Los sistemas inteligentes de identificación y reconocimiento biométrico y los derechos humanos

Intelligent identification and biometric recognition systems and human rights

✍ Miguel L. Lacruz Mantecón*

Resumen

Se dice que la inteligencia artificial llegará ser un avance técnico de mayor envergadura que la máquina de vapor en la revolución industrial y que sus repercusiones económicas, sociales y jurídicas serán trascendentales. Los beneficios que esta tecnología conllevarán serán incontables, como hacer más fácil la vida humana o liberar al trabajador de las labores más pesadas y repetitivas. Sin embargo, no hay rosa sin espinas. Algunos autores alertan de los inconvenientes y peligros que también traerá la nueva tecnología. Este es el tema de este artículo, que quiere advertir del riesgo que para los derechos fundamentales del ser humano pueden suponer algunas aplicaciones de la IA.

Palabras clave

Inteligencia artificial, derechos fundamentales, sistemas de reconocimiento biométrico, nudges, perfilado predictivo, calificación social

---

* Profesor titular de Derecho Civil en la Universidad de Zaragoza. El trabajo ha sido escrito al amparo del Proyecto de investigación «Derecho e inteligencia artificial: nuevos horizontes jurídicos de la personalidad y la responsabilidad robóticas», IP. Margarita Castilla, Universidad de Cádiz (PID2019-108669RB-100 / AEI / 10.13039 / 501100011033).

Abstract

Artificial Intelligence is going to be a technical advance greater than the steam engine in the age of Industrial Revolution, and therefore its economic, social and legal repercussions are going to be transcendental. The benefits this technology will bring us will be countless, making human life easier and freeing the worker from the heaviest and most repetitive tasks. However, there is no rose without thorns, and some authors warn of the inconveniences and dangers that new technology will also bring. This is the topic of this article, which wants to warn of the risk that some applications of AI may pose to the fundamental rights of human beings.

Keywords

Artificial intelligence, human rights, biometric recognition systems, nudges, predictive profiling, social credit system

Sumario:

I. LA INTELIGENCIA ARTIFICIAL INVASIVA Y LOS DERECHOS FUNDAMENTALES

En la desaparecida República Democrática Alemana, las actividades sociales de la población y su afecto o desafecto al régimen eran controladas por la *Stasi*, abreviatura del *Ministerium für Staatssicherheit*, es decir, la policía política del régimen comunista. Aunque contaba con numerosos agentes de plantilla, el instrumento principal de este control lo constituían los «colaboradores informales», delatores espontáneos que informaban acerca de las actividades e ideología sus conocidos, amigos, compañeros de trabajo o familiares. El número de colaboradores de activos superaba en cada momento los 200 000, lo que no está nada mal, aunque lejos del sueño totalitario de poner a la mitad de la población del país a vigilar a la otra mitad. No obstante, este sueño del control total es hoy posible, pues contamos con la ayuda de unos delatores incansables y muy diligentes, los sistemas de inteligencia artificial (en adelante, IA), de los que se hablará a continuación. Efectivamente, gracias a la tecnología de la IA ya existen sistemas de control y seguimiento individualizado de las actividades privadas, en particular en China, como veremos más adelante; a título de anécdota, en Singapur actualmente patrullan robots que reconocen conductas no autorizadas como fumar en

casi cualquier sitio o aparcar el coche donde no se debe (Chee Siong, 2023)[1]. Todo indica que vivimos un cambio social como consecuencia de la nueva tecnología. Como nos dicen Pollicino y Paolucci (2022, p. 9), es un hecho que las nuevas ciudades son ciudades inteligentes, cuyo funcionamiento «tiene sus raíces en la combinación del Internet de las Cosas (IoT), el *Big data*, la computación ubicua y la nube. Todos estos elementos son los fundamentos de la arquitectura sobre las que descansa la (ideal) ciudadanía inteligente, y son los encargados de hacerlo más abierta, optimizable y, sobre todo, controlable».

Además, la IA es tremendamente invasiva, puesto que es una tecnología muy fisgona. Según Megías Quirós (2022, p. 140), la limitación de los riesgos derivados de la IA será el objetivo que inspire las más recientes elaboraciones regulatorias en la materia, como son la *Recomendación sobre la Ética de la Inteligencia Artificial* de la UNESCO, de noviembre de 2021[2] (y el subsiguiente *Report of the International Bioethics Committee on the ethical issues of neurotechnology*, de 15 de diciembre de dicho año), así como la europea *Ley de la Inteligencia Artificial*, de 21 de abril de 2021[3].

Estos peligros, por otra parte, derivan precisamente de la perfección del funcionamiento de los sistemas inteligentes, que, como nos señala Megías Quirós (2022, p. 143), al tiempo que traen muchos beneficios, plantean evidentes riesgos para los derechos humanos. En este sentido, recoge De Asís Roig (2022, p. 35) las palabras de Michelle Bachelet, Alto Comisionado de las Naciones Unidas para los Derechos Humanos, en su discurso «Derechos humanos en la era digital ¿Pueden marcar la diferencia?» de 17 de octubre de 2019, cuando dijo: «Es esencial que en esta era digital prestemos especial atención a los derechos humanos […]. La revolución digital plantea un considerable problema de derechos humanos a escala mundial. Sus beneficios indudables no anulan sus riesgos evidentes».

Esta idea de la peligrosidad de la IA es compartida por varios autores, como Martin Ebers (2023), quien nos dice que los sistemas de IA pueden dañar de manera impredecible la vida, la salud y la propiedad de las personas, así como:

---

1 Desde 2021 se realizan pruebas de vigilancia en Singapur con un robot llamado *Xavier*.

2 Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), París, del 9 al 24 de noviembre de 2021, en su 41.ª reunión.

3 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen Normas Armonizadas en Materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, COM/2021/206 final.

> [...] afectar a los valores fundamentales en los que se basan las sociedades occidentales, dando lugar a violaciones de los derechos fundamentales de las personas, incluidos los derechos a la dignidad humana y a la autodeterminación, a la privacidad y a la protección de los datos personales, a la libertad de expresión y de reunión, a la no discriminación o al derecho a la tutela judicial efectiva y a un juez imparcial, así como a la protección de los consumidores. (p. 254)

Pollicino y De Gregorio (2021) advierten que la tecnología inteligente puede ser lesiva *per se* para los derechos de las personas, como consecuencia de su falta de transparencia. En otras palabras, tiene consecuencias negativas sobre derechos fundamentales de las personas, como el derecho a la libre determinación, libertad de expresión y privacidad. Pero además:

> [...] la difusión de la toma de decisiones automatizada también desafía a los sistemas democráticos por su impacto en el discurso público y la imposibilidad de comprender las decisiones que se realizan mediante sistemas automatizados que afectan a los derechos y libertades individuales. (p. 5)

Otros, como Matefi y Darius (2022), afirman que, aunque la IA nos trae innegables beneficios en muchos ámbitos, también en el del derecho, hay que asumir que

> […] derechos fundamentales como el derecho a la intimidad, a la dignidad, a la libertad de expresión, a la libertad de movimiento y a la seguridad de las personas, y muchos otros derechos de la personalidad o fundamentales reconocidos internacionalmente, son infringidos por el uso inapropiado de la IA. (pp. 75-76)

Es precisamente para minimizar los riesgos que afectan a estos derechos que la Unión europea ha seguido dos modelos de regulación distintos, uno ético y otro jurídico, elaborando primero textos de fijación de directrices éticas, y luego de propuestas normativas, que culminan en la ya citada Ley de Inteligencia Artificial[4]. Este texto, según Megías Quirós (2022, p. 158), concreta los derechos reconocidos en la Carta de Derechos Fundamentales de la UE que pueden verse afectados

[4] *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el Que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión*, 21 de abril de 2021, COM(2021) 206 final.

por el uso de sistemas inteligentes. Serían los siguientes: el derecho a la dignidad humana (art. 1); el derecho a la vida privada y familiar y la protección de datos de carácter personal (arts. 7 y 8); el derecho a la no discriminación y la igualdad entre hombres y mujeres (arts. 21 y 23); el derecho a la libertad de expresión y reunión (arts. 11 y 12); el derecho a la tutela judicial efectiva y a un juez imparcial, a la presunción de inocencia y los derechos de la defensa (arts. 47 y 48); y, asimismo, los derechos de determinados grupos, como el de las condiciones justas y equitativas del trabajador (art. 31), o el derecho a la protección del consumidor (art. 28), los derechos del niño (art. 24) y la integración de las personas discapacitadas (art. 26).

La preocupación por la irrupción de los sistemas inteligentes y su posible efecto negativo para la protección de los derechos de las personas se detecta en otros textos europeos. Destaca Coca Payeras (2023, p. 24) con *Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales*. Este texto impone la necesidad de garantizar el respeto a los derechos y libertades fundamentales consagrados en la Carta de derechos fundamentales, así como la necesidad de que la tecnología de IA se desarrolle de manera que sitúe a las personas en su centro. Además, alerta sobre la utilización de herramientas de IA por las autoridades judiciales para la toma de decisiones sobre prisión preventiva, o para dictar sentencias, calcular las probabilidades de reincidencia y determinar la libertad condicional o resolver litigios en línea.

