítimo para aplicar las normas de residencia, y que la diferencia de trato entre los nacionales extranjeros y los alemanes, de quienes se conservan menos datos, está justificada para el fin pretendido. Sin embargo, el TJUE resolvió que los datos conservados en el AZR no podían utilizarse para combatir la delincuencia en general, ya que éste no es el fin para el que se recogieron los datos en principio.

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

En esta línea de trabajo, el Tribunal Europeo de Derechos Humanos (TEDH), *véase* el asunto S. y Marper contra Reino Unido[30], plantea la solicitud de supresión de expedientes –huellas dactilares, muestras celulares y perfiles de ADN– de la base de datos de ADN utilizada para la identificación de delincuentes en el Reino

Unido. En este caso, los solicitantes estaban preocupados porque, a pesar de que años atrás habían sido absueltos de cargos, la policía se había negado a eliminar sus expedientes de la base de datos. El TEDH concluyó que la conservación por tiempo indefinido de las muestras de ADN de personas que habían sido detenidas, pero posteriormente habían sido absueltas o a las que se les retiraron los cargos presentados, es una violación del derecho a la intimidad. Asimismo, el Tribunal resaltó el riesgo de estigmatización, ya que los datos de personas que no habían sido condenadas por ningún delito eran tratados del mismo modo que los datos de las personas condenadas. Además, el Tribunal también reconoció que el daño que puede causar la retención de estos datos es especialmente importante en el caso de menores de edad, dada la importancia de su desarrollo psicosocial y su integración en nuestra sociedad.

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

Para recoger y tratar los datos personales con el fin de elaborar perfiles, las autoridades policiales y de gestión de fronteras deben cumplir cuatro criterios legales esenciales. De modo que, la recogida y el tratamiento de los datos deben: (1) estar definidos y regulados por ley –cualquier limitación de los derechos de respeto a la vida privada y a la protección de los datos debe estar estipulada por ley y respetar dichos derechos en lo esencial–, así como la ley debe cumplir los criterios de calidad y claridad, es decir, que sea accesible al público y suficientemente clara y precisa para que el público entienda su aplicación y consecuencias; (2) tener un fin válido, lícito y apropiado –los fines legítimos están establecidos en la propia ley y no se pueden ampliar–; (3) ser indispensables para alcanzar dicho fin –el tratamiento de los datos personales debe limitarse a lo que sea necesario para alcanzar los fines para los que se hayan recogido–; y (4) no ser excesivos –las autoridades responsables del tratamiento de datos personales deben alcanzar un equilibrio entre el fin y los medios empleados para conseguirlo–.

Esta herramienta del triple test de igualdad, que analiza si las medidas adoptadas por las autoridades estatales son legales, legítimas y necesarias, ha sido utilizada de forma reiterada en la jurisprudencia del TEDH. En la materia que nos ocupa, es de especial interés, por ejemplo, el caso de Gillan y Quinton contra Reino Unido[31], en el que los demandantes, dos nacionales británicos, trataron de impugnar la legalidad de las facultades de identificación y registro que habían sido utilizadas contra ellos por vía de una revisión judicial. La medida se adoptó conforme a las secciones 44 a 47 de la Ley de Terrorismo de 2000, que establecían: (1) con el fin de prevenir actos de terrorismo, cualquier policía podía ser autorizado por oficiales de alto rango a realizar actuaciones de identificación y registro; (2) dicha autorización estaba sujeta a confirmación por el Secretario de Estado y tenía una limitación temporal, pero se podía prorrogar indefinidamente; (3) aunque la finalidad de los registros era encontrar objetos que pudieran utilizarse para cometer actos terroristas, no era necesario que las actuaciones de identificación y registro se basaran en sospechas de que la persona o personas identificadas portaran objetos de esa índole; y (4) las personas que se negasen a someterse al registro podían ser

privadas de libertad y/o multadas. En este caso, el uso de poderes coercitivos por parte de las autoridades policiales para identificar a una persona y registrar su vestimenta y sus pertenecías representa una clara injerencia en el derecho al respeto de la vida privada. Su gravedad se amplifica debido a la exposición pública de información personal, que conlleva un elemento de humillación y vergüenza. En cuanto a la evaluación de la proporcionalidad y necesidad, el Tribunal expresó una serie de dudas sobre la proporcionalidad y la necesidad de la ley: el criterio legal para la autorización de las identificaciones no era exigente; la amplitud de facultades legales es tal que los demandantes se enfrentan a enormes obstáculos a la hora de demostrar que una autorización y confirmación pueda exceder las facultades de las autoridades competentes (*ultra vires*) o suponga un abuso de poder; el alcance geográfico de la autorización era muy amplio y el límite de tiempo se ampliaba continuamente, por lo que se reducía el carácter específico de la autorización; las limitaciones de la discrecionalidad de los agentes eran más de forma que de fondo; había pocas perspectivas de recurso judicial porque el agente que realizaba la identificación no tenía obligación de demostrar que sus sospechas eran razonables; por tanto, era prácticamente imposible demostrar que había ejercido sus facultades de manera indebida. Estas consideraciones llevaron al TEDH a concluir que los artículos pertinentes de la Ley de Terrorismo “no limitan suficientemente ni se encuentran sujetos a una protección legal adecuada contra los abusos” y, por tanto, constituyen una violación del artículo 8 CEDH .

