IUS ET SCIENTIA
2022 • Vol. 8 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2022


# *Big brother* ¿Ciencia ficción o realidad?*

## *BIG BROTHER*, SCIENCE FICTION OR REALITY?

**María Dolores García Sánchez**
Universidad de Sevilla
mgarcia8@us.es 0000-0002-1074-7509

Recibido: 08 de diciembre de 2021 | Aceptado: 12 de marzo de 2022

"No creo que la sociedad que he descrito en1984 necesariamente llegue a ser una realidad, pero sí creo que puede llegar a existir algo parecido".
George Orwell

**RESUMEN**

En un mundo globalizado y generador de multitud de datos e información, la hipervigilancia constituye uno de sus rasgos caracterizadores.
En el presente estudio, examinaremos este fenómeno del Big Brother contraponiendo el sistema de crédito social existente en China con la regulación que, en materia de una potencial vigilancia masiva de la población, podemos encontrar en Europa, en aras de aumentar la seguridad ciudadana frente a las nuevas amenazas mundiales. Dos modelos sociales diferentes que, no obstante, evidencian una estremecedora realidad: seamos conscientes de ello o no y, a pesar de los límites establecidos en torno a esta cuestión y a una mayor conciencia de su peligro para los derechos fundamentales en el entorno europeo, no estamos exentos de esta hipervigilancia. En este sentido, la importación de los derechos fundamentales a la esfera digital resulta imperante para evitar convertir nuestros Estados de Derecho en Estados policiales.

**PALABRAS CLAVE**

Inteligencia Artificial
Big data
Vigilancia masiva
Protección de datos
Derechos fundamentales
Seguridad nacional
Puntuación social
Sistemas de identificación biométrica remota

**ABSTRACT**

In a globalized world that generates a multitude of data and information, hypervigilance constitutes one of its characterizing features.
In this study, we will examine this Big Brother phenomenon by contrasting the existing social credit system in China with the regulation that, in terms of potential mass surveillance of the population, can be found in Europe, in order to increase citizen security facing the new global threats. Two different social models that, however, show a shocking reality: whether we are aware of it or not and, despite the limits established around this issue and a greater awareness of its danger for fundamental rights in the European environment,

**KEYWORDS**

Artificial Intelligence
Big data
Mass surveillance
Data protection
Fundamental rights
National security
Social score
Remote biometric identification systems

* El presente estudio se enmarca en el Proyecto de Investigación "Biomedicina, Inteligencia Artificial, Robótica y Derecho: los Retos del Jurista en la Era Digital" (PID2019-108155RB-I00).

we are not exempt from this hypervigilance. In this sense, the importation of fundamental rights into the digital sphere is imperative to avoid turning our rule of law into a police state.

## I. PALABRAS PREVIAS

Los relatos de ciencia ficción distópica no se encuentran tan alejados de la realidad.

Mundialmente conocida es la novela de George Orwell *1984*: un mundo absolutamente controlado por pantallas, carente de libertades y derechos, en el que un gobernante tirano –*Big Brother*– es capaz de ver, escuchar y manipular a los ciudadanos. En un alarde de visión profética, este autor nos acercó ya en 1949 lo que ha dejado de ser un "futuro lejano".

Hoy en día, los avances en *big data* e inteligencia artificial (en adelante IA) dotada de *machine learning* posibilitan la presencia de este Gran Hermano.

En efecto, la información y los datos disponibles a nivel mundial han crecido de manera exponencial en los últimos años como resultado de la globalización y la aparición de Internet. Los mismos pueden proceder de múltiples fuentes, tales como la infinidad de actuaciones online que realizamos cada día (mandar un email, dar *like* a un comentario en Facebook o a una serie en Netflix, hacer *click* en un enlace, la reserva de un billete de avión…), los datos biométricos proporcionados por sensores de huellas dactilares, sistemas de reconocimiento facial o de voz, pulsómetros, etc.



El *big data* y la IA, posibilitan el almacenamiento y análisis masivo de dichos elementos y permiten extraer conclusiones con una base más sólida, así como una toma de decisiones más efectiva al tener en cuenta un mayor número de variables, en comparación con los tradicionales instrumentos de almacenamiento de información.

Los sistemas dotados de este tipo de tecnología, además, forman parte de nuestro entorno cotidiano y nos reportan numerosos beneficios, haciéndonos la vida más fácil (como en el caso de los asistentes digitales o aparatos destinados a la limpieza del hogar). Todo ello sin olvidar sus grandes ventajas en el plano industrial (a modo de ejemplo, los vehículos sin conductor), sanitario (tales como el almacenamiento de datos clínicos para la detección precoz de enfermedades) e incluso de defensa, para la preservación de la seguridad nacional mediante la implantación de cámaras de videovigilancia dotadas de reconocimiento facial o la cesión de datos entre los proveedores de servicio.

No obstante lo anterior, no podemos perder de vista que la IA y el *big data* –como el dios griego Jano– tienen dos caras, y sus evidentes utilidades no pueden hacernos perder de vista los riesgos que también plantea su uso.

Precisamente por la cantidad de datos manejada por este tipo de sistemas, de entre ellos, sobresale especialmente el potencial peligro de hipervigilancia masiva de la población, esto es, de una cesión –generalmente involuntaria e inconsciente– de innumerables datos relativos a nuestra esfera privada.

Y, si a estos sistemas dotados de *big data* y *machine learning* le añadimos un canal de transmisión de la información tan instantáneo y de espectro global como lo es la Red,

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

nos encontramos ante el caldo de cultivo perfecto para la aparición de este gobernante tirano tecnológico vaticinado por Orwell, si no se le hace frente con un adecuado marco regulatorio en el que los derechos fundamentales sean los claros protagonistas.

En concreto, es en China donde el *Big Brother* ha alcanzado (hasta la fecha), su máximo exponente.

## II. EL SISTEMA DE CRÉDITO SOCIAL CHINO

Imagina ir caminando por la calle con prisas. Llegas a un paso de cebra con el semáforo rojo, pero no se aprecian coches a la vista y cruzas. ¿Quién no se ha visto en esa misma situación?

Pues, si ello te ocurre en China es posible que aprecies tu foto algunos días más tarde, así como tu nombre y número de identificación gubernamental, en una enorme pantalla en el paso de peatones que cruzaste cuando no estaba en verde.

El número ingente de cámaras de seguridad repartidas por todo el país juntos con los sistemas de reconocimiento facial, IA y *big data* nutren lo que se conoce como "sistema de crédito social" y posibilita esta y otras escenas salidas de un episodio de Black Mirror.

### 1. ¿Qué es el sistema de crédito social?

Con base en el "Proyecto de planificación para el desarrollo de un sistema de crédito social (2014-2020)"[1], aprobado el 14 de junio de 2014 por el Consejo de Estado Chino, se trata de un sistema digital de control, registro y puntuación basado en datos que clasifica y evalúa a individuos[2], funcionarios, empresas, organizaciones y asociaciones, penalizando y sancionando el mal comportamiento, por un lado, y por otro, concediendo ciertas ventajas a quienes se comportan de manera ejemplar.[3]

En este punto, resulta importante señalar que el sistema de crédito social sigue siendo una extensión del sistema legal y administrativo existente bajo el control del partido del Estado. En consecuencia, la limitación oficial a la "aplicación de las leyes" no evita la extralimitación ni las violaciones de los derechos humanos, pues no debemos perder de vista que nos encontramos ante un Estado autoritario y de control en el que la censura se halla a la orden del día.



1. Consejo de Estado Chino, (2014), Planning Outline for the Construction of a Social Credit System (2014-2020). Recuperado el 3 de noviembre de 2021 de https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/

2. Como se desprende de la definición apuntada, el sistema de crédito social califica no solo a los individuos, si no también a las empresas. Sin embargo, en el presente estudio nos centraremos en sus efectos para los ciudadanos, dejando al margen a las compañías.

3. Digital Guide IONOS, (2021), *Sistema de crédito social chino: una puntuación con muchas consecuencias*. Recuperado el 3 de noviembre de 2021 de: https://www.ionos.es/digitalguide/online-marketing/analisis-web/que-es-el-sistema-de-credito-social-chino/

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

Las bases de datos se encuentran administradas por la Comisión Nacional de Desarrollo y Reforma (NDRC), el Banco Popular de China y el sistema judicial del país (Lee, 2020).

Actualmente, continúa siendo un proyecto piloto con vistas a su introducción en todo el territorio, la cual, si bien estaba prevista para 2020, se ha visto retrasada. En enero de 2021, el Comité Central del Partido Comunista chino emitió una nueva hoja de ruta para la "construcción de una sociedad del Estado de derecho" hasta 2025. La misma, incluye una sección sobre el sistema de crédito social, en la que se destaca su importancia para la agenda del desarrollo legal en China en tanto que pilar de apoyo del sistema legal (Drinhausen y Brussee, 2021).

## 2. Funcionamiento

Dado que el Gobierno Chino se encuentra todavía implantando el sistema en el país y no lo presenta de manera homogénea, existen hoy en día, versiones diferentes en cuanto a su estructura. Asimismo, tampoco hay claridad respecto a la forma en que se ponderarán los factores de evaluación en el sistema de puntuación nacional, cómo o quién anota estas calificaciones, de qué manera se pueden verificar, o si cada infracción tendrá un impacto negativo inmediato.[4]-.