Esta resolución expresa también gran preocupación por el uso de las fuerzas policiales y servicios de inteligencia de bases de datos de reconocimiento facial, como la base *Clearview AI*, una base de datos de más de 3000 millones de imágenes que se han recopilado de redes sociales y otros lugares de internet. Asimismo, se preocupa por el uso de la inteligencia artificial en el control de fronteras, como, por ejemplo, el proyecto europeo *iBorderCtrl*, un sistema inteligente de detección de mentiras, que, como dice Coca Payeras (2023), «elabora perfiles de los viajeros a partir de una entrevista automatizada por ordenador realizada a través de la cámara web del viajero antes del viaje y un análisis de 38 microgestos basado en la inteligencia artificial, probado en Hungría, Letonia y Grecia». Ante estos sistemas de reconocimiento o biométricos, la resolución pide a la Comisión que, por medios legislativos y no legislativos, y si es necesario a través de procedimientos de infracción, prohíba el tratamiento de datos biométricos, incluidas las imágenes faciales, mediante vigilancia masiva en espacios públicos con fines coercitivos (epígrafe 31).

II. LOS SISTEMAS DE IA Y SU INCIDENCIA EN LOS DERECHOS FUNDAMENTALES

1. El paso de la regulación ética a la normativa: la *Ley de la IA*

Como señala, desde la filosofía del derecho, Francisco de Asís Roig (2022, p. 38), la evitación de estos males pasa por una defensa de los derechos fundamentales con base jurídica, eventualmente complementada con el reconocimiento de nuevos «neuroderechos» (con la precaución de no crear una inflación de los mismos que los devalúe) y, asimismo, con nuevas normas y textos internacionales. Da cuenta así de que la Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos, en su informe sobre *El derecho a la privacidad en la era digital* (2021), proclama que los Estados deben establecer mecanismos de supervisión y reparación relacionados con la privacidad. Y la UNESCO, a través de su Comité Internacional de Bioética, emitió un informe el 15 de diciembre de 2021 sobre *Cuestiones Éticas de la Neurotecnología*, en el que se encuentran sugerencias como las siguientes:

a) Agregar protocolos a los tratados internacionales, como la Declaración Universal de los Derechos Humanos, para abordar los desafíos que plantean las neurotecnologías.

b) Reforzar la Declaración Universal de los Derechos Humanos, considerando que la neurotecnología desafía los derechos humanos existentes y que se requerirán nuevas garantías en función de las posibilidades de vulneración.

c) Elaborar una Nueva Declaración Universal de Derechos Humanos y Neurotecnología.

En esta línea, el Congreso chileno aprueba el 12 de abril de 2021 una reforma constitucional que reconoce el derecho a la integridad neuronal.

Volviendo al ámbito europeo, la vía por la que se opta es más la de la defensa de los derechos de la persona que la de la creación de nuevos neuroderechos. Resume Megías Quirós (2022, p. 155) que la evolución de la normativa europea sobre IA y protección de los derechos humanos, señalando que los primeros textos europeos sobre cuestiones éticas de la IA siguen un camino similar al de la UNESCO, fijando inicialmente algunos principios éticos objetivos en tema de IA, pero luego incidiendo en la vía jurídico-normativa. El primer texto del Parlamento Europeo con contenido ético significativo fue la Carta sobre robótica, en la Resolución del

16 de febrero de 2017[5]. Le sigue la Resolución del 12 de febrero de 2019[6], sobre política industrial global europea en materia de inteligencia artificial, en la que, «[…] además de instar a la Comisión a revisar y adaptar la legislación europea a la nueva realidad desde una perspectiva ética, concretaba nuevos principios para complementar la legislación e insistía en la aprobación "de una carta ética de buenas prácticas para la IA"». En España tenemos la *Carta de derechos digitales*, adoptada en julio de 2021 por el Gobierno, que se inscribe en el contexto de la Estrategia Española Nacional de Inteligencia Artificial de 2020, pero que carece de efectos normativos.

Es a partir de 2020, cuando la UE reconoce la insuficiencia del marco ético para una protección eficaz de los derechos humanos frente a la IA, que se pasa a proponer a la Comisión la aprobación de dos reglamentos de aplicación en los Estados de la UE. Como nos dice Megías (ibid.), «[e]l primer Reglamento propone un marco regulador de la IA con la conversión de principios éticos en obligaciones jurídicas, porque «los principios éticos comunes solo son eficaces cuando están también asentados en Derecho y porque las orientaciones éticas son un buen punto de partida, pero no garantizan que los desarrolladores, desplegadores y usuarios actúen de manera justa ni aseguran la protección eficaz de las personas». El segundo Reglamento es la *Resolución 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial*, que propone el establecimiento de un régimen de responsabilidad civil, objetiva y subjetiva, para que pueda reclamarse cualquier daño causado por la IA.

Sin embargo, en 2021, el paso definitivo hacia una regulación de una IA que va más allá de la ética lo da la *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial*[7], la llamada *Ley de Inteligencia Artificial* (LIA), que establecería un marco jurídico mediante normas claras para garantizar una IA fiable, segura y respetuosa con los derechos fundamentales. Destaca en este sentido Coca Payeras (2023, p. 24) que, entre los objetivos de la *Ley de la IA*, según su «Exposición de

---

5 Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).

6 Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088(INI))

7 Bruselas, 21 de abril de 2021, COM(2021) 206 final, 2021/0106(COD)

motivos», están los de «garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión», así como los de «mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA».

En definitiva, no bastan los principios éticos para la salvaguarda de los derechos fundamentales, y por eso la «Exposición de motivos» de la LIA dice que, en consecuencia, «[…] las normas relativas a la IA […] deben estar centradas en las personas, a fin de que la población tenga la seguridad de que la tecnología se usa de un modo seguro y en consonancia con la ley, lo que también implica respetar los derechos fundamentales».

Los últimos textos europeos siguen también esta línea, en particular la Declaración conjunta del Parlamento Europeo, el Consejo y la Comisión del 23 de enero de 2023 sobre los Derechos y Principios Digitales para la Década Digital[8]. Como dice Coca Payeras (2023, p. 37), en su Preámbulo esta Declaración insiste en su primer capítulo en que las personas constituyen el núcleo de la transformación digital de la Unión Europea, y que esta tecnología debe servir y beneficiar a todos los europeos para que cumplan sus aspiraciones, «[…] en total seguridad y respetando plenamente sus derechos fundamentales. Nos comprometemos a: […] b) adoptar las medidas necesarias para que los valores de la UE y los derechos de los ciudadanos reconocidos por el Derecho de la Unión se respeten tanto en línea como fuera de línea; c) fomentar y garantizar una acción responsable y diligente por parte de todos los agentes digitales, públicos y privados, en el entorno digital; d) promover activamente esta visión de la transformación digital, también en nuestras relaciones internacionales». Como vemos, una reiteración continua de la necesidad de respeto de los derechos de las personas (y por tanto, un reconocimiento del riesgo que plantean estas nuevas técnicas para estos derechos).

II. La IA como generadora de riesgo para los derechos de las personas

2.1. Sistemas prohibidos (con excepciones)

En la citada *Ley de la IA*, Propuesta de Reglamento europeo de abril de 2021, se distingue inicialmente en su articulado, tras una serie de conceptos y definiciones, una serie de *Prácticas de Inteligencia Artificial Prohibidas*, según reza el Título II de esta Ley. Veamos cuáles son estas aplicaciones técnicas de la

8 *Diario Oficial de la Unión Europea*, 22 de enero de 2023, C 23/1.

IA que son prohibidas por conllevar riesgos inaceptables para los derechos fundamentales, señalando así el artículo 5 (LIA) que quedan prohibidas las siguientes *prácticas* de inteligencia artificial:

- Las técnicas subliminales *que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento* provocando perjuicios físicos o psicológicos a esa persona o a otra. Es decir, técnicas de persuasión subliminal. Asimismo, las *técnicas de persuasión* que aprovechen vulnerabilidades de grupos específicos de personas debido a su edad o discapacidad física o mental *para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo* de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra. En definitiva, técnicas de persuasión y alteración subliminal de comportamientos.
- La utilización de sistemas de IA por las autoridades públicas para evaluar o clasificar a personas físicas *atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas*, de forma que la clasificación social resultante dé lugar a situaciones de trato perjudicial o desfavorable en contextos sociales sin relación con el que generó los datos de clasificación, o que sea desproporcionado con respecto al comportamiento social clasificado. Estamos ante técnicas de perfilado de sujetos y calificación social de los mismos.
- El uso de *sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público* salvo que sea estrictamente necesario para la búsqueda selectiva de víctimas concretas de un delito, incluidos menores desaparecidos; la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas, como un atentado terrorista. En particular, la identificación de personas relacionadas con delitos especialmente importantes como pertenencia a organización delictiva, terrorismo, trata de seres humanos, explotación sexual de niños y pornografía infantil, tráfico de drogas o de armas[9]. Una técnica de identificación biométrica se traduce en la vigilancia espacial de los sujetos en tiempo real y, como veremos, se puede trasladar sus resultados, una vez identificado el sujeto, al ámbito de la calificación social del mismo.

[9] Se trata de los delitos recogidos, como nos dice el art. 5.1.iii de esta *Ley de la IA*, en la «Decisión Marco 2002/584/JAI del Consejo, para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años […]».

Estos sistemas de identificación biométrica son especialmente agresivos para los derechos fundamentales, por lo que, además de esta prohibición, se establece en la *Ley de la IA* una serie de cautelas para su utilización, como lo son el tener en cuenta sus consecuencias para los derechos y las libertades de las personas implicadas, la adopción de salvaguardias para su uso, el establecimiento de limitaciones temporales, geográficas y personales y, además, *autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema*.

