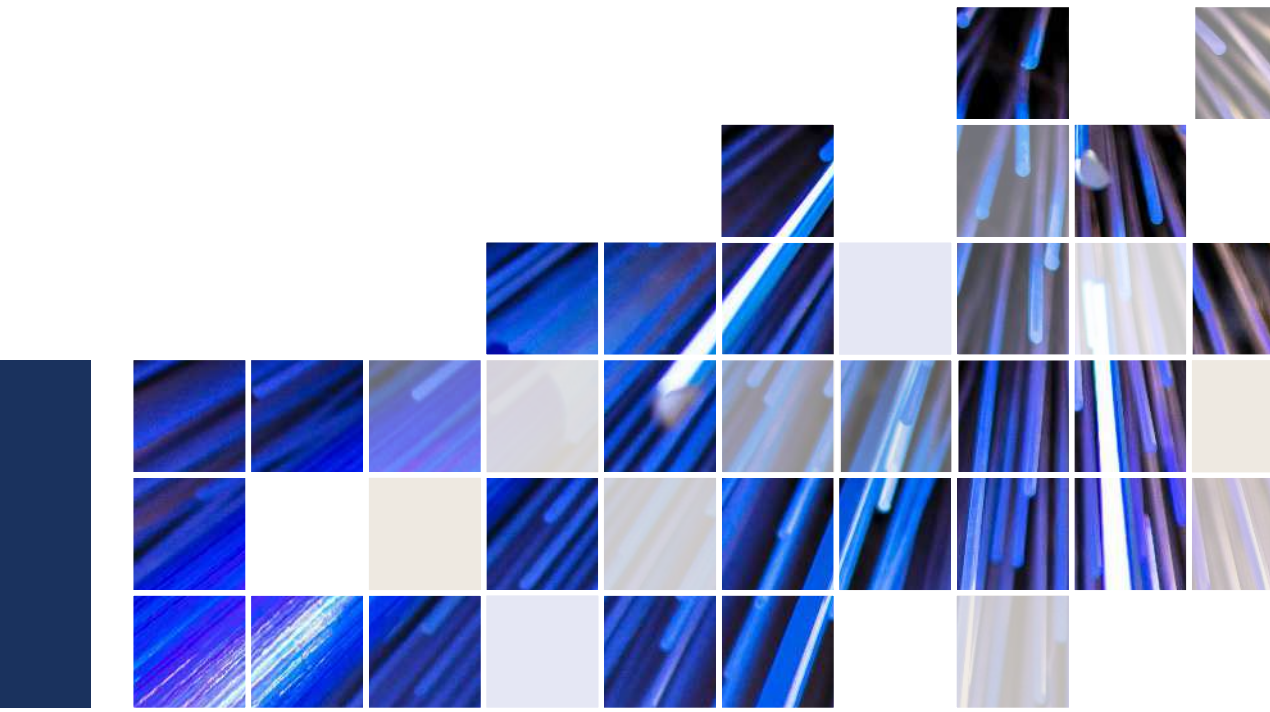
TEMAS

La transformación de la justicia a través de la Inteligencia Artificial

Análisis comparado mundial y 40 propuestas disruptivas

Alfonso Peralta Gutiérrez



LA LEY

ARANZADI LA LEY, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es
Atención al cliente: https://areacliente.aranzadilaley.es/publicaciones

Edición: mayo 2026

Depósito Legal: M-9612-2026
ISBN versión impresa: 979-13-88078-39-2
ISBN versión electrónica: 979-13-88078-40-8

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.
Printed in Spain

ÍNDICE SISTEMÁTICO

CAPÍTULO 1

CONTROL JUDICIAL DE LOS ALGORITMOS

I. INTRODUCCIÓN

Llevamos ya unos pocos años hablando de la inteligencia artificial como cuarta revolución industrial, y en los últimos meses no hay día que no surja una noticia sobre usos, riesgos, o declaraciones de expertos sobre esta tecnología emergente. Y lo que nos queda.

Sabemos las estimaciones de lo que va a suponer la inteligencia artificial a la economía, los beneficios de una próxima era de las máquinas, su afectación transversal a todos los sectores, pero también sus riesgos, como la opacidad («la caja negra»), los sesgos, imprevisibilidad, o fallos de eficacia que pueden repercutir negativamente en derechos fundamentales, como la igualdad y no discriminación, dignidad humana, privacidad, libertad de expresión, presunción de inocencia o derecho a un juez imparcial.

La inteligencia artificial se alimenta de un conjunto enorme de datos y de información, pero no siempre tiene el conocimiento para comprender toda esa información y evaluarla conforme a su contexto, y mucho menos la sabiduría para interpretarla y aplicarla a su contexto, e incluso a problemas distintos. Por ello, la IA ha de considerarse una herramienta, y como cualquier herramienta podrá utilizarse para hacer el bien o el mal. Lo que hay es que regular los malos usos, sus prohibiciones, y castigarlos.