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

2. El especial deber de información sobre la lógica utilizada y las consecuencias previstas

En los casos de elaboración de perfiles, el Reglamento General de Protección de Datos obliga a facilitar a la persona física información significativa sobre la lógica aplicada, así como sobre la importancia y las consecuencias previstas del tratamiento de datos. Esta información debe facilitarse tanto en el momento de recoger los datos –mediante una notificación– como en el caso de que el interesado solicite información adicional –ejercitando su derecho de acceso a los datos–. A tal efecto, conviene analizar el contenido de la Directiva (UE) 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. En su considerando 38 especifica que el tratamiento automatizado “debe estar sujeto a las garantías apropiadas, lo que incluye informar de manera específica al interesado (...), en particular para que (...) pueda (...) obtener una explicación de la decisión adoptada tras dicha evaluación, o ejercer su derecho a impugnar la decisión”[32].

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

infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2088/977/JAI del Consejo. "Considerando 38. El interesado debe tener derecho a no ser objeto de una decisión que evalúe aspectos personales que le conciernen que se base únicamente en un tratamiento automatizado de los datos y que tenga efectos jurídicos adversos que le conciernan o le afecten significativamente. En todo caso, este tipo de tratamiento debe estar sujeto a las garantías apropiadas, lo que incluye informar de forma específica al interesado, así como el derecho a la intervención humana, en particular para que el interesado pueda expresar su punto de vista, obtener una explicación de la decisión adoptada tras dicha evaluación, o ejercer su derecho a impugnar la decisión. Queda prohibida la elaboración de perfiles que dé lugar a la discriminación de personas físicas por razones basadas en datos personas que, por su naturaleza, son especialmente sensibles en relación con los derechos y las libertades fundamentales, con arreglo a las condiciones previstas en los artículos 21 y 52 de la Carta (de Derechos Fundamentales de la Unión Europea)".

En el marco de estas operaciones, las autoridades estatales deberán poner a disposición del interesado la siguiente información: identidad y datos de contacto del responsable del tratamiento; en su caso, los datos de contacto del delegado de protección de datos; los fines del tratamiento a que se destinen los datos personales; el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma; y la existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento. Además, a fin de permitir el ejercicio de sus derechos, deberá informar sobre: la base jurídica del tratamiento; el plazo durante el cual se conservan los datos personales, o cuando esto no sea posible, los criterios utilizados para determinar ese plazo; cuando corresponda, las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales; cuando sea necesario, más información, en particular cuando los datos se hayan recogido sin conocimiento del interesado[33].

33 *Ibidem.* Artículo 13. Información que debe ponerse a disposición del interesado o se le debe proporcionar.

Este "derecho a la explicación" puede resultar difícil de aplicar en la práctica. Algunas personas pueden tener los conocimientos digitales necesarios para comprender el código de un algoritmo, mientras que para otras basta recibir información simplificada sobre la finalidad del tratamiento y las interconexiones de los datos utilizados. La clave para evaluar si la explicación facilitada es significativa es su objetivo. Una persona debe recibir información suficiente para entender la finalidad, la justificación y los criterios que llevaron a tomar una decisión. Además, debe tenerse en cuenta que el derecho a una explicación no es un derecho absoluto. Es decir, que los Estados miembros pueden limitar este derecho por ley en determinados supuestos, en particular, por razones de seguridad nacional; defensa; seguridad pública; prevención, investigación, detección o enjuiciamiento de infracciones penales; ejecución de sanciones penales, protección del interesado o de los derechos y libertades de otros; o ejecución de demandas civiles. No obstante, facilitar información razonable sobre la finalidad y las consecuencias previstas del tratamiento constituye una buena práctica aconsejable. La adopción de procedimientos sencillos para explicar la lógica aplicadas y los criterios para adoptar una decisión servirá en última instancias para mejorar la transparencia y la rendición

de cuentas.

En cuanto al derecho de acceso del interesado a los datos personales, las autoridades estatales deberán reconocer el derecho del interesado a obtener del responsable del tratamiento de sus datos confirmación de si están tratando o no datos personales que le conciernen y, en caso de que se confirme el tratamiento, acceso a dichos datos personales y a la siguiente información: fines y base jurídica del tratamiento; categorías de datos personales de que se trate; destinatarios o las categorías de destinatarios a quienes hayan sido comunicados lo datos personales, en particular los destinatarios establecidos en terceros países o las organizaciones internacionales; el plazo durante el cual se conservan los datos personales, o cuando esto no sea posible, los criterios utilizados para determinar ese plazo; la existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado, o la limitación de su tratamiento; el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma; y la comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen[34].

34 *Ibidem.* Artículos 14. Derecho de acceso del interesado a los datos personales.

Este derecho de acceso también podrá restringirse, total o parcialmente, siempre y cuando dicha restricción constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales de los intereses legítimos de la persona física afectada para: evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o la ejecución de sanciones penales; proteger la seguridad pública; proteger la seguridad nacional; y/o proteger los derechos y libertades de otras personas[35].