2.2. Sistemas de alto riesgo

No terminan aquí las amenazas de la IA a los derechos fundamentales, aparte de estos sistemas prohibidos o de riesgo inaceptable, la *Ley de la IA* también refiere una serie de sistemas que se admiten pero que son calificados como de *alto riesgo*. Se trata de sistemas de IA referidos en los Anexos II y III de esta Ley, que se aplican a tareas como las relacionadas con la salud, funcionamiento del tráfico rodado y el suministro de agua, gas, calefacción y electricidad, o sistemas de selección para el acceso a instituciones educativas y al empleo. Asimismo, se incluyen los sistemas para la calificación crediticia o solvencia, o los sistemas empleados por las autoridades públicas para la aplicación de la ley, o la administración de justicia y la gestión de la migración, el asilo y el control fronterizo.

Pero, como puede comprobarse, aquí no se está haciendo referencia a una aplicación técnica de la IA en particular, sino a la utilización de los sistemas inteligentes en funciones de control de ámbitos sensibles (datos médicos, regulación del tráfico, control de suministro de agua y energía), en los cuales se precisa una vigilancia especial para evitar daños a las personas. Es decir que el concepto de *alto riesgo* va aquí referido a determinados ámbitos de utilización de la IA, mientras que el concepto de *prohibición* —o riesgo inaceptable— se aplica directamente a técnicas concretas de IA que actúan inmediatamente sobre las personas.

2.3. Diferencia entre ambos tipos de sistemas

A partir de lo anterior, veo que es posible diferenciar, por un lado, sistemas inteligentes que son, por el riesgo que producen para los derechos fundamentales, lesivos *per se* para estos derechos, cuya utilización o está prohibida o solo es posible con carácter excepcional y con fuertes medidas de control; por otro lado, están los ámbitos en los que el mal funcionamiento de sistemas inteligentes conlleva un riesgo de afectación a los derechos fundamentales, ya sea por gestionar infraestructuras o instalaciones básicas para la vida en sociedad (suministros de agua,

electricidad, líneas de datos) o por tratarse de actividades que implican intervención pública o que tienen carácter especialmente delicado (administración de justicia, educación, empleo, instituciones financieras), en las cuales pueden producirse fácilmente lesiones a los derechos de las personas por un funcionamiento sesgado o por una avería del sistema.

Esto es lo que diferencia la lesión en uno y otro caso: en el supuesto de los sistemas inteligentes de riesgo inaceptable o prohibidos, los daños se producen por el buen funcionamiento del sistema, que consigue resultados que van más allá de lo que se podría esperar mediante la intervención exclusivamente humana; en cambio, en los sistemas inteligentes que actúan en ámbitos sensibles o de alto riesgo, los daños derivan del mal funcionamiento del sistema, que padece errores o disfunciones (sesgos, averías, bucles o caídas del sistema) que producen lesión a los derechos de las personas.

Veamos a continuación de qué riesgos estamos hablando y cuáles son estas técnicas de IA peligrosas para los derechos fundamentales.

III. LAS TÉCNICAS DE IA AGRESIVAS CON LOS DERECHOS FUNDAMENTALES

1. Los sistemas de datos biométricos, en general

Los sistemas de reconocimiento de personas por sus datos biométricos son invasivos por sí mismos e impactan directamente en la protección de datos personales prescrita en el artículo 16 del Tratado de Funcionamiento de la Unión Europea. Se trata de la utilización de sistemas inteligentes que, a través de videocámaras, reconocen los rasgos faciales de las personas y, a partir de estos, la identidad de cada persona en particular. A esto se puede añadir que, mediante diversos periféricos (medidores de tensión arterial, cámaras termográficas, escáner de huellas, micrófonos), se obtienen otros datos corporales como huellas dactilares, temperatura corporal, frecuencia cardiaca, sudoración o respiración del sujeto, tono de voz, movimiento de las pupilas, datos que permiten ampliar la exploración a informes sobre el estado de salud, emociones o incluso pensamientos de la persona, como veremos luego.

La *Ley de la IA* de 2021 procede a definir los «Datos biométricos» en el art. 3, núm. 33) como «[…] los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha

persona, como imágenes faciales o datos dactiloscópicos»[10]. Distingue Cotino Hueso (2023, p. 348) entre identificadores «fuertes», los cuales son más utilizados por las tecnologías identificadoras de primera generación (huellas dactilares, ADN, estructura del iris, rostros, voz), e identificadores «débiles», que cada vez cobran más protagonismo (formas de andar, patrones de vasos sanguíneos, patrones de pulsación de teclas etc.): «[c]on la nueva generación de tecnologías se va más allá de la finalidad de identificación y se habla de "biometría del comportamiento" para el perfilado, reconocimiento de emociones o categorización de personas. Es por ello que, frente a los datos biométricos ligados únicamente a la identificación, se propone el concepto más amplio inclusivo de "datos basados en la biometría"».

A continuación, el art. 3 LIA define los distintos sistemas de datos biométricos, definiciones que nos proporcionan una muestra de las diferentes aplicaciones de esta técnica:

> 34) Sistema de reconocimiento de emociones: un sistema de IA destinado a detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos. 35) Sistema de categorización biométrica: un sistema de IA destinado a asignar a personas físicas a categorías concretas, como un sexo, edad, color de pelo, color de ojos, tatuajes, origen étnico u orientación sexual o política, en función de sus datos biométricos. 36) Sistema de identificación biométrica remota: un sistema de IA destinado a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada.

A su vez, estos sistemas de identificación remota pueden funcionar *en tiempo real* —es decir, procediendo a una identificación instantánea— o *en diferido*.

Apunta Ebers (2022, p. 267) a que el art. 5.1.d) de la LIA prohíbe los sistemas de IA de identificación biométrica remota (*biometric identification system* o BIS) «en tiempo real» en espacios de acceso público (por ejemplo, los sistemas de reco-

10 Repite la definición del art. 3 de la *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo*, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, «13) "datos biométricos": datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos».

nocimiento facial utilizados para identificar a una persona en la calle), pero que este enfoque de prohibir únicamente los sistemas de identificación biométrica utilizados para la aplicación de la ley es demasiado restrictivo, y sus excepciones demasiado amplias. Critica también que el reconocimiento automatizado de características como el sexo, la sexualidad o el origen étnico, lo que se conoce como *biometric categorization systems* o BCS, así como el reconocimiento automatizado de las emociones (*emotion recognition system* o ERS)[11], no están prohibidos por la LIA.

Por su parte, el Gobierno estadounidense elabora en octubre de 2022 un texto de directrices denominado *AI Bill Of Rights - Making Automated Systems Work For The American People*[12], en el que se tiene en cuenta la identificación biométrica. Y autores como Margaret Hu (2022) advierten que estos sistemas biométricos —que ya están siendo usados para fines de vigilancia y control de fronteras, seguridad e inmigración— son de «alto riesgo», así como pueden colisionar con derechos constitucionales fundamentales y derechos humanos. En definitiva, se trata de un desafío normativo-constitucional de primer orden.

El análisis de estos datos biométricos permite conseguir toda una serie de resultados que vamos a ver a continuación, además de que su incidencia sobre los derechos fundamentales de las personas puede ser radical. Es cierto que esta técnica tiene una serie de utilidades prácticas, como la de utilizar la «huella facial» para desbloquear un teléfono móvil o la de acceder a cuentas bancarias, pero su utilización principal es policial, como veremos. Da cuenta Lucasiewicz (2022, p. 391) de una curiosa utilización del reconocimiento facial, la de encontrar en los bancos de gametos a los donantes más semejantes a los receptores del material genético, para lograr que los hijos se les parezcan.

Pese a estos usos poco conflictivos, como señala Cotino Hueso (2022, p. 71), la tecnología biométrica tiene el potencial de impactar prácticamente en todos los derechos fundamentales de las personas. Entre ellos, la Agencia de la Unión Europea para los Derechos Fundamentales (FRA) menciona los siguientes derechos: «la dignidad humana, al respeto de la vida privada, la protección datos personales, la no discriminación, los derechos del niño y de los mayores, los

---

11 Un sistema inteligente de reconocimiento de emociones trata de detectar diferentes emociones del sujeto mediante la información procedente de las expresiones faciales, el movimiento corporal, los gestos y el lenguaje.

12 *AI Bill Of Rights - Making Automated Systems Work For The American People,* October 2022. En https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf

derechos de las personas con discapacidad, la libertad de reunión y asociación, la libertad de expresión, el derecho a una buena administración, y el derecho a un recurso efectivo ante la ley y a un juicio justo». Y esto en las distintas aplicaciones de la recolección de datos biométricos, que pasaremos a examinar.

2. Aplicaciones de los datos biométricos

2.1. Sistemas de identificación y localización de personas

Los sistemas biométricos llevan tiempo siendo utilizados para asuntos como desbloquear el teléfono móvil, aunque su aplicación estrella consiste en la vigilancia policial, identificación de personas y seguimiento de las mismas. La incidencia de estas técnicas sobre los derechos fundamentales es brutal. Advierte Cotino Hueso (2022, p. 72) que nada impide hoy a la policía detectar a un ciudadano en la vía pública o en una manifestación, identificarlo y analizar si está en alguna base de datos específica, georreferenciarlo y reconstruir sus recorridos e interacciones con otras personas y, además, evaluar su comportamiento. Cabe añadir que si procesamos los datos de su teléfono móvil, la información puede completarse con todos los perfiles que quepa extraer de dicho dispositivo.

Desde EE. UU., el profesor de la Universidad George Washington, Jonathan Turley (2020), señala que las sociedades-pecera, en las que no existe ningún tipo de intimidad, han sido una creación literaria y cinematográfica de éxito, así en títulos como *1984*, *Fahrenheit 451*, *Minority Report* o *Total Recall*. Pero estas tecnologías suponen un ataque a la intimidad personal y ya hay sentencias que afirman la lesividad de las mismas, como la del Tribunal de Apelaciones del Noveno Circuito de los Estados Unidos, en *Patel vs. Facebook*, *Inc.*[13], que condenó a Facebook en 2019 por la recopilación no consensuada de archivos faciales de los usuarios. El tribunal concluyó que la creación de una base de datos de rostros e identidades constituía una conducta contraria a la Illinois Biometric Information Privacy Act (BIPA).