Tras dos años de tramitación parlamentaria y mucha discusión académica y legislativa, el 14 de junio de 2024 se produjo el debate y votación de la ley europea de inteligencia artificial, posiblemente la ley más importante sobre la materia del mundo, quedando a expensas de las negociaciones interinstitucionales. Es la hora de la regulación de la IA y comenzar a interpretarla y aplicarla. Y es algo que incluso la propia industria está pidiendo a gritos. Que la muchas veces autoidentificada como libertaria y anarcocapitalista Silicon Valley demande regulación, cuyo uno de los principales lemas era «muévete rápido y rompe cosas», es algo inédito y sólo comprensible desde la envergadura del gran desafío al que nos enfrentamos.

Para ello, **se hace necesaria la creación de las autoridades de supervisión a nivel europeo y español, el diseño de sus estatutos, la coordinación con otras autoridades como la AEPD y el supervisor europeo, la puesta en marcha de los registros de archivos y de operadores de alto riesgo, adopción de sistemas estandarizados de auditoría de algoritmos y cumplimiento normativo y la implementación del sand-**

box[1] **o banco de pruebas para comenzar a ponerlos en práctica, formación para auditores que sean capaces de evaluar la implementación y que previamente hayan sido acreditados como organismos de evaluación**. O, por ejemplo, **¿cómo se coordinará un sello español de la IA con un sello europeo y unas normas estandarizadas internacionales y qué valor añadido aportará nuestro marcado en un mundo globalizado?** Asimismo, las compañías tienen que empezar a pensar en el **procedimiento que exige la ley, la verificación de los requisitos del sistema, el examen del diseño, la preparación de la documentación y un sistema de control interno o vigilancia posterior continuada durante todo el ciclo de vida de la IA,** así como la **creación de una nueva figura en el organigrama corporativo o la adaptación de una ya existente** que asuma tales funciones de lo que ya se está llamando en la jerga tecnológica, como **RAI Champion (*Responsable AI Champion*) o AICO (*AI Compliance Officer*)**

Es decir, no es poco lo que todavía queda para una verdadera regulación y aplicación de la normativa de esta tecnología. Así, se espera que la aprobación de las normas estandarizadas (podríamos asimilarlo al reglamento técnico desarrolle la ley) como fecha límite el 30 de abril de 2025, y los contratos adjudicados de sandbox y sello español de IA tienen un plazo de ejecución de 30 meses, esto es, 30 de diciembre de 2025[2]. Sin embargo, todo ello se ha retrasado sin estar a día de hoy finalizado.

Y en esto, las administraciones públicas deberían ser las primeras en comenzar a aplicar la ley europea una vez sea publicada y en dar ejemplo, estando obligadas a ello. Así, con la aprobación por el Parlamento Europeo quedarán prohibidos definitivamente los *«sistemas de IA para realizar evaluaciones de riesgo de personas físicas o grupos de personas físicas con el fin de evaluar el riesgo de una persona física de delinquir o reincidir o para predecir la ocurrencia o reincidencia de una infracción penal o administrativa real o potencial basada en la elaboración de perfiles»*. Por lo tanto, no sólo es que administraciones públicas deben comenzar a revisar sus sistemas y publicar los algoritmos, algo que no han hecho ni con VioGèn, ni con Veripol, ni con RisCanvi en Cataluña, los cuales carecen de una mínima transparencia o mínima auditoría del sistema de predicción de riesgo de violencia de género considera que la calidad de los datos es mejorable o presenta sesgos y

(1) MÉNDEZ, Manuel Ángel. Rebelión de funcionarios TIC contra las Big Four. «Llevamos años aquí y nos ningunean». EL CONFIDENCIAL. 8 de junio de 2023. Consultado el 25 de junio de 2023. Disponible en: https://www.elconfidencial.com/tecnologia/2023-06-08/funcionarios-tic-big-four-deloitte-pwc-ernst-young-kpmg_3656785/

(2) *Vid*. Nota al pie 1.

discriminaciones. De igual manera, hasta que no lo publicó El Confidencial[3], [4] se desconocía que la Seguridad Social usaba un algoritmo secreto para «cazar» posibles fraudes en bajas laborales. De igual manera, ya están saliendo las primeras informaciones sobre que la Agencia Tributaria se espera comience a utilizar nuevas herramientas basadas en IA para el análisis de datos que permitan hacer un control más eficiente de los datos y de esa manera detectar quiénes cumplen y quiénes no, con el pago de los impuestos que les corresponden[5].

Desde Hacienda ya están dando los primeros pasos en este sentido con el sistema de vigilancia que permite actualmente detectar el fraude fiscal y también prevenirlo, ayudando en esta tarea a los inspectores.