35 *Ibidem.* Artículos 15. Limitaciones al derecho de acceso.

3. La correcta gestión y conservación de los datos

Los autoridades responsables de la recogida y el tratamiento de datos personales con fines de elaboración de perfiles no sólo deben tratar los datos de manera lícita, sino también velar por que los datos no sean: accesibles por parte de personas no autorizadas; utilizados para fines distintos del fin original; ni conservados durante más tiempo del necesario. A tal efecto, las autoridades y los agentes de policía y de gestión de fronteras deben velar por que se apliquen medidas adecuadas para proteger la integridad y la seguridad de los datos. Deben controlar todo acceso, y uso de los datos, mediante la creación y el mantenimiento de los registros de todas las actividades de tratamiento o categorías de actividades de tratamiento[36]. Estos registros deben contener: el nombre y los datos de contacto de las autoridades y del delegado de protección de datos; los fines del tratamiento; las categorías de destinatarios a quienes se comunicaron o se comunicarán los datos personales; una descripción de las categorías de los interesados y de las categorías de datos

personales; el uso de la elaboración de perfiles; una indicación de la base jurídica para la operación de tratamiento; cuando sea posible, los plazos previstos para suprimir las diferentes categorías de datos personales; cuando sea posible una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 29, apartado 1 , de la Directiva 2016/680 (UE).

36 *Ibidem.* Artículo 24. Registro de las actividades de tratamiento.

Además, cuando se implemente la elaboración de perfiles informatizada para los fines comprendidos en la Directiva 2016/680 (UE), las autoridades deberán conservar registros de las operaciones de recogida, modificación, consulta, divulgación (incluidas transferencias), combinación y supresión de datos. Estos expedientes y registros ayudarán a los agentes a demostrar que cumplen los requisitos legales durante los controles internos y externos. Por ejemplo, si una persona presenta una reclamación, las autoridades policiales y las autoridades responsables de la gestión de fronteras deberán poner estos expedientes y registros a disposición de las autoridades nacionales encargadas de la protección de datos. Los datos personales no deben conservarse durante más tiempo del necesario para alcanzar el fin legítimo establecido. Si se conservan durante períodos más largos, deberá justificarse debidamente. En estos casos, las autoridades deberán asegurarse de revisar periódicamente dicha conservación para garantizar su integridad y seguridad.

4. Evaluaciones de impacto del tratamiento automatizado

No es sencillo detectar y prevenir un uso indebido o el tratamiento ilícito de datos personales. Los conocimientos especializados necesarios para entender algoritmos complejos y grandes bases de datos hacen que sea difícil realizar controles adecuados. Para resolver este problema, el Reglamento General de Protección de Datos y la Directiva 2016/680 (UE) incluyen garantías con el fin de orientar a los agentes de policía y de gestión de fronteras antes, durante y después del tratamiento de los datos. Se refieren a: evaluaciones del impacto relativas a la protección de datos, y protección de los datos desde el diseño y por defecto.

El marco jurídico de la UE obliga a las autoridades policiales y a las autoridades responsables de la gestión de fronteras a realizar evaluaciones de impacto antes de llevar a cabo cualquier tratamiento de datos que pueda entrañar un riesgo elevado para los derechos de las personas físicas[37]. Esto significa que las evaluaciones de impacto no sólo deberán realizarse cuando el resultado del tratamiento pueda violar las normas de protección de datos o la intimidad, sino en cualquier situación que pueda derivar en una violación de cualquier derecho fundamental, como pueden ser los derechos a la igualdad y a la no discriminación, a la libertad de expresión e información, a la libertad de pensamiento, de conciencia y de religión, a la educación, a la sanidad, al asilo, y a la protección en caso de devolución, expulsión o extradición. Las evaluaciones de impacto son especialmente importantes si la elaboración de perfiles puede acarrear consecuencias jurídicas para las personas físicas. En estos casos, la Directiva 2016/680 (UE) obliga a realizar evaluaciones de

impacto.

37 *Ibidem.* Artículo 27. Evaluación de impacto relativa a la protección de datos.

Las evaluaciones de impacto deben realizarse antes del propio tratamiento automatizado, y su objetivo es doble: *a priori* , antes del tratamiento de los datos, una evaluación de impacto relativa a la calidad de los datos o del algoritmo de tratamiento contribuye a detectar y, llegado el caso, a remediar posibles violaciones de los derechos fundamentales; a posteriori, una vez tratados los datos, el agente puede verse en la obligación de demostrar que ha actuado de manera lícita. La evaluación del impacto puede ayudar a demostrar que se han adoptado todas las medidas necesarias para garantizar el cumplimiento de la ley. Una evaluación de impacto puede variar significativamente en función del tipo y el volumen de los datos personales tratados, y del tipo y la finalidad del tratamiento. Puede incluir una verificación de calidad de los datos, controles técnicos de los algoritmos de tratamiento, o una revisión completa de los objetivos del tratamiento, etc.