El objetivo, eventualmente, es que el sistema lo sea a nivel nacional y que los ciudadanos cuenten con un número de identidad que les vincule a un registro permanente.

Aun cuando no se ha confirmado oficialmente por las autoridades chinas, en base a los proyectos precursores, se estima que, a modo de carné por puntos, todos los ciudadanos partirían con una puntuación base –determinada después de recopilar, agregar y analizar datos de diferentes fuentes– que pueden ganar o perder en función de su comportamiento cívico, pudiendo ser incluidos en listas negras –una práctica que, dicho sea de paso, resulta muy habitual en el país-.

Si su conducta resulta positiva –es decir, ajustada a lo establecido por el Gobierno–, se suman puntos. Por el contrario, cualquier actitud negativa, les haría perderlos, derivándose de este aumento o reducción de puntos, una serie de beneficios o perjuicios.

A modo de ejemplo, entre tales beneficios podrían encontrarse el conseguir acceso a préstamos o a servicios públicos como la educación o privilegios para viajar. Como contrapartida, las personas con un bajo crédito social pueden tener prohibido adquirir billetes de tren o avión durante al menos un año, incluso si necesitan salir del país por alguna emergencia o razones laborales.

La mayoría de las fuentes de datos se recopilan de fuentes tradicionales, como registros financieros, penales y gubernamentales, así como de datos existentes de las oficinas de registro junto con fuentes de terceros, como las plataformas de crédito en línea. Y, actualmente, el gobierno chino se encuentra experimentando con la recopilación de datos a través de videovigilancia y transferencias en tiempo real.

4. Ibídem



IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

En concreto, entre los más importantes factores de evaluación de los ciudadanos se encontrarían los antecedentes penales, su comportamiento en el transporte público, su solvencia y su actuación como consumidores tanto en el mundo físico como en la red –por ejemplo, la realización de compras frívolas– e, incluso, los hábitos alimenticios y las evaluaciones de los superiores o arrendatarios.

No obstante, debe reiterarse que, por ahora, el sistema aún se encuentra en desarrollo y está relativamente fragmentado en lo que respecta al intercambio de datos entre diferentes bases de datos. Es decir, hoy en día no se trata de un sistema unificado y estandarizado, pues, aunque las bases del sistema de crédito social son iguales a nivel nacional, existen varios modelos locales para su implementación –en concreto, los datos apuntan a la existencia de 28 modelos–, lo cual se refleja en diferencias significativas en su efectiva instauración. La creación de vías de intercambio de datos horizontales y verticales continúa obstaculizada por las diferencias regionales e institucionales en los datos recopilados y la falta de estándares unificados y almacenamiento centralizado.

En otras palabras, la implementación fragmentada y los estándares inconsistentes obstaculizan la integración interregional. Y esta fragmentación constituye, asimismo, un riesgo añadido para aquellos afectados por este sistema, pues, ante dicho contexto descentralizado, el aumento en las cantidades de datos implica un mayor riesgo de fuga de estos y abuso de información (Drinhausen y Brussee, 2021).

Mejorar estos aspectos se ha convertido en una prioridad para el gobierno chino en los años venideros.

Pero quizás, el hecho de que aún se encuentre en ciernes no es relevante pues, en la mayoría de las ocasiones, la percepción de la vigilancia es suficiente para persuadir a la población. El sentirse vigilados (aunque no lo sean efectivamente), supone *de facto* una coartación de la libertad individual, pues ello les conduce a actuar como si lo estuvieran.



## 3. Objetivo de este sistema

El Gobierno de China plantea este sistema de crédito social como una medida para fomentar la armonía y permitir acabar con abusos de individuos y empresas, midiendo el comportamiento social y la confiabilidad (Martí, 2020).

En concreto, conforme al Proyecto de planificación social, se pretende lograr avances claros en la construcción de la sinceridad en los asuntos gubernamentales, en materia comercial y en la credibilidad judicial, así como un aumento sustancial en los niveles de satisfacción social y en el mercado. Asimismo, se pretende el fortalecimiento del sentido de la sinceridad en toda la sociedad, logrando una clara mejora en el entorno crediticio para el desarrollo económico y social.

La razón de ser de este sistema descansaría en la promoción de un comportamiento socialmente ejemplar que implique una responsabilidad personal preventiva que elimine los comportamientos negativos.

Ante esta afirmación, la siguiente pregunta viene de suyo: ¿qué es un comportamiento socialmente ejemplar? La respuesta es simple: el gubernamentalmente deseado, pues no debemos perder de vista el contexto político del país analizado.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

Con este comportamiento gubernamentalmente deseado se aspira a aumentar la transparencia y seguridad ciudadana, empleando para ello la digitalización generalizada. Es decir, la seguridad se alza como justificación para injerir sin apenas límites en prácticamente todos los ámbitos de la vida de los ciudadanos.

Así las cosas, este sistema sirve también como herramienta del gobierno para imponer un control en casi todos los aspectos de la vida de los ciudadanos.

## 4. Elementos que posibilitan la vigilancia masiva y percepción ciudadana

Como ya adelantamos, este escenario se posibilita gracias al *big data* y al abundante número de cámaras de vigilancia con sistemas de reconocimiento facial.

Sin embargo, a lo anterior, debe añadirse la monitorización en la Red y la falta de restricciones en el intercambio de datos entre los proveedores de Internet y de telefonía y las autoridades, sin que exista prácticamente protección de datos.

En efecto, como apuntamos *ut supra*, el sistema de crédito social se incardina dentro del Estado de vigilancia ya existente en China, donde los gigantes tecnológicos juegan un papel esencial. De esta forma, de la estrecha relación entre las autoridades estatales y las empresas tecnológicas se ha derivado un aumento significativo en el monitoreo en línea y la cobertura de vigilancia con cámaras en casi todo el país, así como en las pruebas con IA y análisis de *big data*, con preeminencia en el sector de la seguridad pública urbana (Drinhausen y Brussee, 2021).

En especial, en la lucha contra la pandemia de la COVID-19, el gobierno chino ha mostrado con orgullo los beneficios del monitoreo integral con cámaras *Safe City*. En este sentido, la crisis sanitaria ha puesto de manifiesto la estrecha cooperación e intercambio de información entre el gobierno y las empresas privadas en el ámbito de la seguridad pública.



En definitiva, se trata de un sistema intrínsecamente orweliano dado el rastreo de comportamiento que lleva a cabo sobre las personas que, además es inexacto pues, otorga a los ciudadanos una calificación de credibilidad basada en datos que resulta incompleta en la mayoría de los casos como consecuencia de un rastreo incorrecto o el hecho de que los registros son difundidos entre muchas empresas sin llegar a consolidarse (Lee, 2020).

Nos encontramos ante el patente ejemplo de cómo la laxitud en la regulación en torno a la protección de datos y a la recopilación de información de manera indiscriminada y generalizada, así como la falta de límites en su cesión, puede conducir a una sociedad hipervigilada con ciudadanos transparentes en la que los derechos fundamentales queden desnaturalizados en segundo plano.

Sin embargo, en contra de lo que pueda parecer, lo cierto es que este tipo de sistemas goza de una visión favorable por gran parte de la población china (Marr, 2019)[5], que percibe los cambios como una manera más efectiva y eficiente de promover el buen comportamiento de los ciudadanos y protegerles del fraude y la corrupción. Evidentemente,

5. En concreto, una encuesta realizada en 2018 muestra una aprobación de un 80 % por parte de la población china.

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

aquellos con acceso a beneficios sociales por disponer de una mayor puntuación responden de manera más favorable a este sistema.

La población china es consciente de que el gobierno dispone de mucha información sobre ellos y que se encuentran vigilados en múltiples áreas de su vida privada, así que un sistema que digitaliza y comparte dicha información no es tan disonante para ellos como puede serlo para los americanos o los europeos.

## III. LA HIPERVIGILANCIA EN EUROPA Y EN EL CONTEXTO DE LA UNIÓN

En contraposición al contexto chino y a la normalización –y exaltación orgullosa– de este control activo de la población, tenemos el escenario europeo. En el mismo, la cuestión relativa a la vigilancia masiva de la población y su encaje con el derecho a la seguridad nacional y las libertades y derechos ciudadanos continúa siendo una cuestión difícil de abordar y muy debatida por el foro.

### 1. La propuesta de Reglamento Europeo sobre IA[6]

En el marco de la UE, se ha dado recientemente un importante paso al frente, abordando una propuesta de regulación de la IA[7] en aras de atender a los potenciales peligros



6. 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, de 21 de abril de 2021, {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final} https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

De conformidad con el art. 1 de la propuesta, el objeto de la misma se concreta en el establecimiento de normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión; prohibiciones de determinadas prácticas de IA; requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas; normas armonizadas de transparencia aplicables a los sistemas de IA destinados a interactuar con personas físicas, los sistemas de reconocimiento de emociones y los sistemas de categorización biométrica, así como los sistemas de IA usados para generar o manipular imágenes, archivos de audio o videos; normas sobre el control y la vigilancia del mercado.