Dada su potencial peligrosidad, el tratamiento jurídico que reciben estos sistemas en la *Ley de la IA* europea no es suficientemente protector de los derechos fundamentales. Como señala Cotino Hueso (2022, pp. 69 y 70), las prohibiciones y restricciones de los arts. 5 y 6 de la indicada Ley no impiden realmente la vulneración de derechos, pues los «sistemas de identificación biométrica» que en

13 *Patel v. Facebook, Inc.,* N.º 18-15982 (9th Cir. 2019)

principio estarán prohibidos son los que funcionan en tiempo real, en espacios de acceso público y con fines policiales. Luego a contrario, «…no estarían prohibidos los reconocimientos faciales que no funcionen a partir de imágenes en tiempo real, algo que ha sido especialmente criticado… Tampoco estarían prohibidos en los lugares que no sean de acceso al público, como locales de empresas y fábricas, oficinas y lugares de trabajo, las prisiones, zonas de control fronterizo y espacios en línea (Considerando 9 AIA[14])». Quedan fuera de la prohibición estos ámbitos, y también las finalidades de defensa e inteligencia y el ámbito de la migración y solicitudes de asilo, según el art. 5.4 AIA, versión Presidencia checa 2022. En el ámbito estrictamente privado, no hay que excluir las finalidades de seguridad privada en establecimientos de acceso público (supermercados, transporte, estadios, escuelas) ni tampoco las finalidades privadas de marketing, comercio u otras.

Desde el punto de vista de la normativa de protección de datos, el tratamiento de los datos obtenidos mediante técnicas biométricas está sometido al régimen general de protección de datos de la ley española, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD), en su art. 9, al tratarse de una *categoría especial* de datos. Aparecen específicamente mencionados los datos biométricos como categoría especial también en el art. 9 del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales[15] (RGPD), y se les suman las garantías de los tratamientos automatizados del art. 22 de dicho Reglamento. Sin embargo, el mismo art. 9 RGPD permite excepcionalmente el tratamiento de estos datos especiales cuando *g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado*.

Apunta Cotino Hueso (2022, p. 73) que el uso de sistemas biométricos en el ámbito policial y penal quedará bajo la regulación especial de la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa

14 AIA es la denominación en inglés de la LIA: *Artificial Intelligence Act*.

15 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…*

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[16]. En esta Directiva, el tratamiento de los datos biométricos como datos personales aparece en el art. 10:

> El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física… solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando: a) lo autorice el Derecho de la Unión o del Estado miembro…

Y la necesidad estricta, y consiguiente autorización, nos la señala el art. 5 de la LIA, que permite el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público para fines de aplicación de la ley con los objetivos siguientes:

> i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos; ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista; iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo 62, precepto este que hace referencia a una larga serie de delitos[17].

16 De la misma fecha es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos, que sustituye al anterior Reglamento General de Protección de Datos de 1995.

17 Como son los de: pertenencia a organización delictiva, terrorismo, trata de seres humanos, explotación sexual de los niños y pornografía infantil, tráfico ilícito de estupefacientes y sustancias psicotrópicas, tráfico ilícito de armas, municiones y explosivos, corrupción, fraude, blanqueo del producto del delito, falsificación de moneda, delitos de alta tecnología, en particular delito informático, delitos contra el medio ambiente, incluido el tráfico ilícito de especies, ayuda a la entrada y residencia en situación ilegal, homicidio voluntario, agresión con lesiones graves, tráfico ilícito de órganos y tejidos humanos, secuestro, detención ilegal y toma de rehenes, racismo y xenofobia, robos organizados o a mano armada, tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte, estafa, chantaje y extorsión de fondos, violación de derechos de propiedad industrial y falsificación de mercancías, falsificación de documentos administrativos y tráfico de documentos falsos, falsificación

Como señala Turley (2020, pp. 2206 y 2207), a diferencia de inventos anteriores, esta nueva técnica no es el resultado de un simple avance tecnológico como en las escuchas telefónicas o los dispositivos de escucha no intrusivos como los micrófonos direccionales. Además, está diseñada en gran parte para utilizar imágenes o datos que se coloquen por el propio sujeto a disposición de cualquiera en un ámbito público. Los datos de los que se nutre son variadísimos, desde la imagen facial o del iris a sistemas que identifican a las personas por su manera de caminar, o por reconocimiento de su voz, sistemas de reconocimiento de pulsaciones de teclas, sistemas de reconocimiento de venas en las manos y muchos más: El ejército estadounidense han comenzado a utilizar una tecnología que puede detectar con láseres infrarrojos la *firma cardíaca* única de personas con una precisión del 95 % y un alcance de 200 metros.

La utilización policial de estos sistemas ha sido discutida desde su inicio, como exponen Pollicino y Paolucci (2022, p. 9): Frente a la utilización por la policía inglesa de sistemas de reconocimiento de asistentes a eventos públicos, entre mayo de 2017 y abril de 2019, un activista por los derechos humanos, el Sr. Bridges, reclamó ante los tribunales exigiendo el respeto a su derecho a la privacidad. Rechazada su demanda en primera instancia, el tribunal de apelación la admitió, declarando ilegal el uso de la tecnología biométrica por lesión a la privacidad y a la protección de datos de los particulares, con efectos negativos sobre la libertad de expresión y asociación[18]. Por su parte, relata Cotino Hueso (2023, p. 348) que la utilización de sistemas de reconocimiento para fines policiales de vigilancia o seguridad pública es ya un hecho incluso en las democracias europeas, dando cuenta de su uso en países como Inglaterra, Alemania, EE. UU., Brasil, Países Bajos o Italia. En los Países Bajos, varios municipios utilizan reconocimiento facial durante los carnavales y otros grandes eventos y desde 2016 la policía holandesa utiliza el sistema de reconocimiento facial CATCH a través de las imágenes de los teléfonos inteligentes, las cámaras corporales y la nube. En Italia el Garante italiano de la protección de datos considero inadmisible el 16 de abril de 2021 el «Sistema Automatico di Riconoscimento Immagini» *SARI*, utilizado desde 2019. En Alemania, en Hamburgo con motivo de una reunión del G20 en 2017 se implantó un sistema de reconocimiento facial a partir de grabaciones para la detección e investigación de delitos, aunque. Se usa también esta

de medios de pago, tráfico ilícito de sustancias hormonales, tráfico ilícito de materiales radiactivos, tráfico de vehículos robados, violación, incendio voluntario, delitos incluidos en la jurisdicción de la Corte Penal Internacional, secuestro de aeronaves y buques, sabotaje.

18 *Bridges v. South Wales Police*, Case N.°: C1/2019/2670

identificación por empresas privadas, sobre todo almacenes y tiendas, y así en España, la cadena de supermercados *Mercadona*, recibió una fuerte sanción por implantar un sistema inteligente biométrico que controlaba si quienes accedían a algunos establecimientos estaban en sus listas de «personas con una orden de alejamiento o medida judicial análoga en vigor»[19].

2.2. El perfilado predictivo

El perfilado se define en el art. 4.4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[20]:

> 4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Surge como técnica que parte de la obtención de datos del sujeto, para empezar el de su identidad personal y digital (su dirección IP, número de móvil, dirección de correo electrónico, avatar o *nickname*), y otros acerca de sus intereses vitales (políticos, deportivos, ideológicos o religiosos), nivel económico y de gasto, preferencias de consumo y de entretenimiento, etc. Su objeto es obtener una imagen del sujeto que permita abordarlo con mensajes de todo tipo, desde publicidad y ofertas de turismo o inmobiliarias a información política o económica, con el objeto de provocar decisiones de compra o actuaciones de cualquier tipo en dicho sujeto-objetivo. Todos tenemos la experiencia de los reclamos que llegan a nuestro móvil, comerciales o de ocio.

La incidencia del perfilado en los derechos fundamentales tiene lugar sobre todo en el derecho a la intimidad y privacidad: su funcionamiento implica la creación de bases de datos de características personales de conjuntos de sujetos muy amplios. Bien es verdad que en muchos casos el identificador del sujeto no es sino

---

19 Resolución de la Agencia Española de Protección de Datos, procedimiento sancionador PS 120/2022

20 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). «DOUE» núm. 119, de 4 de mayo de 2016.

una dirección IP, pero a partir de ahí y relacionando este dato con otros, es fácil llegar a la identidad real del mismo. Desde una finalidad sobre todo mercantil, el perfilado evoluciona a un ámbito de previsión de la conducta futura del sujeto, partiendo de los datos obtenidos y de las conductas observadas en el pasado, y de datos de tipo emocional obtenidos indirectamente.