5. La protección de datos integrada en el diseño

Con independencia de si una evaluación de impacto detecta o no la posibilidad de una violación de derechos fundamentales, se pueden aplicar medidas para evitar cualquier riesgo de ilegalidad. Esto es lo que se conoce como “protección de datos desde el diseño” y “protección de datos por defecto”[3839].

38 Reglamento General de Protección de Datos. Artículo 25. Protección de datos desde el diseño y por defecto. “1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. 3. Podrá utilizarse un mecanismo de certificación aprobado con el arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo”.

39 Directiva (UE) 2016/680. Artículo 20. Protección de datos por diseño y por defecto. “1. Los Estados miembros dispondrán que el responsable del tratamiento, teniendo en cuenta el estado de la técnica y el coste de la aplicación, y la naturaleza, el ámbito, el contexto y los fines de tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas planteados por el tratamiento, aplique, tanto en el momento de determinar los medios para el tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas, como por ejemplo la seudonimización, concebidas para aplicar los principios de protección de datos, como por ejemplo la minimización de datos, de forma efectiva y para integrar las garantías necesarias en el tratamiento, de tal manera que esta cumpla los requisitos de la presente Directiva y se protejan los derechos de los interesados. 2. Los Estados miembros dispondrán que el responsable del tratamiento

aplique las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad. En concreto, tales medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin intervención de la persona, a un número indeterminado de personas físicas".

La protección de datos desde el diseño tiene por objeto garantizar que, antes y durante el tratamiento de los datos, se apliquen medidas técnicas y organizativas para garantizar los principios de protección de datos. Por ejemplo, cuando sea viable, los datos personales podrían "seudonimizarse". La seudonimización es una medida por la que no se pueden atribuir datos personales a una persona sin información adicional, que se conserva por separado. La clave que permite reidentificar a los interesados deben conservarse por separado y de manera segura. Al contrario que los datos anonimizados, los datos seudonimizados siguen siendo datos personales y, por tanto, deben respetar las normas y los principios de protección de datos. La protección de datos por defecto garantiza que "sólo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento". Esto afecta a: la cantidad de datos personales recogidos y conservados; los tipos de tratamiento que pueden afectar a datos personales; el plazo máximo de conservación; el número de personas con autorización de acceso a dichos datos personales.

El objetivo principal de la protección de datos desde el diseño y de la protección de datos por defecto es ayudar a las autoridades y los agentes de la policía y gestión de fronteras a diseñar programas de elaboración algorítmica de perfiles que cumplan los requisitos de derechos fundamentales, en particular los principios de licitud, transparencia y seguridad. Sin embargo, este tipo de medidas también pueden demostrar cómo cumplen las autoridades con el requisito legal de rendición de cuentas. Las autoridades responsables del tratamiento de datos tienen la obligación legal de aplicar "medidas técnicas y organizativas" para demostrar que cumplen con la legislación de la UE. Por ejemplo, si una persona presenta una reclamación, las autoridades judiciales y de protección de datos nacionales pueden solicitar a las autoridades que demuestren cada uno de estos puntos: (1) la legitimidad, necesidad y proporcionalidad de la elaboración de perfiles informatizada; (2) la licitud del fin perseguido; (3) la información facilitada a los interesados; (4) la integridad y seguridad de los datos; (5) las medidas y los controles de calidad aplicados antes y durante las operaciones de elaboración de perfiles.

IV. (Re)pensar la discriminación: propuesta lege referenda

Como hemos podido ver en apartados anteriores, la elaboración de perfiles es una técnica de investigación legítima, si se utiliza de forma lícita. Para que esto sea así, el perfil debe basarse en justificaciones objetivas y razonables y respetar los derechos fundamentales, tales como el derecho a la no discriminación. De modo que, se considerará que la elaboración del perfil es ilícita si incluye actos de trato diferenciado injustificado basados en motivos protegidos; o si constituye una

injerencia innecesaria en la vida privada de las personas físicas.

El principio de no discriminación, también conocido como "principio de igualdad" o cláusula de "no discriminación" constituye uno de los valores fundamentales de la Unión Europea[40]. Éste se encuentra definido en el Derecho originario de la Unión Europea, más específicamente, en el artículo 21 de la Carta de Derechos Fundamentales[41], en el que se entiende por discriminación "cuando (...) una persona es tratada de manera menos favorable de lo que sea, haya sido o vaya a ser tratada otra en una situación comparable" por razón de una característica personal percibida o real. Piénsese, a modo de ejemplo, en las siguientes categorías o motivos protegidos: "sexo, raza, color, lengua, religión, opiniones políticas u otras, origen nacional o social, pertenencia a una minoría nacional, fortuna, nacimiento o cualquier otra situación"[42]. Esta cláusula de no discriminación deberá interpretarse de acuerdo con lo dispuesto en los artículos 18 a 25 del Tratado de Funcionamiento de la Unión Europea –sobre no discriminación y ciudadanía de la Unión–. Asimismo, en el marco del Derecho derivado de la Unión Europea, el principio de igualdad se ha desarrollado y consolidado; como es el caso de la Directiva 2000/78/CE del Consejo, de 27 de noviembre de 2000, relativa al establecimiento de un marco general para la igualdad de trato en el empleo y la ocupación.