Por su parte, en atención al art. 2 de la propuesta, el Reglamento resultaría aplicable a los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la Unión, con independencia de si dichos proveedores están establecidos en la UE o en un tercer país; los usuarios de sistemas de IA que se encuentren en la Unión; los proveedores y los usuarios de los sistemas de IA que se encuentren en un tercer país, cuando la información de salida generada por el sistema se utilice en la Unión.

Sin embargo, el Reglamento no resultaría aplicable a los sistemas de IA desarrollados o utilizados exclusivamente con fines militares, ni tampoco a las autoridades públicas de terceros países ni a las organizaciones internacionales que entren dentro del ámbito de aplicación del Reglamento cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de acuerdos internacionales con fines de aplicación de la ley y cooperación judicial con la UE o con uno o varios Estados Miembros.

7. En su art. 3 se define el "sistema de IA" como el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el Anexo I y que puede, para un conjunto determinado

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

que su uso puede llegar a plantear: la Propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas armonizadas en materia de IA, de 21 de abril de 2021.

En ella, se concretan una serie de disposiciones para el desarrollo, la introducción en el mercado y la utilización de los sistemas de IA en la UE a partir de un enfoque proporcionado basado en el concepto de "riesgo". En este sentido, se distinguirá entre los usos de la IA que generan: i) un riesgo inaceptable, ii) un riesgo alto, y iii) un riesgo bajo o mínimo.

En esta línea, se establece una sólida metodología de gestión de riesgos con el objeto de definir los sistemas de IA que plantean un "alto riesgo" para la salud y los derechos fundamentales de la persona, los cuales habrán de cumplir una serie de requisitos horizontales –sin limitación a sectores concretos– obligatorios para garantizar su fiabilidad y ser sometidos a procedimientos de evaluación de la conformidad. Igualmente, se imponen obligaciones previsibles, proporcionadas y claras a los proveedores y usuarios de dichos sistemas y, particularmente, cuando se utilizan robots conversacionales o ultrafalsificaciones, solo se establecen obligaciones mínimas en materia de transparencia. Todo ello, a los efectos de garantizar un elevado nivel de protección para los derechos consagrados en la Carta de Derechos Fundamentales de la Unión Europea (CDFUE).

Por su parte, en el caso de los usos de IA que suponen un riesgo inaceptable por ser contrario a los valores de la Unión como, por ejemplo, las que vulneran derechos fundamentales, la propuesta de Reglamento opta directamente por su prohibición.

Entre ellas encontraríamos, entre otras, el veto a las autoridades públicas para que realicen una calificación social basada en la IA, así como el uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de aplicación de la ley –salvo contadas excepciones que posteriormente referiremos–.

Ambos elementos –sistemas de puntuación o calificación social y los sistemas de vigilancia biométrica remota– suponen un potencial riesgo de vigilancia masiva para la ciudadanía europea (tal y como hemos tenido ocasión de examinar en el supuesto de China).



## A. Sistemas de puntuación o calificación social

Hemos de comenzar el análisis dispensado a tales sistemas con una aproximación a su concepto.

---

de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en el entorno con el que interactúa. Se trata de un concepto que, si bien ofrece seguridad jurídica, proporciona la flexibilidad necesaria para amoldarse al desarrollo de la ciencia, pues, el anexo al cual se remite –en tanto que lista de técnicas y estrategias para el desarrollo de la IA–, puede ser modificado por la Comisión en virtud de actos delegados a los efectos de adaptarlo a la evolución del mercado y a los avances tecnológicos, sobre la base de características que sean similares a las técnicas y estrategias incluidas. Con ello se trata de adoptar una definición única de IA que resista el paso del tiempo y lo más tecnológicamente neutra posible, aportando, al mismo tiempo, la seguridad jurídica necesaria.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

Comoquiera que existe un apartado concreto relativo a la definición de los términos empleados en la propuesta de Reglamento, lo primero que apreciamos es la carencia de una delimitación conceptual de este tipo de instrumentos. Ello resulta relevante por cuanto que conforma uno de los usos prohibidos de los sistemas de IA y, por tanto, la falta de precisión descriptiva redunda en una merma de la seguridad jurídica.

A pesar de que, como acabamos de indicar, no existe una definición específica de este tipo de sistemas de IA que proporcionan una puntuación o calificación social, una referencia más detallada al respecto puede encontrarse en el Considerando 17 de la propuesta de Reglamento. Junto con lo establecido en el art. 5 de la misma –que lo concibe como una práctica excluida– tales sistemas podrían ser definidos como aquellos que evalúan o clasifican la fiabilidad de las personas físicas en atención a su comportamiento social en múltiples contextos – como por ejemplo su actividad en las redes sociales– o de características personales o de su personalidad conocidas o predichas. Además, la calificación social resultante debe desencadenar una o varias de las situaciones siguientes: un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros en contextos sociales que no guarden relación con aquellos donde se generaron o recabaron los datos originalmente, o que resulte injustificado o desproporcionado con respecto a su comportamiento social o a la gravedad de este.

En efecto, esta clase de sistemas que proporcionan calificaciones sociales de personas físicas para su uso con fines generales por parte de las autoridades públicas (o en representación de estas) pueden tener resultados discriminatorios y abocar a la exclusión a determinados grupos. De esta manera, podrían ser menoscabados el derecho a la intimidad y a la no discriminación, así como los valores de igualdad y justicia.



### *a. Cuestiones controvertidas*

De lo hasta ahora comentado nos asaltan dos cuestiones:

- Por un lado, se alude a esta prohibición en el caso de las "autoridades públicas", dejando al margen el uso que de tales sistemas de puntuación pudiesen hacer los entes privados –que, aun no estando prohibidos, tendrían la consideración de alto riesgo–. En consecuencia, cabría la posibilidad de que las autoridades públicas tuviesen acceso a la puntuación social elaborada por tales empresas privadas, y nada se dice respecto a la prohibición de uso de tales datos de calificación obtenidos por otras fuentes que sí empleen tales sistemas de IA.[8]
- Por otro lado, como se infiere del propio art. 5, la propuesta prohíbe que las autoridades realicen una calificación social basada en IA con fines generales, pero ¿qué ocurriría si concurriera un fin específico, en apariencia legítimo, como por ejemplo aumentar la seguridad ciudadana?

8. Conforme a lo previsto en el art. 5, la prohibición se limita a "la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA" (sin aludir a la prohibición de uso de datos de calificación social ya obtenidos por otras fuentes), por parte de las autoridades públicas o en su representación.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

Si bien se guarda silencio sobre este punto, entendemos que la respuesta que se impone es la prohibición de su uso en todo caso. Y ello por dos razones: la primera por el hecho de que, si el legislador europeo hubiese querido habilitarlo en determinados supuestos legítimos, habría señalado expresamente tales excepciones –como ocurre en el caso de los sistemas de vigilancia biométrica remota y que después abordaremos–. Y, en segundo lugar, porque nos encontramos ante una utilización de estos sistemas de IA que, como hemos visto, pueden atentar contra el derecho a la intimidad y a la no discriminación, los cuales, en tanto que derechos fundamentales, únicamente pueden ser objeto de una limitación expresa, que debe derivar de la propia norma que los declara y regula. En efecto, como se establece en el art. 52 de la CDFUE[9], "Cualquier limitación del ejercicio de derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Solo podrán introducirse limitaciones, respetando el principio de proporcionalidad cuando sean necesarias y respondan efectivamente a criterios de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás".

En consecuencia, dado que no se establece en la norma reguladora finalidad específica alguna para el empleo de sistemas de IA que proporcionan una puntuación social en aras de admitir excepcionalmente su uso y, en tanto que instrumento potencialmente limitador de derechos fundamentales –intimidad y no discriminación–, entendemos que la prohibición para las autoridades públicas es absoluta.

## B. Sistemas de identificación biométrica remota



A diferencia del instrumento anterior del que no se proporcionaba una definición específica, en este caso, encontramos una detallada conceptualización en el art. 3 de la propuesta de Reglamento, con varias definiciones relacionadas con este tipo de instrumentos.

De esta manera, los "sistemas de identificación biométrica remota" se conciben como aquellos sistemas de IA destinados 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 de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada. Todo ello con independencia de la tecnología, los procesos o los tipos de datos biométricos[10] concretos que se usen.[11] Este matiz

9. Carta de Derechos Fundamentales de la Unión Europea, de 30 de marzo de 2010, (2010/C 83/02) https://www.europarl.europa.eu/charter/pdf/text_es.pdf

10. Por su parte, los "datos biométricos" se definen como aquellos 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 conformen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

11. Respecto de este tipo de sistemas de vigilancia biométrica masiva y, desde una perspectiva ética general, cabe hacer referencia a lo previsto en el art. 12 de la propuesta de *Reglamento del Parlamento Europeo y del Consejo sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas* conforme al cual, "el uso y la recogida de

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

en torno al desconocimiento previo sobre si la persona en cuestión se halla en la base de datos resulta acorde con las normas de la UE sobre protección de datos, que prohíben, en principio, el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física, excepto en situaciones específicas (art. 9 del Reglamento General de Protección de Datos[12]).

A la vista de lo anterior, no puede obviarse que el peligro del uso indebido de tales sistemas se concreta fundamentalmente en el riesgo de una vigilancia masiva para la ciudadanía, con un grave riesgo para los derechos fundamentales (aunque con distinto grado de incidencia en función del tipo de sistema de identificación biométrica masiva, como veremos).