Con esta finalidad, el perfilado, como estudio probabilístico o actuarial del individuo y la posibilidad de que observe un determinado comportamiento, ha sido desarrollado sobre todo en el ámbito penal, donde Solar Cayón (2022, p. 382) advierte que es habitualmente empleado en la mayoría de jurisdicciones estatales para informar las decisiones judiciales sobre medidas cautelares, en particular la concesión o no de libertad provisional. Señala que estos sistemas de evaluación de riesgos de reincidencia criminal se basan en modelos estadísticos generados automáticamente mediante *machine learning*, a partir del análisis de grandes volúmenes de datos correspondientes a casos pasados. Con este aprendizaje los sistemas inteligentes son capaces de detectar una serie de correlaciones entre determinados factores personales y sociales y el riesgo de comisión de futuros delitos: «[…] indicadores relativos a las circunstancias personales del acusado (edad y sexo, nivel de estudios, contexto familiar, situación socio-laboral, consumo de drogas […]), elementos socio-demográficos (lugar de residencia, contexto socioeconómico, relaciones sociales […]) y su historial judicial (detenciones y delitos previos, historial de violencia, precedentes de incomparecencia ante el tribunal […])». Todos estos datos son factores predictores del riesgo de reincidencia futura, asignando a cada uno un valor en función del análisis de los casos pretéritos. Por su parte Juliá-Pijoan (2023, p. 443) nos señala, como ejemplos de estos sistemas, el programa americano COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) o el catalán RISCANVI, programas de gestión penitenciaria que con base en datos personales del sujeto detectan su posibilidad de reincidencia delictiva. Y advierte que el sesgo en el que pueden incurrir estos programas es el de la búsqueda de diferencias cerebrales a partir de un modelo de «normalidad cerebral» puramente arbitrario.

Naturalmente, el siguiente paso consistirá en pasar de la ayuda para la decisión administrativa a la decisión judicial automática, a los «jueces-robot», como nos cuenta De Asís Pulido (2022, p. 328) que ya funcionan en China, si bien todavía en funciones de apoyo y dejando la decisión final al juez humano, como el programa Xiao Zhi, en la Corte Suprema Popular de China:

> Esta máquina organiza los eventos del proceso, analiza la presentación de los casos en lo relativo a su admisibilidad, resume los puntos en los que las

> partes están en desacuerdo, ayuda en la evaluación de las pruebas y crea propuestas de resoluciones judiciales (Chen/Li, 2020, 15).

Estos sistemas pueden funcionar tanto en modo decisorio como en predictivo, pero este tema excede de los límites de este breve trabajo. O incluso cabe dar un paso más y, como nos dicen los argentinos Salvi y Nigri (2022, p. 3), entrar en el terreno de la ciencia-ficción, configurando sistemas predictivos que se anticipen a la comisión del crimen, como se ve en la película *Minority Report*.

El perfilado implica la clasificación de las personas según las características que se determinen en el algoritmo. A esto se refiere el art. 3 de la LIA cuando define en su número 35 a un «Sistema de categorización biométrica» como […] sistema de IA destinado a asignar a personas físicas a categorías concretas, como un sexo, edad, color de pelo, color de ojos, tatuajes, origen étnico u orientación sexual o política […] Claro que olvida algo importante, datos económicos e intereses de consumo. O peor, datos médicos y neurológicos, pues como nos cuenta González Tapia (2022, p. 328), mediante inteligencia artificial se puede lograr una extracción indirecta de datos neuronales de las personas a través de patrones de comportamiento, detección de emociones, tono y modulación del lenguaje, y datos biométricos. Y pone como ejemplo la detección temprana de enfermedades «[…] que puede hacerse, entre otros medios, a través del patrón de tecleo en el móvil con relación al Párkinson, de deambulación con respecto al Alzheimer o patrones de atención […]. Así mismo, datos relativos a navegación por las redes sociales y el análisis de los mensajes arrojados en ellas, permiten detectar riesgos como comportamientos o ideaciones suicidas». En el ámbito laboral, los datos obtenidos sobre las emociones sentidas por los trabajadores pueden informar sobre su motivación.

Otro ámbito en el que se desarrolla el perfilado es el de la averiguación de tendencias políticas, pues como señala Garriga Domínguez (2022, p.452), el desarrollo actual de la tecnología de IA permite el perfilado ideológico de los usuarios de cualquier plataforma, tanto con finalidades de marketing como políticas: «[…] La aplicación de la IA en estos ámbitos permite el perfilado ideológico individual y, a través de las técnicas de focalización podrá elaborarse información política personalizada, El desarrollo de los procesos de segmentación de mercados ha evolucionado hacia una segmentación psicográfica avanzada, que se basa en un algoritmo que determina una serie de rasgos demográficos y de actitud que permite distinguir a cada individuo para cada segmento objetivo y que permite hacer predicciones precisas de la reacción de la audiencia objetiva […] la cantidad y calidad de la información personal que se encuentra en las redes sociales, permite

a los anunciantes mejorar el alcance e impacto de su publicidad […]. Obviamente, estas técnicas pueden utilizarse para vender un producto determinado, pero también para favorecer una determinada ideología». Y, naturalmente, a partir de esta personalización, se abre la vía hacia la interpretación interesada, el *nudge* político y la información parcial o sesgada. En suma, la desinformación del sujeto, cuyas decisiones dejan de ser libres porque no han sido libremente formadas.

Esto ya lo vaticinó Víctor Drummond (2004, pp. 117 y 118), al considerar que las simples *cookies*, pese a su aspecto inofensivo, permitían un control de la navegación en Internet del sujeto y de sus perfiles y hábitos de consumo. Control propio de los sitios web de comercio electrónico, ya que «cuando se efectúa una compra o cualquier otro negocio en la red, el usuario deberá proporcionar voluntariamente una serie de datos personales. En ese momento, su nombre, dirección, número de tarjeta de crédito, entre otros datos, se integrarán automáticamente a una misma base de datos, junto con otras informaciones involuntariamente recogidas a través de las cookies». Este cruce de datos es un ejemplo auténtico de la transformación de datos en un principio irrelevantes en un perfil peligrosamente público del ciudadano.

Las cookies ya están superadas, el problema actual lo plantean las técnicas de detección de la huella digital, de las que nos habla Fernando Pablo (2023, p. 33), técnicas que permiten el seguimiento de comportamiento en Internet de los usuarios finales, sin la protección de la Directiva 2002/58/CE, generando información que se puede recopilar con fines de identificación y seguimiento, utilizando técnicas que se describen como «toma de huellas digital del dispositivo» (generalmente sin el conocimiento del usuario), almacenando datos sobre sus actividades en línea o la ubicación física de su equipo. Como señala la *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales* en el sector de las comunicaciones electrónicas[21] en su Considerando 15, «[…] a medida que la tecnología avanza, aumentan también los medios técnicos para la interceptación. Dichos medios pueden abarcar desde la instalación de equipos que recopilan datos de los equipos terminales de las zonas seleccionadas, como los denominados receptores de IMSI (identidad internacional de abonado móvil), hasta algunos programas y técnicas que, por ejemplo, efectúan un seguimiento subrepticio de los hábitos de navegación para crear perfiles de usuarios finales».

21 COM/2017/010 final - 2017/03 (COD)

Como ejemplo de esto, es bien conocido el escándalo de *Cambridge Analytica*, una consultora política británica, que obtuvo los datos de millones de usuarios de Facebook sin su consentimiento y mediante sistemas de IA los utilizó para crear perfiles psicológicos. Estos perfiles luego se utilizaron para ofrecer anuncios políticos personalizados en la campaña presidencial americana de 2016. Este campo del perfilado proporciona información para luego proceder a enviar *nudges* que influyan en la conducta de los sujetos, concepto este del que luego nos ocuparemos.

2.3. El reconocimiento de emociones y la detección del pensamiento

Ya hemos visto que uno de los campos en los que la captación de datos biométricos es muy efectiva es el de los datos sobre frecuencia cardiaca, respiración, expresión facial, movimiento de las pupilas, temperatura corporal, cuya combinación puede indicar la presencia de determinados estados emocionales. Por ejemplo, el software de la compañía española *Decoditive* permite determinar mediante una sencilla cámara si el sujeto está haciendo trampas al ajedrez o la eficacia real de los anuncios que está contemplando[22], simplemente examinando el campo visual y movimiento de las pupilas del sujeto.

La misma *Ley de la IA* hace expresa referencia a la utilización de los datos biométricos para la labor policial en los interrogatorios, y la averiguación de la veracidad o falsedad de las declaraciones de las personas. Se está refiriendo a datos que revelan estados emocionales, tales como frecuencia cardiaca, sudoración, movimiento de las pupilas, tono de voz o incluso frecuencia y fuerza de pulsación de las teclas del ordenador. Es en concreto en el Considerando 38 en el que se expone que son de alto riesgo los sistemas de IA para la aplicación de la ley, entre los que deben incluirse «[…] en particular, los sistemas de IA que las autoridades encargadas de la aplicación de la ley utilicen para realizar evaluaciones del riesgo individuales, los polígrafos y herramientas similares, o los sistemas utilizados para detectar el estado emocional de una persona física». Y en su art. 3.34 la LIA define al «Sistema de reconocimiento de emociones» como «un sistema de IA destinado a detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos».