O también existe BOSCO[6], un software que utiliza el Gobierno, de algoritmo igualmente secreto, que las eléctricas utilizan para decidir quién es beneficiario del denominado bono social eléctrico y que se ha denunciado que además de su opacidad tiene fallos y sesgos.

A tenor de ello, directamente estos sistemas —según la última versión del Reglamento Europeo (si ésta se mantiene)— el primer día de su entrada en vigor deberían dejar de utilizarse por el Gobierno español.

El ejecutivo holandés utilizaba el algoritmo SyRI para detectar diversas formas de fraude, incluidos los beneficios sociales, las asignaciones y el fraude fiscal, y en 2020 el Tribunal de Distrito de La Haya declaró que este sistema violaba los derechos humanos.

De igual manera, en el Reglamento quedan prohibidos los sistemas de reconocimiento facial y biométrico a tiempo real no selectivos, pero se permiten si se utiliza a posteriori previa resolución judicial para análisis de imágenes obtenidas. Así, el sistema ABIS, siglas en inglés que responden a «sistema automático de identificación biométrica», que está entrenando el Ministerio del Interior y que además no ha consultado previamente a la AEPD, lo primero que deberá hacer será adaptarse a los

(3) JIMÉNEZ ARANDIA, Pablo y MÉNDEZ, Manuel Ángel. La Seguridad Social usa una IA secreta para rastrear bajas laborales y cazar fraudes. EL CONFIDENCIAL. 17 de abril de 2023. Consultado el 25 de junio de 2023. Disponible en: https://www.elconfidencial.com/tecnologia/2023-04-17/seguridad-social-ia-inteligencia-artificial-inss-bajas-empleo-algoritmos_3611167/#:~:text=Desde%202018%2C%20la%20Seguridad%20Social,EC%20Dise%C3%B1o

(4) JIMÉNEZ ARANDIA, Pablo. Preguntas sin respuesta sobre el sistema predictivo de la Seguridad Social. EL CONFIDENCIAL. 17 de abril 2023. Consultado el 25 de junio de 2023. Disponible en: https://www.elconfidencial.com/tecnologia/2023-04-17/preguntas-sin-respuesta-del-sistema-predictivo-de-la-seguridad-social_3610544/

(5) LENCINA, Fernanda. Así te vigila Hacienda con una poderosa Inteligencia Artificial para evitar fraudes. The Huffington Post. 2 de agosto de 2023. Consultado el 2 de agosto 2023. Disponible en: https://noticiastrabajo.huffingtonpost.es/economia/hacienda-te-vigila-con-inteligencia-artificial/

(6) OLLERO, Daniel J. El algoritmo secreto del Gobierno que decide si te llevas una subvención para la factura de la luz. EL MUNDO. 3 julio de 2019. Consultado el 25 de junio de 2023. Disponible en: https://www.elmundo.es/tecnologia/2019/07/03/5d1b89fbfc6c83a2358b46ca.html

requisitos del reglamento europeo como sistema de alto riesgo. Y el legislador deberá prever un nuevo artículo 588 nonies de la Ley de Enjuiciamiento Criminal para autorizar este tipo de sistemas.

Es decir, el camino no ha terminado con la aprobación del Reglamento europeo de IA, sino que acaba de comenzar, y como veremos a continuación los tribunales tendrán mucho que decir.

II. JURISPRUDENCIA EXTRANJERA DE CONTROL JUDICIAL DE LOS ALGORITMOS: COMPAS, SYRI, ROBODEBT Y OTROS (PROYECTO SENSING, HESSENDATA, EDWARD BRIDGES V. SOUTH WALES POLICE; «IBORDERCTRL: INTELLIGENT PORTABLE BORDER CONTROL SYSTEM»; PATEL V. FACEBOOK; CLEARVIEW; UBER; DELIVEROO; PEOPLE V. SUPERIOR; CORONAPP; CHATGPT Y OTROS)

A) COMPAS

El caso Compas es ya archiconocido y el caso prototípico de los posibles sesgos en los algoritmos y cómo éstos pueden afectar a la función jurisdiccional.

Lo abordamos hace ya varios años en la primera edición del curso «El Derecho y la Inteligencia artificial» del Consejo General del Poder Judicial en colaboración con la Universidad de Granada[7].

Su acrónimo significa Correctional Offender Management Profiling for Alternative Sanctions y en español puede traducirse como Administración de Perfiles de Criminales para Sanciones Alternativas del Sistema de Prisiones de EE. UU. Esta herramienta destinada al sector público es utilizada por el Departamento de Correcciones y Rehabilitación del Estado de California (lo que vendría a ser, Vigilancia Penitenciaria), para ayudarles a la clasificación, supervisión y gestión de la rehabilitación de los criminales y la adopción de medidas de seguridad. Compas determinaría los riesgos, evaluaría las necesidades y la flexibilidad de las medidas. Este sistema fue implantado en 2006-07, y habría ya evaluado más de un millón de presos.