## *a. Tipos de sistemas de identificación biométrica remota*

El art. 3 de la propuesta de Reglamento lleva a cabo, además, una definición por separado de los sistemas de identificación biométrica remota "en tiempo real" o "en diferido", lo cual resulta relevante puesto que presentan características distintas, se utilizan de manera diferente y entrañan riesgos diversos.

En este sentido, el sistema de identificación biométrica remota "en tiempo real" se trataría de aquel en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Dicho término englobaría no únicamente la identificación instantánea, sino también demoras mínimas limitadas, a



datos biométricos con fines de identificación remota en zonas públicas, como el reconocimiento biométrico o facial, entraña riesgos específicos para los derechos fundamentales, por lo que solo serán desplegados o utilizados por las autoridades públicas de los Estados miembros para fines de interés público esencial. Dichas autoridades velarán por que dicho despliegue o uso se haga público, sea proporcionado y específico, se restrinja a unos objetivos y una ubicación concretos y esté limitado en el tiempo, de conformidad con el Derecho de la Unión y nacional, en particular el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE, y teniendo debidamente en cuenta la dignidad y la autonomía humanas y los derechos fundamentales establecidos en la Carta, en particular, el derecho al respeto de la intimidad y a la protección de los datos personales". Por su parte, el Considerando 38 de la propuesta mencionada pondrá de relieve que cuando las autoridades públicas utilicen estas tecnologías por razones de interés público esencial, esto es, para garantizar la seguridad de las personas y hacer frente a situaciones de emergencia nacional, y no para garantizar la seguridad de los bienes, dicho uso deberá siempre hacerse público, ser proporcionado, específico, restringirse a objetivos concretos y estar limitado en el tiempo. Además, deberá tener debidamente en cuenta la autonomía y dignidad humanas y los derechos fundamentales establecidos en la Carta. Igualmente, dichos criterios y límites habrían de estar sujetos a tutela judicial y sometidos a control y un debate democrático con participación de la sociedad civil. *Vid*., Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas; propuesta de Reglamento del Parlamento Europeo y del Consejo sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas (Anexo), de 20 de octubre de 2020 , https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html#title2

12. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo 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), de 27 de abril de 2016, https://www.boe.es/doue/2016/119/L00001-00088.pdf

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

fin de evitar la elusión de las normas aplicables –más restrictivas que para los casos "en diferido"– mediante la generación de demoras mínimas. Estos sistemas implican el uso de material "en directo" o "casi en directo" tales como grabaciones de video generadas por una cámara u otros dispositivos con funciones similares (Considerando 8 de la propuesta de Reglamento).

Por su parte, tal sistema "en diferido" se define de manera negativa con respecto al anterior. Es decir, se considera "en diferido" todo sistema de identificación biométrica remota que no sea en tiempo real y en el que, por tanto, se produciría una demora relevante entre la recogida de datos, su comparación y la posterior identificación. En este caso, se utilizan materiales como imágenes o grabaciones de video captadas por cámaras de televisión en circuito cerrado o dispositivos privados que se han generado con anterioridad a la aplicación del sistema a las personas físicas en cuestión (Considerando 8 de la propuesta de Reglamento).

Los sistemas de IA destinados a la identificación biométrica remota de las personas físicas pueden dar lugar a resultados sesgados y tener consecuencias discriminatorias, lo cual es especialmente relevante en lo que respecta a la etnia, el sexo o la discapacidad. Por esta razón, ha de considerarse que estos sistemas, tanto "en tiempo real" como "en diferido" conllevan un alto riesgo y como tal se califican en todo caso en el Anexo III de la propuesta[13].

No obstante la consideración de sistemas de alto riesgo tanto en el caso de la identificación biométrica remota "en tiempo real" como "en diferido", se estima que el uso de sistemas de IA para la identificación biométrica remota "en tiempo real" de personas físicas en espacios de acceso público con fines de la aplicación de la ley invade especialmente los derechos y las libertades de las personas afectadas, en la medida en que puede inferir en la vida privada de gran parte de la población, provocar la sensación de encontrarse bajo vigilancia constante y disuadir indirectamente a los ciudadanos de ejercer la libertad de reunión y otros derechos fundamentales. Por añadidura, la inmediatez de las consecuencias y las escasas oportunidades para llevar a cabo comprobaciones o correcciones adicionales en relación con el uso de sistemas que operan en tiempo real –o casi–, acrecienta el riesgo para los derechos y libertades de las personas afectadas.

En consecuencia, la propuesta de Reglamento clasifica este tipo de sistemas de identificación biométrica remota "en tiempo real" con fines de aplicación de la ley como uno de los usos prohibidos de la IA en su art. 5, si bien, excepciona tres situaciones que aparecen enumeradas de manera limitativa y definidas taxativamente. En ellas, su utilización deviene estrictamente necesaria para lograr un interés público esencial cuya importancia es superior a los riesgos. Tales situaciones se concretan en la búsqueda de

13. En este mismo sentido, se pronunciaba el Libro Blanco sobre la IA al establecer que "el uso de aplicaciones de IA para la identificación biométrica remota y otras tecnologías de vigilancia intrusiva deben considerarse siempre de riesgo elevado (…). *Vid*., Libro Blanco sobre la inteligencia artificial-un enfoque europeo orientado a la excelencia y la confianza, de 19 de febrero de 2020, COM (2020) 65 final, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf



IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

posibles víctimas de delito, incluidos los menores desaparecidos; determinadas amenazas para la vida, la seguridad de las personas físicas o amenazas de atentado terrorista; la detención, la localización, la identificación o el enjuiciamiento de los autores o sospechosos de los delitos mencionados en la Decisión Marco 2002/584/JAI del Consejo de 13 de junio de 2002 relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros[14], siempre que la normativa del Estado miembro implicado determine una pena o medida de seguridad privativa de libertad cuya duración máxima sea de al menos 3 años, tal y como se defina en el Derecho de dicho Estado miembro.[15]

En resumen: en la actualidad existen dos tipos de sistemas de identificación biométrica remota ("en tiempo real" y "en diferido"), teniendo la consideración de "alto riesgo" todos sus usos permitidos, esto es, los sistemas de identificación biométrica remota "en diferido" y las excepciones legalmente contempladas en el caso de la identificación biométrica "en tiempo real". Sin embargo, no debe perderse de vista la aludida especial afectación de los derechos y libertades de las personas físicas en el caso de los sistemas de identificación biométrica "en tiempo real" frente a aquellos "en diferido" –no obstante, la misma clasificación como sistemas de alto riesgo–, pues ello, no solo determina que los usos no incluidos en las excepciones legalmente contempladas sean considerados como prohibidos, sino también la sujeción de los permitidos a concretos requisitos.

### *b. Requisitos para el uso de los sistemas de identificación biométrica "en tiempo real"*



Para velar por que estos sistemas "en tiempo real" se empleen de manera responsable y proporcionada, en estas situaciones limitadas y detalladamente definidas, deben tenerse presente ciertos aspectos.

Estos se concretan en la naturaleza de la situación que dé lugar al posible uso y, en particular, la gravedad, probabilidad y magnitud del perjuicio que se produciría de no emplearse el sistema; las consecuencias que su uso puede tener sobre los derechos y las libertades de todas las personas implicadas y, más concretamente, la gravedad, probabilidad y magnitud de dichas consecuencias; y las salvaguardias y condiciones que acompañen a su uso, fundamentalmente en lo que respecta a las limitaciones temporales, geográficas o personales.

Asimismo, la utilización de los sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso al público con fines de aplicación de la ley debe estar

14. La relación de delitos que posibilitan la emisión de una orden de detención y entregan aparecen relacionados en el art. 2 de dicha Decisión Marco. Vid., Decisión Marco del Consejo, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados Miembros, de 13 de junio de 2002, (2002/584/JAI) https://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81377

15. Tal y como se indica en el Considerando 19 de la propuesta de Reglamento, fijar este umbral para la pena o medida de seguridad privativa de libertad con arreglo al Derecho nacional contribuye a garantizar que el delito sea lo suficientemente grave como para llegar a justificar el uso de sistemas de identificación biométrica "en tiempo real".

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

sujeta a límites temporales y espaciales adecuados que tengan presente las pruebas o indicios relativos a las amenazas, las víctimas o los autores. Igualmente, la base de datos de personas de referencia debe ser adecuada para cada caso en cada una de las tres situaciones excepcionales previamente mencionadas (Considerando 20 de la propuesta de Reglamento).

Dicho uso ha de encontrarse autorizado[16] de manera expresa y específica por una autoridad judicial o por una autoridad administrativa independiente de un Estado miembro[17], previa solicitud motivada y de conformidad con las normas detalladas del Derecho interno. Sin embargo, en una situación de urgencia debidamente justificada[18] se podrá empezar a utilizar el sistema antes de obtener la autorización correspondiente, que podrá ser solicitada durante el uso o con posteridad a este. No obstante, en estos casos de urgencia, ha de limitarse al mínimo indispensable y cumplir con las salvaguardias y las condiciones oportunas de conformidad con lo postulado en el Derecho interno y según corresponda en cada caso concreto de urgencia por parte de las fuerzas o cuerpos de seguridad, quienes deben tratar de obtener una autorización lo antes posible e indicar los motivos por los que no han podido hacerlo con anterioridad (Considerando 21 de la propuesta).