---

22 «El CEO de Decoditive, Joan Buch, recogió el premio en la categoría e-commerce de la Barcelona New Economy Week (BNEW 2021) de manos de la ministra Nadia Calviño». *El Español*, 21 octubre 2021, en https://www.elespanol.com/invertia/disruptores-innovadores/disruptores/startups/20211028/startup-cazaba-tramposos-ajedrez-atrapar-clientes-neuromarketing/622687953_0.html

Da cuenta Cotino Hueso (2023, p. 348) que estos sistemas permiten leer emociones, detectar la verdad de las manifestaciones, y predecir futuros comportamientos y que desde hace años se utilizan para el control de fronteras en EE. UU., con el denominado Agente Virtual Automatizado para la Evaluación de la Verdad en Tiempo Real (AVATAR - *Automated Virtual Agent for Truth Assessments in Real Time*), que analiza el comportamiento no verbal y verbal de los viajeros. En Europa, la Comisión Europea financió el proyecto *Intelligent Portable Control System (iBorderCtrl*), con herramientas de detección del engaño y de evaluación de respuestas de solicitantes de visa de entrada que generó una relativa reacción desde la sociedad civil, y que finalmente ha sido retirado. Las grandes compañías de aplicaciones informáticas han producido sistemas de reconocimiento biométrico y facial para identificar personas y detectar emociones y estados de ánimo, así en junio de 2022, Microsoft anuncia que retira sus sistemas *Azure Face.*

Y al lado de estas técnicas, tenemos la nueva rama de la neurología que es la neurotecnología, que define Moreu Carbonell (2022, p. 72) de modo muy amplio como el conjunto de métodos e instrumentos que permiten una conexión directa de dispositivos técnicos con el cerebro y el sistema nervioso, con independencia de si se trata de técnicas de estimulación cerebral invasivas o no invasivas: «La neurotecnología es un concepto interdisciplinar en el que confluyen la inteligencia artificial, la informática y las neurociencias. Las investigaciones del cerebro pueden ya medir, registrar, alterar y manipular la actividad cerebral; es lo que se conoce como neuromodulación o alteración de la actividad cerebral por medio de la introducción de estímulos». Hoy por hoy, la neurotecnología tiene un uso beneficioso para la humanidad, pero presenta riesgos jurídicos, éticos y morales, amenazando, como nos dice la autora, la privacidad y la seguridad de las personas, y la propia definición de persona. Para evitar estos males, propone la autora el desarrollo de una nueva especialidad jurídica, el *Neuroderecho*, y la conformación de nuevos neuroderechos de las personas.

La nueva tecnología supone un paso más en la invasión de la privacidad, pues ya no se trata de inferir estados emocionales a partir de datos biométricos, sino directamente de acceder a los pensamientos de la persona mediante una lectura de los patrones de estímulo eléctrico cerebral. Estamos ante la lectura de los pensamientos, cuya aplicación puede ser muy beneficiosa en medicina, como recogen Vicente Domingo y Rodríguez Cachón (2023, p. 499), refiriéndose al proyecto *Neuralink* impulsado por Elon Musk, que diseña implantes cerebrales para que los pacientes con parálisis cerebral puedan controlar dispositivos con la mente. Y también *Facebook*, hoy *Meta*, ha iniciado un programa de 40 millones de dólares

para conseguir mediante cascos de electrodos no invasivos, convertir en texto lo que está pensando una persona, sin necesidad de implantes o scanner cerebral. Mientras que desde las universidades de Singapur y Hong Kong, los investigadores Chen, Qing y Zhouy (2023) dan cuenta de la posibilidad de decodificación de las señales cerebrales en imágenes y videos.

Los neuroderechos adquieren por tanto su verdadero significado frente a esta neurotecnología inteligente, que como vemos es especialmente invasiva. Recoge Moreu Carbonell (2022, p. 83) de los investigadores Marcello Ienca y Roberto Andorno hasta cuatro neuroderechos: Derecho a la libertad cognitiva o «autodeterminación mental», una actualización del derecho a la libertad de pensamiento y de conciencia. Derecho a la privacidad mental, que protege frente a cualquier información que pueda obtenerse de nuestros cerebros por medio de neurotecnologías. Derecho a la integridad mental, contra las intrusiones en el cerebro. Y, por último, derecho a la continuidad psicológica, que garantiza la percepción de la propia identidad como seres humanos. Vicente Domingo y Rodríguez Cachón (2023, p. 513) recogen por su parte la enumeración de la *NeuroRights Foundation*, del neurólogo Rafael Yuste (derecho a la identidad e integridad personal y mental, al libre albedrío, a la privacidad mental, al acceso equitativo y a la protección contra los sesgos), y afirman que una eventual aceptación de esta propuesta de los neuroderechos como nueva categoría de Derechos Humanos llevaría aparejada una modificación de la Declaración Universal de los Derechos Humanos.

3. Las técnicas subliminales y el nudge

La *Ley de la IA* también se ocupa, para declararlas prácticas prohibidas en su artículo 5 —como ya se ha dicho—, de los sistemas de IA que utilicen «[…] técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque […] perjuicios físicos o psicológicos a esa persona o a otra». O bien sistemas que aprovechen vulnerabilidades de un grupo específico de personas, ya por edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de personas de dicho grupo.

En cuanto a estas técnicas, ha señalado Ebers (2023, p. 265) que ni el artículo 5 ni el Considerando 16 de la LIA definen qué es una «técnica subliminal», o en qué consiste alterar *sustancialmente* el comportamiento de una persona. Y además este art. 5 solo cubre las prácticas de IA que tienen la intención directa de perjudicar a otras personas. En realidad, la mayoría de estas prácticas serán

ilegales conforme al Derecho penal en la mayoría de los Estados, si lo que intentan es engañar a las personas (posiblemente para estafarlas), y además la Directiva sobre prácticas comerciales desleales (2005/29/CE) ya prohíbe las prácticas comerciales que distorsionan el comportamiento humano en determinadas condiciones. Como advierte De Miguel Asensio (2021, p. 4), todas estas técnicas están prohibidas por el art. 5 de la LIA por generar riesgos inadmisibles que contravienen los valores de la Unión europea. Sin embargo, opina el autor que además de esta normativa, el perjudicado por sistemas inteligentes puede acudir a la normativa de protección del honor, intimidad y propia imagen, a la de protección de datos personales e incluso a la de protección del consumidor y a la de responsabilidad por productos defectuosos. Por ello el autor estima que la nueva LIA viene a cubrir estos espacios desprotegidos, los daños de difícil encuadre en las figuras «normales» del daño.

¿A qué técnicas de modificación de comportamientos se puede referir la LIA? La influencia inconsciente en el comportamiento de las personas fue el tema de una famosa obra del año 1957, *The Hidden Persuaders*, de Vance Packard (traducida al español como *Las formas ocultas de la propaganda*). En este libro, dedicado a la publicidad y su influencia en los consumidores, se toma como premisa la falta de racionalidad de muchos comportamientos de consumo, y la anécdota que mejor muestra este aspecto es la siguiente:

> Un bazar cuyos dueños consideraban con creciente escepticismo la racionalidad de sus clientes puso a prueba un experimento. Uno de los renglones de menor salida era un artículo que valía catorce centavos. Cambió el precio ofreciendo dos de dichos artículos por veintinueve centavos. Las ventas aumentaron rápidamente en un 30 % al ofrecerlo a precio «rebajado» (Packard, 1992, p. 15).

Es decir, que las técnicas de marketing y publicidad no se basan en la lógica y racionalidad de la compra del producto, sino en la investigación de los motivos que realmente deciden las conductas del consumidor. Y a partir de ahí, manipulando las imágenes asociadas al producto, se intenta influir sobre las conductas de compra del consumidor: el hecho básico es que el ser humano es manipulable.

Más allá del marketing, una de las técnicas que se usa en la actualidad para influir en los comportamientos sociales es el *nudging*. Señalan Costas Pérez y Tucat (2021, p. 9) que los *nudges* o «empujones» se popularizan a partir de la publicación del libro *Nudge: Improving Decisions About Health, Wealth, and Happiness,* de Cass Thaler y Richard Sunstein, en 2009. Los *nudges* (palabra

que significa pequeños «empujones» o «codazos»; también se ha traducido como «acicates») son intervenciones que buscan modificar la toma de decisiones individuales, intentando cambiar el comportamiento de las personas en una dirección concreta, pero sin prohibir ninguna opción, ni alterar en gran medida los incentivos económicos. Es decir, que no son órdenes coercitivas para los ciudadanos, sino que inducen a un comportamiento que se considera adecuado o deseable, como señalaban Thaler y Sunstein.

Los *nudges* actúan precisamente partiendo de la posibilidad de influencia en el comportamiento humano de toma de decisiones, pues como hemos visto muchas decisiones se toman siguiendo criterios no estrictamente racionales sino emocionales. Esta técnica pasa del mundo del marketing al de la Administración pública, siendo utilizado para fomentar las conductas que resultan más beneficiosas (aunque no se concreta para quién lo son, si para la Administración o los ciudadanos)[23]. Como señalan los indicados autores, los *nudges* en las políticas públicas utilizan «los conocimientos de las ciencias económicas, la neurociencia y la psicología, para incentivar o desincentivar actuaciones concretas de los distintos agentes, y alcanzar así objetivos establecidos por los dirigentes públicos» (Costas y Tucat, 2021, p. 9).

Por su carácter no normativo, los *nudges* constituyen un importante instrumento de políticas públicas en la acción de gobierno que escapa a un control político. El ejemplo más citado es el de incluir en los documentos médicos la opción por defecto de ser donante de órganos, y estableciendo por tanto que el rechazo ha de ser expreso. Con esta modificación, el porcentaje de donantes es significativamente mayor que si la opción de ser donante se tiene que elegir expresamente. Como precisa De Zárate-Alcarazo (2023, p. 69), el *nudging* milita en el campo de lo políticamente correcto: «los *nudges* son un tipo de intervenciones que, aprovechando las limitaciones cognitivas humanas, nos ponen en el «buen camino» o

---

23 Señalan Antonio Cabrales Goitia y Pedro Rey Biel que, según el modelo de Bemelmans-Videc, las políticas públicas se clasifican como *palos, zanahorias o sermones*:

> «Los palos son herramientas reguladoras que buscan forzar el comportamiento de los ciudadanos. Las zanahorias proveen de incentivos para seducir a los individuos, mientras que los sermones, buscan persuadirles. Clasificar a los nudges en uno de estos tres grupos no es tarea sencilla. Los nudges claramente no son palos, puesto que no restringen las opciones disponibles para el individuo ni le castigan si no se comporta como el regulador pretende. Tampoco son zanahorias, puesto que buscan guiar al ciudadano de una forma inconsciente ... Por último, los nudges tampoco son sermones, pues no pretenden persuadir a los ciudadanos de forma abierta mediante la provisión de información […]. Los nudges se encuentran en un término medio entre la zanahoria y el sermón» (Cabrales Goitia y Rey Biel, 2021, p. 40).

la «buena dirección», sin consecuencias negativas para aquella persona que elige no seguir el camino recomendado». Por su carácter meramente orientador de los *nudges* hacia ciertos objetivos o metas y, simultáneamente, su respeto por la autonomía y libertad individual de las personas, al *nudging* también se le denomina paternalismo liberal (libertarian paternalism), y concluye el autor «Por tanto, los *nudges* son mecanismos coercitivos alineados con los valores de las democracias liberales» (Strabheim, 2020).