40 Tratado de la Unión Europea. Artículo 2. "La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Estos valores son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres".

41 Carta de Derechos Fundamentales de la Unión Europea. Artículo 21. Prohibición de la discriminación. "Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual". Convenio Europeo para la Protección de los Derechos Humanos. Protocolo N.º 12. Artículo 1. "El goce de los derechos reconocidos por la ley ha de ser asegurado sin discriminación alguna, especialmente por razones de sexo, raza, color, lengua, religión, opiniones políticas o de otro carácter, origen nacional o social, pertenencia a una minoría nacional, fortuna, nacimiento o cualquier otra situación. Nadie podrá ser objeto de discriminación por parte de una autoridad pública, especialmente por los motivos mencionados en el párrafo 1".

42 Convenio Europeo de Derechos Humanos. Artículo 14. Prohibición de la discriminación. "El goce de los derechos y libertades reconocidos en el presente Convenio ha de ser asegurado sin distinción alguna, especialmente por razones de sexo, raza, color, lengua, religión, opiniones políticas u otras, origen nacional o social, pertenencia a una minoría nacional, fortuna, nacimiento o cualquier otra situación". Para más información acerca de la aplicación de este artículo *véase* Protocolo n.º 12 al Convenio Europeo de Derechos Humanos.

A través del estudio de la legislación europea contra la discriminación[43], podemos observar la existencia de varios tipos de discriminación: (1) la discriminación directa es cuando una persona es tratada de manera menos favorable, única o principalmente por razón de un motivo protegido, como la raza, el género, la edad, la discapacidad o el origen étnico. Por ejemplo, en respuesta a una amenaza terrorista, se confiere a la policía la facultad de identificar y registrar a cualquier

persona que se considere que pueda estar involucrada en actividades terroristas. Se cree que la amenaza proviene de una organización terrorista activa en una determinada región del mundo, pero se carece de información de inteligencia más específica. Si un policía procede a la identificación de un hombre basándose única o principalmente en que se aspecto indique que puede ser originario de esa misma región del mundo, esto constituiría una discriminación directa y sería ilícita; (2) la discriminación indirecta –también conocida como "discriminación de impacto desigual" en el contexto de la acción policial y la gestión de fronteras– es cuando una disposición, un criterio o una práctica de carácter aparentemente neutro colocaría a personas con determinadas características protegidas en una situación de particular desventaja en comparación con otras personas, a menos que tal disposición, criterio o práctica se justifique objetivamente por un fin legítimo y que los medios utilizados para alcanzar tal fin sean necesarios y proporcionados. La discriminación indirecta necesita, en general, estadísticas para valorar si una persona ha sido tratada, en la práctica, de manera menos favorable que otra por razón de su pertenencia a un grupo con determinadas características protegidas.

43 Para un estudio más detallado *véase* VV.AA.; *Manual de legislación europea contra la discriminación* , Agencia de los Derechos Fundamentales de la Unión Europea, 2010, *passim.*

El análisis de la discriminación por un solo motivo no refleja adecuadamente las diversas manifestaciones de un trato desigual. Una discriminación múltiple es aquella que tiene lugar por varios motivos que operan por separado. Por ejemplo, puede que una persona sea discriminada no sólo por su origen étnico, sino también por su edad y su género. La discriminación interseccional describe una situación en la que varios motivos operan simultáneamente e interactúan de manera que son inseparables y producen tipos concretos de discriminación. Por ejemplo, un agente en frontera identifica y registra a un joven afrodescendiente sin motivos razonables para sospechar que haya cometido un delito. No lo discrimina sólo por su edad –no todos los jóvenes son identificados– o por su origen étnico –no todos los jóvenes afrodescendientes son identificados–, sino precisamente porque es al mismo tiempo joven y afrodescendiente.

En el marco de la elaboración algorítmica de perfiles, el artículo 9 del Reglamento General de Protección de Datos establece específicamente que queda prohibido el tratamiento de categorías especiales de datos personales que revelen características personales, como el origen étnico o racial, las opiniones políticas, o las convicciones religiosas o filosóficas[44]. Esta prohibición no se aprecia en casos muy concretos, como la protección del interés o el orden público, siempre que la exención tenga base jurídica, sea proporcionada y necesarias, y establezca garantías adecuadas[45]. Del mismo modo, en el contexto de la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, el artículo 11 de la Directiva (UE) 2016/680 sobre el mecanismo de decisión individual automatizado prohíbe "la elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales" [46], incluidos los datos que revelen el origen étnico o racial y las convicciones religiosas, así como los datos genéticos y biométricos. Una vez más,

se permiten excepciones a esta prohibición en algunos casos, pero deben ser necesarias, contar con garantías adecuadas, y tener una base jurídica o la finalidad de proteger los intereses vitales de una persona física. De modo que, la prohibición de discriminación no implica que no se puedan utilizar características personales como factores legítimos para elaborar perfiles en el contexto de investigaciones criminales o inspecciones fronterizas. Sin embargo, deben existir motivos razonables de sospecha basados en otra información que no sean los motivos protegidos. Por ejemplo, puede que una persona encaje con la descripción concreta de un sospechoso, o que su aspecto no se corresponda con la información que contiene su documento de viaje.