Además, esta autoridad judicial o administrativa competente únicamente concederá la autorización cuente esté convencida, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso de sistemas de identificación remota "en tiempo real" es necesario y proporcionado para alcanzar alguno de los objetivos de las excepciones referidas, el cual habrá de indicarse en la solicitud.

Por su parte, los usuarios de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica deberán informar de su funcionamiento a las personas físicas expuestas a él. Obligación que, no obstante, no se aplicará a los sistemas de IA utilizados para la categorización biométrica autorizada por la ley para fines de



16. Conviene precisar en este punto que, el uso de los sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines distintos de la aplicación de la ley, incluso por parte de las autoridades competentes, no debe estar cubierto por el marco específico contemplado en la propuesta de Reglamento en lo que se refiere al uso de dichos sistemas con fines de la aplicación de la ley. En consecuencia, su uso con fines distintos de la aplicación de la ley no queda supeditado al requisito de obtener una autorización ni a las normas detalladas del Derecho interno aplicables que pudieran hacerlo efectivo (Considerando 23).

17. En este sentido, resulta importante destacar que este uso en el territorio del Estado miembro conforme a lo dispuesto en la propuesta de Reglamento solo debe ser posible cuando aquel haya decidido contemplar expresamente la posibilidad de autorizarlo en las normas detalladas de su Derecho interno, y en la medida en que lo haya contemplado (total o parcialmente) debiendo, en tal supuesto, especificar cuáles de los objetivos admitidos, y en su caso, en relación con cuáles de los delitos indicados, se pude autorizar su uso por las autoridades competentes. En consecuencia, los Estados siguen siendo libres de no ofrecer esta posibilidad, o de hacerlo únicamente en relación con alguno de los objetivos que permitan justificar un uso autorizado conforme a la propuesta de Reglamento (Considerando 22).

18. Esto es, aquellas en las que la necesidad de utilizar los sistemas en cuestión resulte tan imperiosa que imposibilite, de manera efectiva y objetiva, obtener una autorización antes de iniciar el uso (Considerando 21 de la propuesta de Reglamento).

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

detección, prevención e investigación de infracciones penales (con el obvio propósito de evitar poner sobre aviso el posible delincuente).

### *c. Enmiendas a la propuesta de Reglamento en materia de identificación biométrica*

No obstante esta propuesta de regulación, la cuestión relativa la identificación biométrica continúa resultando controvertida.

En este sentido, un estudio encargado por el Departamento de Política para los Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo, a petición de las Comisiones JURI y PETI, propone modificar cuestiones de la propuesta de Reglamento relacionadas con las técnicas de reconocimiento biométrico y de detección del comportamiento de personas (Fernández Hernández, 2021).

El informe –*Biometric Recognition and Behavioral Detection*[19]– que analiza el uso de las técnicas biométricas desde una perspectiva ética y jurídica, pone de relieve que la identificación biométrica, junto con la categorización biométrica, la detección de comportamientos, el reconocimiento de emociones, las interfaces informáticas cerebrales (BCI[20]) y otras técnicas similares, son utilizadas cada vez más por organismos públicos y privados con distintos propósitos (desde la asistencia sanitaria hasta el control de fronteras).

En esta línea, estima que, además de las técnicas biométricas tradicionales, como el reconocimiento facial o las huellas dactilares, estas incluyen otras como el análisis de la dinámica de las pulsaciones de las teclas o del ratón, la dinámica de los gestos, de las firmas, así como las características de la voz y la forma de andar. Sin embargo, normalmente no se incluyen entre los mismos comportamientos que pueden ser controlados en mayor medida por la voluntad humana, como las pautas de compra, el historial de navegación o el contenido de la comunicación. Pese a ello, en la medida en que tales actuaciones se analizan para inferir condiciones de naturaleza genética, fisiológica, conductual, psicológica o emocional que caracterizan a un individuo, puede estar justificado –considera– incluirlos en la noción de técnicas biométricas en un sentido más amplio.

En conjunto, el informe sopesa que la mejora de los sensores y de las capacidades informáticas, así como de la conectividad, anticipa el despliegue masivo de las tecnologías biométricas en una amplia variedad de sectores y para una amplia variedad de propósitos, mucho más allá de su utilización por las fuerzas de seguridad, convirtiendo las tecnologías biométricas en una suerte de tecnologías universales.

Como resultado de lo anterior, las mismas plantean una serie de cuestiones éticas específicas, ya que un individuo no puede cambiar fácilmente sus características

19. Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces (informe), de 6 de Agosto de 2021, https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)696968

20. Las BCI miden la actividad neurológica y traducen la actividad cerebral en datos legibles por la máquina. En general, este tipo de tecnología resulta potencialmente intrusiva, pues permite detectar pensamientos o intenciones y posiblemente también influir en las operaciones del cerebro humano.



IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

biométricas y, además, tienden a entrometerse en el cuerpo humano y, en última instancia, en el ser humano. Asimismo, su uso se asocia más generalmente a la vigilancia a gran escala, a la toma de decisiones mediante algoritmos o la elaboración de perfiles.

En este sentido, se afirma que la principal cuestión ética que plantea la identificación biométrica de personas se relaciona con la fase de registro, eso es, la creación y el almacenamiento de una plantilla única que identifica a una persona concreta. Ello, implica la transformación de las características físicas de un ser humano en meros datos digitales. Y esta plantilla, una vez creada y almacenada, posibilita que cualquiera que la tenga en su poder pueda rastrear y reconocer a dicho individuo en cualquier parte del mundo.

Por su parte, las principales cuestiones éticas que plantearía la detección biométrica de las condiciones humanas (como la intención de cometer un delito, el miedo, la fatiga o la enfermedad) se derivan de su naturaleza potencialmente intrusiva. En particular, son los sistemas que detectan emociones, pensamientos e intenciones humanas los que merecen especial atención desde una perspectiva ética y reguladora y que podrían exigir un nuevo conjunto de "neuroderechos", tales como el derecho a la intimidad cerebral y a la integridad mental.

A la vista de todo lo antedicho, el informe plantea la inclusión en la propuesta de Reglamento de un nuevo Título II bis dedicado a las prácticas restringidas de IA, que incluya las técnicas biométricas y de inferencia –en el sentido amplio indicado–, garantizando un uso responsable de estas que no ahogue la innovación y el crecimiento y que atienda a las consideraciones realizadas.



## 2. La utilización de la IA por las autoridades judiciales en asuntos penales

No son pocos los países occidentales que hacen uso de sistemas de IA con fines coercitivos y judiciales, ante las promesas de que el uso de estos sistemas reducirá determinados tipos de delincuencia y dará lugar a la toma de decisiones más objetivas –unas expectativas que no siempre son acertadas–.

Teniendo presente esta circunstancia, el Parlamento Europeo aprobó el 6 de octubre de 2021, la Resolución sobre la IA en el Derecho Penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016 (INI).[21]

En ella, se hace hincapié en que todas las soluciones de IA para las autoridades policiales y judiciales deben respetar plenamente los principios de la dignidad humana, no discriminación, libertad de circulación, presunción de inocencia y derecho de defensa. Todo ello, con inclusión del derecho a guardar silencio, libertad de expresión e información, libertad de reunión y asociación, igualdad ante la ley, igualdad de armas y el derecho a una tutela judicial efectiva y a un juicio justo, de conformidad con la Carta y con el Convenio Europeo de Derechos Humanos. Y, en línea con lo anterior, tampoco deben

21. Resolución del Parlamento Europeo sobre la inteligencia artificial en el Derecho Penal y su utilización por las autoridades policiales y judiciales en asuntos penales, de 6 de octubre de 2021, (2020/2016 (INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

poder dañar la integridad física de seres humanos ni distribuir derechos o imponer obligaciones jurídicas a las personas.

A tales efectos, el Parlamento Europeo pide una supervisión y un control democráticos estrictos de cualquier tecnología basada en IA utilizada por las autoridades policiales y judiciales, en particular las que puedan readaptarse para fines de vigilancia masiva o de elaboración masiva de perfiles.

En este sentido, considera esencial, tanto para la eficacia del ejercicio del derecho de defensa como para la transparencia de los sistemas nacionales de justicia penal, que un marco jurídico específico, claro y preciso regule las condiciones, las modalidades y las consecuencias del uso de herramientas de IA en el ámbito de las actuaciones policiales y judiciales, así como los derechos de las personas afectadas y procedimientos eficaces y fácilmente accesibles de reclamación y recurso.

De esta manera, se insiste en que, al ser el tratamiento de cantidades ingentes de datos un componente esencial de la IA, el derecho a la protección de la vida privada y el derecho a la protección de los datos personales se aplican a todos los ámbitos de la misma, debiendo respetarse plenamente el marco jurídico de la Unión sobre protección de datos y privacidad.