Pues bien, la unión de estas técnicas de *nudging* con la IA produce interesantes resultados. Como advierte Ortiz de Zárate-Alcarazo (2023, p. 82), la aplicación de la IA puede mejorar la implementación de *nudges* en el sector público, e incluso puede llegar a transformar este tipo de intervenciones dando lugar a lo que podríamos denominar «políticas conductuales inteligentes y, más concretamente, *intelligent nudging*. Los *nudges* inteligentes tendrían niveles de eficacia y eficiencia más elevados que los de sus hermanos no inteligentes gracias al uso de tecnologías de reconocimiento facial, detección de objetos, procesamiento del lenguaje natural, predicción, análisis en tiempo real, etc., que permitirían mejorar todos los pasos del proceso». En este sentido, el investigador de la Universidad de Seikei, Yukari Yamazaki (2020) nos anuncia la llegada del *Hypernudge*, como resultado de la unión del *nudge* y la IA, es decir, el *nudge* creado por una IA entrenada mediante *machine learning*, y advierte que las condiciones de autonomía, dignidad y transparencia, que deben regir el empleo de *nudges*, desaparecen en este caso. Con base en un estudio estadístico, concluye que hay que estar alerta en la utilización de los hypernudges por su menor aceptación que los *nudges* originales.

Desde la filosofía del derecho, señala De Asís Roig (2022, p. 33) que los *nudges* se introducen en el ámbito de las aplicaciones tecnológicas, para actuar como consejeros morales en sistemas inteligentes. Cita así los modelos computacionales *Truth-Teller* y *Sirocco,* y el programa *MeEthEx*, que es una especie de asesor ético en el campo de la medicina para ayudar a resolver dilemas éticos, y que se apoya en los principios de ética biomédica. Otros modelos se configuran como asistentes-guía en la toma de decisiones, como el modelo computacional diseñado por Robbins y Wallace, que es una herramienta para la ayuda en la toma de decisiones y en la resolución colaborativa de problemas, simulando diferentes papeles (asesor, facilitador de grupo, entrenador de interacción y pronosticador). También cita el autor la propuesta de F. Lara, de un asistente virtual para fortalecer la moralidad potenciando la autonomía personal: «Se trata de un asistente basado en el método dialéctico socrático si bien proyectado hacia el aprendizaje moral. El asistente, que denomina *SocrAI*, lo que pretende es formar al usuario no tanto en principios éticos sustantivos sino en pautas generales sobre cómo razonar

mejor» (De Asís Roig, 2022, p. 33). Coincide el autor en la peligrosidad de los *hypernudges*, por la posibilidad de manipulación que conllevan. Naturalmente, el problema de estas técnicas potenciadoras de la eficacia mediante la IA, es que también potencian los problemas del *nudging*, como son la disminución de la libertad individual, de la capacidad de decisión y elección de los ciudadanos, la manipulación y el determinismo.

En suma, a los problemas intrínsecos del *nudge* se añaden los problemas específicos derivados de la IA, especialmente los derivados de la utilización de redes neuronales, como la opacidad algorítmica, los problemas de privacidad, los sesgos, la falta de rendición de cuentas, y sobre todo el ataque a la privacidad e intimidad de las personas, derivando en un paternalismo agobiante. Por ello, Ortiz de Zárate-Alcarazo (2023, p. 85) matiza su consideración sobre estas técnicas diciendo: «En este sentido, la posible perversión de las políticas conductuales inteligentes y su principal riesgo sería el de generar escenarios en los que la ciudadanía tuviera importantes dificultades para salirse del camino establecido y quedasen fácilmente atrapados en senderos de dependencia».

Más allá del *nudge* veremos ahora una técnica de vigilancia y represión (y no modificación) de los comportamientos de los ciudadanos de consecuencias aterradoras: la calificación social.

4. La calificación social

A esta técnica, utilizada tanto para influir en el comportamiento de las personas como para controlarlo, alude el art. 5 (LIA) al prohibir los sistemas de IA utilizados por autoridades públicas o en su representación: «c) […] con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas […]»[24]. Estamos ante un sistema por el que cada persona, convenientemente identificada por técnicas biométricas —de identificación y rastreo en red o por teléfono móvil—, recibe una puntuación o créditos —positivos o negativos, según el comportamiento

[24] Sigue el precepto […] de forma que la clasificación social resultante provoque una o varias de las situaciones siguientes: i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente; ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.

calificado sea aceptable o inaceptable —, cuya suma determina su calificación o crédito social. El origen del invento está en algo que, al principio —como tantas otras cosas— pareció una buena idea, en concreto, en las calificaciones crediticias y las listas de morosos como pueden ser las españolas ASNEF, CIRBE o RAI. Pero, luego, esto se complica cuando se añaden los ingredientes de las bases de datos, las tecnologías de reconocimiento biométrico y las de seguimiento de la actividad de los teléfonos móviles, y de la mera calificación crediticia a efectos de valorar la solvencia del sujeto se pasa a valorar al sujeto en sí, a partir de todo su comportamiento.

Apunta Cotino Hueso (2022, p. 73) que estos preocupantes sistemas biométricos de categorización ni están prohibidos ni en general son de alto riesgo, sino solo sometidos al artículo 52 de la *Ley de IA: Artículo 52. Obligaciones de transparencia para determinados sistemas de IA*:

> […] 2. Los usuarios de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él. Esta obligación no se aplicará a los sistemas de IA utilizados para la categorización biométrica autorizados por la ley para fines de detección, prevención e investigación de infracciones penales.

Opina el autor que sería más adecuado que o bien se regulen como sistemas de alto riesgo o en algunos casos directamente se prohíban.

Para Ebers (2023, p. 267), hay que aclarar cuándo la calificación social tiene lugar *en representación* de las autoridades públicas, pues estas prácticas se realizan mayoritariamente por el sector privado, extendiendo sus efectos a la administración u otras autoridades públicas. Al restringir la prohibición de la calificación social a las autoridades públicas, la LIA «ignora el uso de tales sistemas por parte de entidades privadas, incluso en ámbitos de alto riesgo que podrían afectar a los derechos fundamentales de las personas»; por ejemplo, en las calificaciones crediticias.

Como todo el mundo sabe, pero intenta olvidar, es el sistema de partido único chino el máximo exponente de la implantación de los sistemas de calificación social. Como señalan Roberts, Cowls, Morley y otros (2021, p. 60), esta tecnología viene a ser sancionada por el *Plan de Desarrollo de la Inteligencia Artificial de la Nueva Generación* del Gobierno chino. Este plan tiene tres ámbitos de proyección: Desafío internacional, Desarrollo económico y Gobernabilidad o «Construcción» social, siendo este último el que más nos interesa. El Sistema de Crédito Social todavía no se ha implantado a nivel nacional, pero como nos

dicen los citados autores, los ambiciosos objetivos del mismo «[…] ofrecen un convincente ejemplo de la intención del gobierno de confiar en la tecnología digital, no solo para gobernanza social, sino también para una regulación más detallada del comportamiento» (Roberts et al, 2021, p. 66).

En definitiva, se trata del control de los comportamientos sociales, cuya implantación es un proyecto perfectamente establecido, como se deduce del documento «Esquema para el establecimiento de un sistema de crédito social» del Consejo estatal para la implantación del sistema, publicado en 2014. Este documento subrayó que el Sistema de Crédito Social no solo tenía como objetivo regular las finanzas y acciones corporativas de empresas y ciudadanos, sino el comportamiento social de los individuos, persiguiendo conductas como evasión fiscal, alarmas sobre la seguridad alimentaria y deshonestidad académica, mediante el sistema de «listas negras». Pero a ello hay que añadir otros datos, como que la ciudad de Fuzhou enriquece el currículo social de sus ciudadanos con una cifra que expresa su empleabilidad, según datos de desempeño y constancia en el trabajo, a lo cual hay que sumar el desarrollo de ciudades inteligentes, con tecnologías de vigilancia basadas en el reconocimiento facial y seguimiento de teléfonos móviles para rastrear a quienes el gobierno presenta como potenciales disidentes o terroristas, sobre todo de la etnia uigur.