44 Reglamento General de Protección de Datos. Artículo 9. Tratamiento de categorías especiales de datos personales. "1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física".

45 Reglamento General de Protección de Datos. Artículo 9. Tratamiento de categorías especiales de datos personales. "2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: (...) g. el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial".

46 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2088/977/JAI del Consejo. Artículo 11. Mecanismo de decisión individual automatizado. 3. "La elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales establecidas en el artículo 10 quedará prohibida, de conformidad con el Derecho de la Unión".

El análisis de los perfiles algorítmicos nos obliga a repensar las categorías prohibidas de discriminación. Esto se debe a que, en la elaboración de perfiles tradicionales, la lógica de la discriminación se basaba en el establecimiento de una cadena causal –entre los indicadores a nivel teórico y su representación en la población objeto del escrutinio–. De modo que, en este tipo de perfiles, se podía evitar la discriminación no deseada sobre la base de ciertas características, como el sexo, la raza, o la religión. Sin embargo, con el análisis controlado por datos, esto no es posible. Si bien, el punto de partida sigue siendo la noción del individuo como fuente de información, las categorías se crean a través de suposiciones basadas en la probabilidad. Por ejemplo, los algoritmos de generación de perfiles basados en sistemas bayesianos[47] pueden manejar y procesar flujos continuos de información generada por transacciones para actualizar y ajustar rutinariamente las evaluaciones de riegos del sistema. A diferencia de los algoritmos deterministas, que producen el mismo resultado una y otra vez cuando se ejecutan con la misma base de datos y que, probablemente, pueden experimentar problemas en entornos más complejos. Una vez configurada una red bayesiana, las actualizaciones de la base de datos se pueden analizar e incorporar automáticamente. Esta fluidez supone un cambio importante en la conceptualización de la generación de perfiles,

ya que se crean agrupaciones momentáneas –creando nuevas categorías que no alcanzamos ni a imaginar– que podrían aparecer y desaparecer de un momento a otro.

47 La inferencia bayesiana es un tipo de inferencia estadística en la que las evidencias u observaciones se emplean para actualizar o inferir la probabilidad de que una hipótesis pueda ser cierta. El término ”bayesiano” proviene del uso frecuente que se hace del teorema de Bayes durante el proceso de inferencia. El teorema de Bayes se ha derivado del trabajo realizado por el matemático Thomas Bayes. Hoy en día, uno de los campos de aplicación es la teoría de la decisión (1); visión artificial –simulación de la percepción en general– (2); y el reconocimiento de patrones (3).

Estos sistemas bayesianos, utilizados en un contexto de configuración de “redes neuronales artificiales”[48], pueden plantear una serie de problemas considerables en términos de interpretación de resultados. Como sus procesos internos siguen siendo opacos y la información aprendida de los datos está algo oculta en la red y no puede utilizarse como prueba del resultado, los análisis basados en estos datos se presentan en términos numéricos simplificados o representaciones gráficas, o son completamente ininteligibles para el usuario, generando una serie de desafíos para la legislación europea anti-discriminación. En primer lugar, con la creación basada en datos de perfiles “sospechosos” puede darse la creación de categorías incomprensibles, en el marco del esquema tradicional de la normativa en materia de discriminación. El aumento de los datos y el poder computacional han permitido desarrollar nuevas prácticas de seguridad en las que las técnicas de minería de datos siguen siendo una caja negra tecnológica para los ciudadanos. De modo que, se hace cada vez más difícil entender las categorías que resultan de formas de generación de perfiles basadas en datos. En segundo lugar, podemos apreciar una falta de transparencia, en relación con el tratamiento de los datos por parte de estos sistemas. Las prácticas contemporáneas de recopilación y procesamiento de datos tienden a producir categorías artificiales y no representativas, en lugar de grupos sociales reales de la vida real, es probable que ni siquiera el individuo sea consciente de haberse convertido en parte de una nueva categoría de riesgo. De modo que, en este tipo de casos, las personas que sean víctimas de un error rutinario del sistema no sabrán, con precisión, cuándo o cómo han sido discriminadas. Además, cabe suponer que un gran porcentaje de estos datos utilizados para la elaboración de perfiles son recopilados por el sector privado, originalmente, con fines comerciales y que las medidas de seguridad no son más que una forma de uso secundario. Por ejemplo, una aerolínea puede haber recopilado estos datos mucho antes de que las agencias de seguridad sustrajesen esta información. Llegados a este punto, podemos apreciar un conflicto en el marco europeo de protección de datos. Ni el principio de proporcionalidad ni las limitaciones de propósito pueden aplicarse a las lógicas invertidas de la generación de perfiles basadas en datos, ya que parten de la suposición de que el usuario debe conocer el objetivo de la recopilación y el procesamiento de sus datos. Y, en tercer lugar, debido a la creación de estas nuevas categorías incomprensibles y a la falta de transparencia en el tratamiento de los datos, se puede apreciar una laguna legal en términos de responsabilidad. Es cierto que las propuestas actuales (SEIAV & RNP) no contemplan decisiones basadas exclusivamente en los datos de los

usuarios, sino que en caso de sospecha, se somete la cuestión a una revisión por parte del policía o agente en frontera. No obstante, las autoridades confían en esta tecnología semi-autónoma que, a medida que evoluciona, es cada vez menos comprensible, incluso para sus propios programadores. Como consecuencia, cada vez es más difícil apreciar a quién –o a qué– se le puede atribuir la responsabilidad por la creación de un perfil discriminatorio para el control y gestión de fronteras.