Asimismo, se pone de relieve que el enfoque adoptado en algunos países no pertenecientes a la Unión en relación con el desarrollo, el despliegue y el uso de la tecnología de vigilancia masiva interfiere de manera desproporcionada con los derechos fundamentales y, por lo tanto, no debe ser seguido por la Unión (como sería el supuesto chino que ya hemos examinado). Y, en esta línea, concluye que también deben regularse de manera uniforme en toda la Unión las salvaguardas contra el uso indebido de las tecnologías de IA por parte de las autoridades policiales y judiciales.



Igualmente, se señalan las consecuencias particularmente negativas que una excesiva confianza en la naturaleza aparentemente objetiva y científica de las herramientas de IA puede tener en el ámbito policial y judicial, sin tener presente que sus resultados pueden ser incorrectos, incompletos, irrelevantes o discriminatorios, deviniendo esencial en este sentido que las autoridades adquieran confianza y conocimientos para poner en cuestión recomendaciones algorítmicas o hacer caso omiso a las mismas. Por esta razón se subraya la necesidad de que, en este contexto, todas las decisiones con efectos legales hayan de ser tomadas siempre por un ser humano al que puedan pedirse cuenta de las decisiones que se adopten, sin basarse únicamente en el tratamiento automatizado de datos. Lo anterior resulta esencial para poder garantizar el derecho fundamental al recurso.

Finalmente, teniendo presente los diferentes tipos de uso de reconocimiento facial[22], con diferentes implicaciones para los derechos fundamentales, el Parlamento considera

22. Entre otros, la verificación/autenticación (es decir, la correspondencia entre una cara en vivo y una fotografía en un documento de identidad, por ejemplo, fronteras inteligentes), la identificación (es decir, la correspondencia de una foto con una base de datos de fotografías) y la detección (es decir, la detección de caras en tiempo real desde fuentes como las imágenes de CCTV y su correspondencia con bases de datos, por ejemplo, la vigilancia en tiempo real),

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

que el despliegue de tales sistemas por parte de las autoridades policiales debe limitarse a fines claramente justificados y hacerse con pleno respeto de los principios de proporcionalidad, necesidad y de la legislación aplicable.

En este sentido, pide la prohibición permanente del uso de análisis automatizados o el reconocimiento en espacios accesibles al público de otras características humanas, como la forma de andar, las huellas dactilares, el ADN, la voz y otras señales biométricas y de comportamiento. Y, en el mismo sentido, considera necesaria una moratoria al despliegue de sistemas de reconocimiento facial para fines coercitivos con funciones de identificación, a menos que se utilicen estrictamente para fines de identificación de víctimas de delito, hasta que las normas técnicas puedan considerarse plenamente acordes con los derechos fundamentales, los resultados obtenidos no sean sesgados y no sean discriminatorios, el marco jurídico prevea salvaguardas estrictas para su uso indebido y un control y supervisión democráticos estrictos y existan pruebas empíricas de la necesidad y proporcionalidad del despliegue de estas tecnologías.

E, igualmente, respalda la prohibición de las puntuaciones de las personas a escala masiva mediante la IA, considerando que cualquier forma de evaluación normativa de los ciudadanos a gran escala por parte de las autoridades públicas, en particular en este contexto policial y judicial, da lugar a la pérdida de autonomía, pone en peligro el principio de no discriminación y no puede considerarse conforme con los derechos fundamentales, en particular, la dignidad humana, codificados en el Derecho de la Unión.

## 3. EL TEDH ante la vigilancia masiva de la población



En el contexto de los potenciales peligros de una vigilancia masiva de la población, la regulación anterior debe ser puesta en relación con los pronunciamientos actuales en torno al uso de la tecnología con fines de seguridad nacional –es decir, la legitimidad de los sistemas de vigilancia masiva, y su relación con los derechos fundamentales–, dictados por el Tribunal Europeo de Derecho Humanos (en adelante TEDH), en tanto que máxima autoridad judicial para la garantía de los derechos humanos y libertades fundamentales en Europa.

Un debate sobre el que el tribunal evita pronunciarse de manera contundente, tendiendo a reiterar el amplio margen de apreciación de los Estados a la hora de buscar un equilibrio entre los sistemas de vigilancia de sus ciudadanos y la injerencia en la vida privada de los mismos. Por su carácter reciente, examinaremos la sentencia de 25 de mayo de 2021, dictada en Gran Sala en torno al asunto "Big Brother Watch[23]".

En ella se confirma la condena impuesta casi 3 años después a Reino Unido por sus sistemas de vigilancia masiva amparados por la Ley sobre Regulación de los poderes de Investigación, aprobada el 28 de julio de 2000.[24]

23. STEDH (Gran Sala), Case of Big Brother Watch and others v. The United Kingdom, de 25 de mayo de 2021, (Applications nos. 58170/13, 62322/14 and 24960/15). Recuperado de: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}

24. *Regulation of Investigatory Powers Act* 2000 (RIPA).

IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

Concretamente, el pronunciamiento en cuestión tiene su origen en las denuncias de periodistas y organizaciones de derechos humanos tras las revelaciones de Edward Snowden sobre programas de vigilancia e inteligencia compartida entre EEUU y Reino Unido. En este sentido, los demandantes alegaban que los sistemas de vigilancia electrónica empleados por servicios de inteligencia de Reino Unido habían interceptado masivamente las comunicaciones electrónicas de los ciudadanos ingleses, obteniéndolas de forma indiscriminada de los proveedores de servicios de telecomunicaciones, al mismo que tiempo que procedían a intercambiarlas con Gobiernos extranjeros. De esta forma, se estimaba que dicho sistema de vigilancia masiva del Reino Unido lesionaba, principalmente, el derecho al respecto a la vida privada y familiar (art. 8 del Convenio Europeo de Derechos Humanos, en adelante CEDH), en tanto que se había producido un tratamiento de sus datos personales sin su consentimiento y sin las garantías adecuadas; y la libertad de información (art. 10 CEDH), en tanto las interceptaciones y el intercambio de información efectuados ponían en peligro la protección de las fuentes de los periodistas, elemento angular de la libertad de prensa, y por consiguiente, de todo el sistema democrático (Arenas Ramiro, 2021).

La cuestión, por tanto, radica en si la vigilancia masiva e indiscriminada sin estar basada en ningún tipo de sospecha por parte de los servicios de inteligencia nacionales representa un medio necesario para una sociedad democrática con el fin de garantizar la seguridad nacional. Y también, hasta dónde han de permitir los Estados que, de manera recíproca, otro Estado pueda espiar e interceptar las comunicaciones electrónicas de sus ciudadanos, o bien emplear material de servicios de inteligencia extranjeros que han podido ser interceptados ilícitamente. Cuestiones estas que se dejan, no obstante, sin respuesta (Arenas Ramiro, 2021).



En el fondo, no existe una gran diferencia entre el primer pronunciamiento del TEDH en diciembre de 2018 y el más actual de mayo de 2021.

En este sentido, se hace referencia a 3 regímenes de vigilancia diferentes:

1. La interceptación masiva de comunicaciones;
2. La obtención de datos de comunicaciones de proveedores de servicios de comunicación;
3. La solicitud de interceptación de material de gobiernos extranjeros y agencias de inteligencia.

En cuanto a la primera y segunda de las cuestiones, la sala concluye por unanimidad que los sistemas empleados a tales efectos por Reino Unido lesionan tanto el derecho a la vida privada como a la libertad de información.

Así, considera que las leyes que regulen los sistemas de interceptación masiva de comunicaciones con la finalidad de garantizar la seguridad nacional deben cumplir con un mínimo de requisitos: indicar de forma clara los motivos que puedan dar lugar a una orden de interceptación; recoger una definición de las categorías de personas cuyas comunicaciones pueden ser interceptadas; las circunstancias en que las comunicaciones de un individuo pueden ser interceptadas; fijar un límite en la duración de la interceptación

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

y en su conservación; establecer el procedimiento a seguir para examinar, utilizar y almacenar los datos obtenidos; tomar las precauciones en el proceso de comunicación de los datos interceptados a terceras partes; y establecer las circunstancias en las que los datos interceptados pueden o deben ser borrados y destruidos. Además, las deben concretar los procedimientos y mecanismos de supervisión llevados a cabo por una Autoridad de control independiente, fijando sus poderes de actuación frente a los casos de incumplimiento; y estableciendo, igualmente, los procedimientos para una revisión independiente a posteriori, donde se compruebe el grado de cumplimiento de los requisitos. Se concretan de esta manera en mayor medida las garantías exigidas a este tipo de sistemas de vigilancia masiva.

Igualmente, la Gran Sala recordando que se encuentra en manos de los Estados decidir qué tipo de sistemas de vigilancia deben utilizar para proteger su seguridad nacional, subraya que estos deben estar sujetos a todas las garantías de "extremo a extremo", en todas las etapas de la interceptación masiva de comunicaciones.

De esta manera, concluye que la adquisición de metadatos de comunicaciones mediante poderes de interceptación masiva de comunicaciones resulta tan intrusiva como la interceptación de su contenido. Por ello, considera que la interceptación, retención y búsqueda de datos de comunicaciones debe analizarse teniendo en cuenta las mismas salvaguardas que se aplican al contenido de las comunicaciones.