Señala Cotino Hueso (2022, p. 71) que, en China, el uso de las tecnologías biométricas combina las tecnologías de identificación, categorización y reconocimiento de emociones para su famoso Sistema de Crédito Social, control policial, de la lealtad al partido o de seguimiento de atención y evaluación y control mental en el ámbito educativo. Las consecuencias pueden ser muy peligrosas para las personas, pues como señala el periodista Serrano Martínez[25], los ciudadanos pueden entrar en una lista negra con bastante facilidad, lo que tiene graves consecuencias en la vida real: «[a]cciones tan cotidianas como saltarse un semáforo, fumar en lugares prohibidos, tener deudas impagadas o cometer fraude, además de su correspondiente sanción administrativa, conlleva ciertas

25 «Crédito social chino: el sistema de puntos que ya se exporta a otras sociedades», *El Economista,* Alejandro Serrano Martínez, 17 de junio de 2023. https://www.eleconomista.es/economia/noticias/12325879/06/23/credito-social-chino-el-sistema-de-puntos-que-ya-se-exporta-a-otras-sociedades.html. Añade el autor que también Rusia quiere completar una red de reconocimiento biométrico combinando sus propios algoritmos de IA con su enorme sistema de vigilancia pública: así, en enero de 2020, Moscú implementó un nuevo sistema de reconocimiento facial en tiempo real en toda la ciudad, con más de 160 000 cámaras.

restricciones: como la prohibición de viajar en avión o en trenes de alta velocidad, y la compra de artículos de lujo. En algunas ciudades, se publicita la información de las personas morosas en pantallas LED de centros comerciales, camiones o paradas del autobús, desvelando datos personales y suponiendo un escarnio social para la persona afectada y su familia». Por si fuera poco, si el crédito social es negativo, no se podrá solicitar subvenciones, acceder a prestamos o conseguir matrícula en las mejores escuelas o universidades públicas. Desde esta perspectiva, está claro que las palabras de Cotino Hueso sobre la devastadora incidencia de esta técnica sobre los derechos fundamentales no son nada exageradas.

Para Turley (2020, p. 2185), la realidad es que el Gobierno chino está intentado abiertamente crear una sociedad-pecera, en la que ni siquiera sea necesario el control policial. Si se implanta una tecnología de reconocimiento facial completa, las personas serán reacias a asistir a protestas o manifestaciones cuando el gobierno puede determinar su identidad y tampoco tendrán contactos con personas o empresas que sean consideradas problemáticas por el gobierno, sobre todo teniendo en cuenta las consecuencias de este sistema de calificación social o «puntuación ciudadana», que puede perjudicar también a la familia (colegios, universidad). Además, gran parte de los esfuerzos del reconocimiento biométrico en China han estado dirigidos a identificar minorías, especialmente los uigures y otras etnias vistas como una amenaza para el régimen comunista.

¿Qué aceptación tiene este sistema entre la población? Pues como nos dicen los citados Roberts et al. (2021, p. 67), según una encuesta realizada en China por especialistas occidentales, se detectaron altos niveles de aprobación dentro de la población, aunque ello más por falta de conocimiento de las repercusiones del sistema que por un apoyo explícito. Lo de siempre: la gente normal no tiene nada que temer […] hasta que vienen a por ella y entonces ya no hay nada que hacer.

BIBLIOGRAFÍA

Cabrales, A. y Rey, P. (2021). Mas allá de los nudges: Políticas públicas efectivas basadas en la evidencia de las ciencias del comportamiento. *Gestión y Análisis de Políticas Públicas*, (25), 38-45. https://doi.org/10.24965/gapp.i25.10864

Chee Siong, K. (2023, 16 de junio). Police robots deployed in Singapore. ABS-CBN news. https://news.abs-cbn.com/overseas/multimedia/photo/06/16/23/singapore-deploys-more-police-robots

Chen, Z., Qing, J. y Zhou, J. H. (2024). Cinematic mindscapes: High-quality video reconstruction from brain activity. *Advances in Neural Information Processing Systems*, (36). https://doi.org/10.48550/arXiv.2305.11675

Coca Payeras, M. (2023), Las iniciativas de la Unión europea sobre inteligencia artificial: de la persona electrónica, al difícil equilibrio entre la necesidad de impulsarla y evitar sus riesgos. *Revista de Derecho Civil, vol. 10*(2). http://nreg.es/ojs/index.php/RDC

Costas, E. y Tucat, P. (2021). Nudges: diseño y evaluación. *Gestión y Análisis de Políticas Públicas*, (25), 8-22. https://doi.org/10.24965/gapp.i25.10868

Cotino, L. (2023). Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de Inteligencia artificial y protección de datos. En F. Balaguer Callejón y L. Cotino Hueso (Coord.), *Derecho Público de la inteligencia artificial* (pp.347-402). Fundación Manuel Giménez Abad.

Cotino, L. (2022). Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal. *El cronista del Estado social y democrático de derecho*, (100), 68-79.

De Asís, M. (2022). La justicia predictiva: tres posibles usos en la práctica jurídica. En F. Alonso, J. Garrido y R. Valdivia (Eds.), *Inteligencia Artificial y Filosofía del Derecho* (pp. 285-308). Ediciones Laborum.

De Asís, R. (2022). Ética, Tecnología y Derechos. En F. Alonso, J. Garrido y R. Valdivia (Eds.), *Inteligencia Artificial y Filosofía del Derecho*, (pp. 25-40). Ediciones Laborum.

De Miguel, P. (2021). Propuesta de reglamento sobre inteligencia artificial, *La Ley Unión Europea*, (92).

Ortiz de Zárate-Alcarazo, L. (2023). Las políticas conductuales inteligentes: Oportunidades y riesgos ético-políticos de la Inteligencia Artificial para el nudging. *Revista Española de Ciencia Política*, (62), 67-93. https://doi.org/10.21308/recp.62.03

Drummond, V. (2004). *Internet, privacidad y datos personales* [I. Espín Alba, Trad.]. Reus.

Ebers, M. (2023). El futuro marco jurídico europeo de la inteligencia artificial. *Revista General de Legislación y Jurisprudencia*, (2), 185-221.

Fernando Pablo, M. (2023). Construyendo la dignidad digital de la persona en el entorno digital. De los datos de tráfico, a la plaza y mercado de los servicios de comunicaciones electrónicas. En A. Rodríguez, P. Talavera y J. Domínguez (Coord.), *Desafíos éticos, jurídicos y tecnológicos del avance digital* (pp. 21-40). Iustel.

Garriga, A. (2022). Inteligencia artificial y el fenómeno de la desinformación: el papel del RGPD1 y las garantías recogidas en la propuesta de la ley de servicios digitales. En F. Llano, J. Garrido y R. Valdivia (Eds.), *Inteligencia Artificial y Filosofía del Derecho* (pp. 451-473). Ediciones Laborum.

González, M. (2022). Protección penal de los neuroderechos: el uso directo de las neurotecnologías sobre el ser humano. En F. Llano, J. Garrido y R. Valdivia (Eds.), *Inteligencia Artificial y Filosofía del Derecho* (pp. 313-335). Ediciones Laborum.

Hu, M. (2022). Biometrics and an AI Bill of Rights. *Duquesne Law Review*, (60), 283-301. https://scholarship.law.wm.edu/facpubs/2078

Juliá-Pijoan, M. (2023). Una aproximación al perfilaje criminal desde la investigación neurocientífica. En F. Bueno (Dir.) y I. González (Coord.ª), *Fodertics 11.0: derecho, entornos virtuales y tecnologías emergentes* (pp. 441-453). Comares.

Lucasiewicz, R. (2022). Facial recognition. Matching in gamete donation using AI. *Tratado de Inteligencia artificial y Derecho en el nuevo milenio* (pp. 385-401). Ediciones Olejnik.

Matefi, R. & Darius, C. (2022). Artificial intelligence and its impact on personality rights. *Tratado de Inteligencia artificial y Derecho en el nuevo milenio* (pp. 70-89). Ediciones Olejnik.

Megías, J. (2022). Derechos humanos e Inteligencia artificial. *Revista DIKAIOSYNE*, (37), 140-163.

Moreu, E. (2022). La regulación de los neuroderechos. *Revista General de Legislación y Jurisprudencia*, (1), 71-100.

Packard, V. (1992). *Las formas ocultas de la propaganda* (18.ª ed.). Editorial Sudamericana.

Pollicino, O. y De Gregorio, G. (2021). Constitutional Law in the Algorithmic Society. *Constitutional Challenges in the Algorithmic Society.* Cambridge University Press, pp. 3-24. https://doi.org/10.1017/9781108914857.002

Pollicino, O. & Paolucci, F. (2022). Digital constitutionalism to the test of the smart identity. *Journal of E-Learning and Knowledge Society, 18*(3), 8-21. https://doi.org/10.20368/1971-8829/113581

Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V & Floridi, L. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Soc.* (36), 59-77. https://doi.org/10.1007/s00146-020-00992-2

Salvi, N. & Nigri, S. (2022). Minority Report: the Road to a Deterministic Theory for the Philosophy of Criminal Law, *Opinión Jurídica*, 21(46), 1-18. https://doi.org/10.22395/ojum.v21n46a2

Solar Cayón, J. (2022). Inteligencia artificial y justicia digital. En F. Llano, J. Garrido y R. Valdivia (Eds.) *Inteligencia Artificial y Filosofía del Derecho* (pp. 381-425). Ediciones Laborum.

Turley, J. (2020). Anonymity, Obscurity and Technology: Reconsidering Privacy in the Age of Biometrics, *Boston University Law Review*, (100), 2179-2261. https://www.bu.edu/bulawreview/files/2021/01/TURLEY.pdf

Vicente Domingo, E. & Rodríguez Cachón, T. (2023). Derecho de la Persona, Neurodatos y Neuroderechos: A Research Agenda. *Revista General de Legislación y Jurisprudencia*, (3), 495-526.

Yamazaki, Y. (2020). An Empirical Study for The Acceptance of Original Nudges and Hypernudges. En M. Arias, J. Pelegrín, K. Murata, A. Lara Palma (Eds.), *Societal Challenges in the Smart Society*, 323-336. https://dialnet.unirioja.es/servlet/artículo?codigo=7867256