48 Las redes neuronales –también conocidas como sistemas conexionistas– están formadas por un conjunto de unidades, llamadas neuronas artificiales, conectadas entre sí para transmitir señales. La información de entrada atraviesa la red neuronal –donde se somete a diversas operaciones– produciendo unos valores de salida. Las redes neuronales se han utilizado para resolver una amplia variedad de tareas, como la visión por computador y el reconocimiento de voz, que son difíciles de resolver usando únicamente una programación estructurada –secuencia, selección e iteración–.

V. Conclusiones

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

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

En el desarrollo y uso de perfiles por medios algorítmicos, cabe la posibilidad de que se introduzca un sesgo en cada etapa del proceso. Para evitar esta y otras posibles violaciones de los derechos fundamentales, tanto los expertos en tecnología como los agentes encargados de la interpretación de los datos deben tener una comprensión clara de los derechos fundamentales. Es crucial utilizar datos fiables. Introducir en un algoritmo datos que reflejen sesgos vigentes o procedentes de fuentes poco fiables redundará en resultados sesgados y no fiables.

La elaboración algorítmica de perfiles debe ser legítima, necesaria y proporcionada. El tratamiento de datos debe tener un fin específico. Los interesados tienen derecho a ser informados mediante la notificación de información sobre los datos personales que se recojan y se conserven, sobre el tratamiento y su finalidad, y sobre sus derechos. Los datos deben ser recogidos, tratados y conservados con seguridad. Las autoridades deben documentar las actividades de tratamiento en un expediente –incluida la información sobre el uso que se hace de los datos– y de los registros relacionados –incluida información sobre las personas que acceden a los datos–. Es preciso prevenir y detectar el tratamiento ilícito de datos: (1) mediante evaluaciones de impacto previas; y (2) mediante el uso de herramientas de privacidad integradas "desde el diseño" en el algoritmo.

La elaboración de perfiles mediante la minería de datos predictiva ya es una realidad en todo el mundo, incluida la Unión Europea. Con la interoperabilidad prevista de las bases de datos y los sistemas de seguridad europeos, es probable que se encuentren nuevas formas de generación de conocimiento cada vez más complejas. En este contexto, el legislador europeo debe plantearse si las categorías tradicionales de discriminación siguen siendo efectivas o si éstas deben reformularse. Con esta finalidad, entendemos que se debe evitar el uso de sistemas de información con estructuras en forma de "caja negra" –en los que se controlan los datos de entrada y de salida, pero no su funcionamiento–, y, además, se deben establecer mecanismos que garanticen una mayor comprensión del código de programación de estas bases de datos.

VI. Bibliografía

AMOORE, L.; "Biometric borders: Governing mobilities in the War on Terror". *Political Geography* , n.º 25 (3), 2006, pp. 336-351.

– "Data derivatives: On the emergence of a security risk calculus for our times". *Theory, Culture & Society* , n.º 28 (6), 2011, pp. 24-43.

– The Politics of Possibility: Risk and Security Beyond Probability, Duke University Press, Durham, 2013.

ANRIG, B; BROWNE, W. & GASSON, M.; "The role of algorithms in profiling" en HILDEBRANDT, M. & GUTWIRTH, S.; *Profiling the European Citizen: Cross–disciplinary Perspectives* , Springer, Londres, 2008, pp. 65-88.

ARADAU, C. & VAN MUNSTER R.; "Governing terrorism through risk: Taking precautions, (un)knowing the future". *European Journal or International Relations* , n.º 13 (1), 2007, pp. 89-115.

BECK, U.; "The terrorist threat: World risk society revisited". *Theory, Culture & Society* , n.º 19 (4), 2002, pp. 39-55.

BELLANOVA, R. & DUEZ, D.; "A different view on making of European security; The EU Passenger Name Record system as a socio-technical assemblage".

European Foreign Affairs Review , n.º 17, 2005, pp. 109-124.

BENNET, C. J.; "What happens when you book an airline ticket? The collection and processing of passenger data post-9/11" en ZUREIK, E. & SALTER, M. B.; *Global Surveillance and Policing: Borders, Security, Identity* , editorial Routledge, Cullompton & Portland, 2005, pp. 113-138.

BROWNSWORD, R.; Knowing me, knowing you: "Profiling, privacy and the public interest", en HILDEBRANDT, M; & GUTWIRTH, S; *Profiling the European Citizen: Corss-disciplinary Perspectives* , Springer, Londres, 2008, pp. 345-364.

CAVUSOGLU, H.; BYUNGWAN, K. & RAGHUNATHAN, S.; "An Analysis of the impact of passenger profiling for transportation security". *Operations Research* , n.º 58 (5), 2010, pp. 164-181.