Por su parte, en el caso de los sistemas de obtención de datos de los proveedores de servicios, al hilo de analizar las sentencias del TJUE[25], el TEDH concluye que el acceso debería ser limitado a los fines de la lucha contra la "delincuencia grave" que supongan una amenaza para la seguridad nacional, debiendo el acceso estar sujeto a un control previo por parte de un tribunal u organismo administrativo independiente.[26]



25. Concretamente, se alude a la STJUE de 8 de abril de 2014, asunto Digital Rights Ireland; STJUE de 21 de diciembre de 2016, asunto Tele2 Sverige AB; STJUE de 2 de octubre de 2018, asunto Ministerio Fiscal; STJUE de 6 de octubre de 2015, asunto Maximillian Schrems; STJUE de 16 de julio de 2020, asunto Data Protección Commissioner contra Facebook y Maximilian Schrems; y las SSTJUE de 8 de septiembre de 2017, asunto Privacy International; de 30 de octubre de 2017, asunto La Quadrature du Net; y de 6 de octubre de 2020, asunto Ordre des barreaux francophones et germanophone. En particular, en el último de tales pronunciamientos, el TJUE deja claro que, si bien los Estados son soberanos, la inviolabilidad de la seguridad nacional no puede erigirse a modo de excepción general pues, no hay que olvidar que el derecho a la protección de datos y a la intimidad son derechos fundamentales que, si bien pueden ser objeto de limitaciones en función de las circunstancias, no pueden obviarse con carácter general sin que exista una amenaza grave, auténtica, presente o previsible.

26. Pero, a diferencia de la jurisprudencia del TJUE en materia de amenazas graves a la seguridad nacional que posibilita obligar a los proveedores de servicio a conservar, de forma general e indiscriminada datos de tráfico y localización, siempre que dichas amenazas sean auténticas y actuales o previsibles, el TEDH no exige tales notas de autenticidad y previsibilidad, lo cual, a nuestro juicio no resulta acertado. Nos encontramos ante una práctica que implica una vulneración de la intimidad personal y la privacidad de los sujetos pues tales datos de tráfico y localización pueden conformar un perfil específico de una persona determinada. Constreñirlo al supuesto de que, además de un caso de lucha contra la delincuencia grave, se trate de una amenaza auténtica y previsible, devendría más adecuado al tratarse de la limitación de derechos fundamentales, tal y como se ha venido exigiendo por el TJUE.

Además, el TEDH no se pronuncia de manera tan rotunda como el TJUE en materia de acceso a los

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

Sin embargo, en torno a la cuestión relativa a la solicitud de interceptación de material de gobiernos extranjeros y agencias de inteligencia, considera que no hubo violación del CEDH, pues la legislación británica había establecido normas detalladas y claras que regulaban cuando los servicios de inteligencia podrían solicitar material interceptado a Agencias de inteligencia extranjeras y cómo debería ser examinado. Por tanto, se pronuncia sobre la validez de este tipo de prácticas siempre y cuando se establezcan las medidas de seguridad adecuadas para evitar un abuso de su utilización, de manera que el sistema habría de especificar expresamente el tipo de información, los países de los que provendría aquella y los detalles sobre cómo sería utilizada y conservada una vez interceptada.

Pero se trata de un pronunciamiento que puede llegar a plantear situaciones que se encuentren al margen del CEDH. Tal sería el caso de que se hayan interceptado comunicaciones de manera ilícita por un Estado, lesionándose con ello la vida privada de sus ciudadanos –entre otros derechos–. Y, sin embargo, tales prácticas serían consideradas lícitas por el TEDH si el Estado receptor cumple con las citadas garantías previstas, las cuales, además, se concretan por el propio Estado receptor (Arenas Ramiro, 2021).

Por tanto, habría resultado adecuado que el TEDH se hubiese pronunciado expresamente sobre la necesidad de que la información requerida y la información recibida o aceptada por el Estado con la ayuda de los Gobiernos extranjeros disfrutasen del mismo nivel de protección para poder ser utilizadas.

En definitiva, como puede observarse, el TEDH no se pronuncia expresamente prohibiendo la vigilancia masiva generalizada e indiscriminada, pues evita dictaminar sobre la forma en que los Estados deben combatir las nuevas formas de delincuencia y terrorismo respetando la privacidad de los ciudadanos.

Se sigue dejando la puerta abierta al uso de los sistemas de vigilancia masiva siempre que cumplan con las garantías que se indican en la sentencia y se utilicen de manera proporcionada y, se abre, además, la puerta al intercambio de información entre los sistemas de inteligencia de los Estados, delegando de esta manera en el margen de apreciación nacional su utilización para prevenir, especialmente, posibles ataques terroristas en un mundo globalizado.

Se pierde pues, una excelente oportunidad para definir con claridad las circunstancias en que las comunicaciones privadas pueden ser interceptadas (en lugar de remitirlo a la legislación estatal), así como para aportar pautas más precisas y detalladas sobre los



---

datos electrónicos. Este último, en el asunto Maximilian Schrems afirmó con contundencia que los marcos jurídicos por los que se concede a las autoridades públicas el acceso a los datos de forma generalizada comprometen la esencia del derecho fundamental a la vida privada, garantizado en el art. 7 de la CDFUE (apartado 94 de la sentencia). En efecto, en palabras del TJUE dicho derecho "quedaría privado de alcance si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en razones de seguridad nacional o de prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin que estas prácticas se rodeen de garantías adecuadas y comprobables" (apartado 34 de la sentencia). *Vid*., STJUE de 6 de octubre de 2015, asunto Maximillian Schrems, (C-363/14), Recuperado de: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=143358

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

procedimientos que deben ser acatados por los Estados a fin de examinar, almacenar y acceder a información privada. Y, especialmente, para defender plenamente la importancia de la vida íntima y el secreto de las comunicaciones cuando se enfrentan a sistemas de vigilancia masiva, garantizando los valores propios de toda sociedad democrática, pudiendo estar encaminándonos hacia un Gran Hermano tecnológico. En efecto, los sistemas de vigilancia masiva interfieren en el derecho a la privacidad de los individuos y, al mismo tiempo condicionan el ejercicio de otros derechos fundamentales, como la libertad de expresión, de reunión o de asociación.

Resulta pertinente concluir este apartado con las palabras del Juez Pinto de Albuquerque en su voto particular a la sentencia – y con las cuales coincidimos plenamente–: "Este pronunciamiento altera fundamentalmente el equilibrio existente en Europa entre el derecho al respeto de la vida privada y los intereses de la seguridad pública, al admitir la vigilancia no selectiva del contenido de las comunicaciones electrónicas y los datos de comunicaciones relacionados, y peor aún, el intercambio de datos con terceros países que no gozan de una protección comparable a la de los Estados del Consejo de Europa. Esta conclusión está tanto más justificada si se tiene en cuenta el perentorio rechazo del TJUE al acceso generalizado al contenido de las comunicaciones electrónicas, su manifiesta reticencia a la retención general e indiscriminada de datos de tráfico y ubicación y su limitación de intercambios de datos con servicios de inteligencia extranjeros que no garantizan un nivel de protección esencialmente equivalente al garantizado por la Carta de los Derechos Fundamentales. En estos tres aspectos, el Tribunal de Estrasburgo va a la zaga del Tribunal de Luxemburgo, que sigue siendo el faro de los derechos de privacidad en Europa."



## IV. LA OTRA CARA DEL *BIG BROTHER*

A pesar de unos mayores y más definidos límites en lo que al uso de la IA y protección de datos se refiere en el contexto europeo, como hemos podido comprobar, la configuración del derecho a la seguridad nacional y las libertades y derechos ciudadanos continúa siendo una cuestión difícil de abordar.

En este sentido, la mayor regulación y salvaguardas en torno a los sistemas de IA que pueden llegar a suponer un potencial riesgo de vigilancia masiva no excluye la presencia de este Gran Hermano en nuestra sociedad. Lo que ocurre es que adopta una forma diferente.

A diferencia del *Big Brother* vaticinado por Orwell y que comienza a dejarse entrever –orgullosamente– en China, el que podemos encontrar en occidente es invisible, sutil, y, también, amigable. En términos generales, los ciudadanos no solemos tener la sensación de sentirnos vigilados.

Los avances tecnológicos y las inmensas posibilidades de las que nos dota la red proyectan una imagen de seductora libertad. Podemos acceder a golpe de *click* a innumerables canales en línea, hacer la compra sin salir de casa e, incluso, pedirle a Alexa que nos cambie de canal, que ponga música o que nos recuerde una cita importante. Facebook nos anuncia las publicaciones que les gustan a nuestros amigos, Spotify la

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

música que escuchan y sus cantantes favoritos e incluso, las tiendas online nos informan de la compra de un producto determinado llevada a cabo en ese mismo instante por un usuario concreto. El *Big Brother* de nuestra sociedad nos anima a comunicarnos y a consumir y lo hace apetecible, sencillo y transparente.

Pero, tras esta ilimitada libertad se esconde el riesgo del control pasivo y cesión de nuestro ámbito de privacidad.

El *Big Brother* y el *big data* son dos caras de la misma moneda. En efecto, en la red todo queda registrado y, la memoria online no entiende de lagunas. La huella digital que dejamos es capaz de aportar una representación de nuestra persona mejor que nosotros mismos. Cada interacción en línea, cada compra, cada descarga… conforman microactuaciones que nos perfilan como sujetos y nos define. Y este perfil puede ser conocido y utilizado.