CHENEY-LIPPOLD, J.; "A new algorithmic identity: Soft biopolitics and the modulation of control". *Theory, Culture & Society* , n.º 28 (6), 2011, pp. 164-181.

CRUZ ÁNGELES, J.; Derechos humanos y nuevos modelos de familia. Estudio en el marco de los sistemas europeo e interamericano de protección de derechos humanos, Thomson Reuters Aranzadi, Pamplona, 2018.

– "Procesamiento informático de datos y protección de derechos fundamentales en las fronteras exteriores de la Unión Europea", *Revista Freedom, Security & Justice: European Legal Studies* , n.º 1, 2020, pp. 94-122.

DE VRIES, K.; "Identity, profiling algorithms and a world of ambient intelligence". *Ethics and Information Technology* , n.º 12 (1), 2010, pp. 71-85.

DILLON, M.; "Biopolitics of security" en BURGESS, J. P.; *The Routledge Handbook of New Security Studies* , Routledge, Milton Park & Nueva York, 2010, pp. 61-71.

DILLON, M.; & LOBO-GUERRERO, L.; Biopolitics of security in the 21stcentury; An introduction. *Review of International Studies* , n.º 34 (2), 2008, pp. 265-292.

EDEL, F.; The Prohibition of Discrimination Under the European Convention on Human Rights, Council of Europe Publishing, Estrasburgo, 2010.

GANDY, O. H.; "Engaging rational discrimination: Exploring reasons for placing regulatory constraints on decision support systems". *Ethics and Information Technology* , n.º 12 (1), 2010, pp. 29-42.

GARCÍA ALLER, M.; Lo imprevisible. Todo lo que la tecnología quiere y no puede controlar, editorial Planeta, Barcelona, 2020.

– El fin del mundo tal y como lo conocemos. Las grandes innovaciones que van a cambiar tu vida, editorial Planeta, Barcelona, 2017.

GELLERT R.; DE VRIES K.; DE HERT, P. & GUTWIRTH, S.; "A comparative analysis of anti-discrimination and data protection legislations", en CUSTER B.;

CALDERS, T.; SCHERMER, B. & ZARSKY, T; *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* , Springer, Heidelberg, Nueva York, Dordrecht & Londres, 2013, pp. 61-89.

GILLESPIE, T.; "The relevance of algorithms", en GILLESPIE, T; BOCZOWSKI, P. & FOOT, K.; *Media Technologies: Essays on Communication, Materiality and Society* , MIT Press Scholarship, Cambridge, 2014, pp. 167-194.

HILDEBRANDT, M.; "Defining profiling: A new type of knowledge?", en JILDEBRANDT, M. & GUTWIRTH, S.; *Profiling the European Citizen: Cross-disciplinary Perspectives* , Springer, Dordrecht & Londres, 2008, pp. 17-46.

LEESE, M.; "The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union", *Security Dialogue* , vol. 45 (5), 2014.

LOMBROSO, C.; Le più recenti scoperte ed applicazioni della psichiatria ed antropologia criminale, Fratelli Bocca, Torino, 1893.

– *El delito: Sus causas y remedios* , Victoriano Suárez, Madrid, 1902.

MCCUE, C.; Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis, Elsevier, Oxford, 2007.

SALTER, M. B.; "Passports, mobility and security: How smart can the border be?", *International Studies Perspectives* , n.º 5 (1), 2004, pp. 71-91.

– "Imagining numbers: Risk, quantification and aviation security". *Security Dialogue* , n.º 39 (2), 2008, pp. 243-266.

AA.VV.; *Manual de legislación europea contra la discriminación* , Agencia de los Derechos Fundamentales de la Unión Europea, 2010.

Análisis

Documentos comentados

(Disposición Derogada) Decisión 2007/533/JAI, de 12 de junio . LCEur 2007\1379

- comenta.

(Disposición Vigente) Reglamento (CE) núm. 767/2008, de 9 de julio . LCEur 2008\1384

- comenta.

(Disposición Vigente) Reglamento (UE) núm. 610/2013, de 26 de junio . LCEur 2013\967

- comenta.

(Disposición Vigente) Reglamento (UE) núm. 603/2013, de 26 de junio . LCEur 2013\957

- comenta.

(Disposición Vigente) Reglamento 2017/2226/UE, de 30 de noviembre . LCEur 2017\2141

- comenta.

(Disposición Vigente) Reglamento 2019/817/(UE), de 20 de mayo . LCEur 2019\834

- comenta.

(Disposición Vigente) Directiva 2016/681/UE, de 27 de abril . LCEur 2016\607

- comenta.

(Disposición Vigente) Reglamento 2019/816/(UE), de 17 de abril . LCEur 2019\833

- comenta.

(Disposición Vigente) Directiva 2016/680/UE, de 27 de abril . LCEur 2016\606

- art. 29. ap. 1 comenta.

- art. 11 comenta.

Voces

- DERECHOS Y LIBERTADES
- INFORMÁTICA
- POTESTAD SANCIONADORA DE LA ADMINISTRACIÓN PÚBLICA
- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
- SOCIEDAD DE LA INFORMACIÓN