Es más, el registro de este conocimiento proporcionado por los propios sujetos y por las actuaciones que concluyen podría ser empleado incluso para predecir nuestros comportamientos y elaborar patrones.

En este sentido, ya encontramos casos de lo que se conoce como *predictive policing*, en tanto que sistemas dotados de IA y *machine learning* que tratan de identificar potenciales delincuentes y prevenir la actividad criminal.[27]

Este es, de hecho, el argumento principal para que, –irónicamente– estemos dispuestos a sacrificar, muchas veces sin saberlo, o incluso voluntariamente, nuestras libertades individuales: lograr una mayor seguridad ciudadana. Una cuestión que, como hemos tenido ocasión de comprobar, carece de un abordaje claro y suficiente a la hora de lograr un equilibrio adecuado con el respeto de los derechos fundamentales.



## V. CONCLUSIONES

Con la prohibición de los sistemas aludidos se trata de evitar una situación similar a la acontecida en China en cuanto a la existencia de un sistema de puntuación social y un control activo e incisivo de la población. En efecto, eran estos sistemas de vigilancia masiva mediante la identificación biométrica remota en tiempo real y la falta de límites a la cesión masiva de datos entre los proveedores de servicios lo que, en mayor medida, posibilitaban la existencia de dicho sistema de puntuación social.

Parámetros estos que, en el entorno europeo, como ya hemos puesto de relieve, se encuentran sometidos a límites específicos –como es el caso de la retención masiva y cesión de datos, aun cuando existan aún líneas interpretativas difusas e insuficientes– o directamente prohibidos (como acontece con los sistemas de calificación social).

Sin embargo, esta mayor regulación del fenómeno no excluye la presencia de un Gran Hermano.

27. Si bien la actuación policial predictiva puede analizar los conjuntos de datos necesarios para el establecimiento de patrones, no hay que perder de vista que, correlación no implica causalidad y no pueden hacerse predicciones fiables de comportamiento individual. Por lo tanto, tales pronósticos algorítmicos no deben constituir la única base de la investigación.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

En efecto, tanto si somos conscientes de ello como si no, la hipervigilancia constituye uno de los rasgos identificativos de nuestra sociedad actual, lo cual nos obliga a traer al frente el debate relativo a la seguridad nacional y la libertad y derechos fundamentales de los ciudadanos.

Un debate en el cual una regulación que tome en consideración y trate de ponderar todos los intereses en liza deviene esencial, así como el pleno respeto en el cumplimiento de las normas nacionales, comunitarias e internacionales en materia de derechos fundamentales, a través de una homogeneización de criterios.

A tales efectos, la propuesta de Reglamento Europeo sobre IA, y los límites jurisprudenciales en torno a la protección de datos cuando se encuentra en juego la seguridad nacional, constituye un significativo avance, pues de nada sirven todas las ventajas que puedan sobrevenir del uso de estos sistemas si no se enmarcan en un entorno normativo que pondere adecuadamente los derechos e intereses en presencia. Pero se trata de un avance que, todavía, es deficiente.

Resulta evidente que nos encontramos ante una importante etapa configuradora de la privacidad en un mundo digitalizado y abierto a nuevas amenazas en contra de la seguridad nacional. Y, en la prevención e investigación de estas nuevas modalidades delictivas globalizadas y en su persecución, la IA y los sistemas de *big data* tienen mucho que aportar.

Pero lo anterior, no puede avocarnos a convertir a todos los sujetos en potenciales sospechosos, por muchas garantías que se establezcan, pues estaríamos chocando frontalmente contra un derecho tan basilar de los Estados democráticos como lo es la presunción de inocencia.

La importación de los derechos humanos a la esfera digital deviene pues crucial, especialmente en el contexto de la vigilancia estatal. El sistema de crédito social chino es el epítome de las desastrosas consecuencias del avance tecnológico sin un compromiso acorde con los derechos humanos.

Debemos evitar a toda costa convertir nuestros Estados democráticos en Estados policiales en los que la seguridad nacional se convierta en la excepción capaz de justificar una vigilancia social masiva sin límites pues, el solo hecho de sentirnos constantemente observados, ya supone una coacción de la propia libertad individual.

Esa es la idea misma del panóptico de Bentham: si un sujeto cree que podría estar siendo observado, actuará como si lo estuviera. Una noción que George Orwell también entendió perfectamente.

## Bibliografía

Arenas Ramiro, Mónica (2021), Reino Unido y sistemas de vigilancia: la STEDH Big Brother Watch, de 25 de mayo de 2021, *Diario La Ley*. Recuperado el 11 de noviembre de 2021 de https://diariolaley--laleynext--es.us.debiblio.com/Content/Documento.aspx?params=H4sIAAAAAAAAEAE2OwWrDQAxEv6a6FIpjx-Ski-tLIJTQmt7ltbBFNrvNruzGf1-l7qGCQYh5jOY2c1o7visuMoqn4ISer5RIlchriGG9YpdmBqU-Y7V_OrjCtDOVQE5n8m10uKsehyzcUW8UxDRwalYsQKOSf-eM-7KEPMXvN-7JPpBJDQ2nLlmHAtitsqqqs6xoWTtkA_JSRgzJMMk4nk258ZkpuOtPIeAziJL5Q_rqDDxfr8vFr_gebWdXCeg2bB87bbkn5lTyH4a_GD0aQSgoLAQAAWKE#tDT0000332555_NOTA28



IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces (Informe), de 6 de Agosto de 2021, https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)696968

Carta de Derechos Fundamentales de la Unión Europea, de 30 de marzo de 2010, (2010/C 83/02) https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Consejo de Estado Chino, (2014), Planning Outline for the Construction of a Social Credit System (2014-2020). Recuperado el 3 de noviembre de 2021 de https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/

Digital Guide IONOS, (2021), *Sistema de crédito social chino: una puntuación con muchas consecuencias*. Recuperado el 3 de noviembre de 2021 de: https://www.ionos.es/digitalguide/online-marketing/analisis-web/que-es-el-sistema-de-credito-social-chino/

Drinhausen, Katja y Brussee,Vincent, (2021), *China's Social Credit System in 2021: From fragmentation towards integration*. Recuperado el 5 de noviembre de 2021 de: https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration

Fernández Hernández, Carlos B (2021), El Parlamento Europeo estudia nuevas enmiendas a la propuesta de Reglamento sobre IA en materia de identificación biométrica, *Diario la Ley*, Recuperado el 11 de noviembre de 2021 de https://diariolaley--laleynext--es.us.debiblio.com/Content/Documento.aspx?params=H4sIAAAAAAAAEAE2OQUvEQAyFf425CDIdC-5lLnU9CLKIFu_pNLTB2YzOpHX7743Wg4fHI7yPl_e5UNl6umhYeeKEEhmvz1h5RaibZNnOoS8LgeJQw217dRedqTF5wKgLpmOOwbufg1fqcTAKchmpdFtwoFkxvVANrfdQ5_x1QvuEylk6LHs3j2M4PTjnfHNo2oODlUo1ILzxRKIEM0_zk0l3vhKWOD_jROFROHK-wfpxgSTvtuX1N_wPdouqlQ0qewYxmR9R6R4Tyfg34xvS2eXSCwEAAA==WKE

Lee, Amanda, (2020), *What is China's social credit system and why is it controversial?* Recuperado el 5 de noviembre de 2021 de: https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial

Libro Blanco sobre la IA al establecer que "el uso de aplicaciones de IA para la identificación biométrica remota y otras tecnologías de vigilancia intrusiva deben considerarse siempre de riesgo elevado (…). Vid., Libro Blanco sobre la inteligencia artificial-un enfoque europeo orientado a la excelencia y la confianza, de 19 de febrero de 2020, COM (2020) 65 final, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas; propuesta de Reglamento del Parlamento Europeo y del Consejo sobre los principios éticos para el desarrollo, el despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas (Anexo), de 20 de octubre de 2020 , https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html#title2

Marr, Bernard, (2019), *Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?-* Recuperado el 6 de noviembre de 2021 de: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/?sh=4dd9089048b8

Martí, Rosa, (2020) *El crédito social chino: cuando el gobierno te pone nota*. Recuperado el 5 de noviembre de 2021 de: https://www.esquire.com/es/actualidad/a30361853/credito-social-chino-que-es/



IUS ET SCIENTIA • 2022
Vol. 8 • Nº 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02

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, de 21 de abril de 2021, {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo 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), de 27 de abril de 2016, DOUE-L-2016-80807, https://www.boe.es/doue/2016/119/L00001-00088.pdf

Resolución del Parlamento Europeo sobre la inteligencia artificial en el Derecho Penal y su utilización por las autoridades policiales y judiciales en asuntos penales, de 6 de octubre de 2021, (2020/2016 (INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

STEDH (Gran Sala), Case of Big Brother Watch and others v. The United Kingdom, de 25 de mayo de 2021, (Applications nos. 58170/13, 62322/14 and 24960/15). Recuperado de: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}

STJUE de 6 de octubre de 2015, asunto Maximillian Schrems, (C-363/14), Recuperado de: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=143358



IUS ET SCIENTIA • 2022
Vol. 8 • N° 1 • pp. 9-34
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i01.02