Se trata de un sistema que analiza 137 parámetros a través de cuestionarios y del historial del delincuente con información relativa al consumo de sustancias estupefacientes, entorno familiar, antecedentes penales o grado de inserción social. Pero también entre esos parámetros estaría la pobreza, la raza, el nivel educativo y rasgos de la personalidad. Así, el riesgo de reincidencia estaría fundamentado en 7 factores criminológicos importantes: los déficits de educación, económicos y de habilidades; actitudes antisociales; compañías criminales y aislamiento; tempera-

(7) Herramientas de inteligencia artificial en el ámbito jurídico comparado. VV. AA., HERRERA TRIGUERO, Francisco; PERALTA GUTIÉRREZ, Alfonso; TORRES LÓPEZ, Leopoldo Salvador. El derecho y la inteligencia artificial. 2022. 24/10/2022. Editorial Universidad de Granada. 978-84-338-7049-0

mento, impulsividad y ausencia de autocontrol; disfuncionalidades parentales y maritales; adicciones a drogas o alcohol y desviaciones sexuales.

Utilizando esos criterios realizaría un scoring o puntuación predictiva del riesgo de reiteración delictiva de los presos y sujetos a libertad condicional, así como propondría otra serie de medidas de reinserción según el nivel adjudicado. Esto ha producido un importante cuestionamiento del algoritmo[8], puesto que sería altamente probable el riesgo de reincidencia para un joven desempleado con un primer delito menor frente una persona mayor con un delito violento.

Lo más polémico de este sistema de puntuación predictiva ha resultado a raíz de un informe de un equipo de investigadores liderado por Julia Dressel, estudiante de informática en el Dartmouth College, que, tras analizar la validez de los resultados de COMPAS, encontró que el algoritmo que utiliza no es más fiable que cualquier humano sin preparación. Y además había sospechas de que el sistema favorecía a los blancos frente a los negros[9], [10].

Un caso que puso en tela de juicio el sistema fue el Caso Loomis v. Wisconsin[11]. En febrero de 2013, Eric Loomis fue condenado al conducir un coche usado en un tiroteo. Negó haber participado en el tiroteo, pero reconoció conducir el coche usado en el mismo. Loomis fue condenado por los dos delitos más leves, resistencia a la autoridad y hurto de vehículo. Sin embargo, en la vista del juicio se consultó el sistema COMPAS y el tribunal fundó parte de la condena en dicha evaluación. La defensa recurrió por considerar vulnerado el derecho a un proceso debido porque el algoritmo del programa es secreto (lo que se denomina «black box») y porque la sentencia se fundó entre otros factores en la raza del condenado lo que sería discriminatorio. El Tribunal Supremo de Wisconsin desestimó el recurso considerándola no discriminatoria y fundada en cuanto que la raza fue solo uno de los factores a tener en cuenta. De igual manera, a la vista de que el sistema utiliza información facilitada por el investigado, éste podría negarse a contestar los cuestionarios, así como se reconoció la importancia de individualización de las sentencias, sostuvo que se valoraron más pruebas y admitió que COMPAS sólo compara el riesgo de reincidencia respecto a grupos sociales similares al del investigado.

(8) CORVALÁN, Juan. *El peligro de la inteligencia artificial como oráculo del sistema penal*. 30 de agosto de 2017. Disponible 23 enero 2020. Infobae. https://www.infobae.com/opinion/2017/08/30/el-peligro-de-la-inteligencia-artificial-como-oraculo-del-sistema-penal/

(9) COMPAS Recidivism Risk Score Data and Analysis. Broward County Clerk's Office, Broward County Sheriff's Office, Florida Department of Corrections, ProPublica. Enero 2020. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

(10) DEL CAMPO, Adelaida. *Luces y sombras de la Inteligencia Artificial aplicada a la justicia*. 11 mayo de 2019-. Confilegal. Disponible 23 enero 2020. https://confilegal.com/20190511-luces-y-sombras-de-la-inteligencia-artificial-aplicada-a-la-justicia/

(11) Caso Loomis v. Wisconsin 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017), https://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/

B) Syri y Robodebt

En su lucha contra el fraude, el gobierno holandés ha cruzado la información personal de los residentes en muchas bases de datos. Este sistema, denominado SyRI (Systeem Risico Indicatie, ***SyRI,*** que significa «indicación de riesgo del sistema»), pretendía prevenir y combatir el fraude, a través de identificar «perfiles de ciudadanos poco probables» que requirieran un examen más detenido. En definitiva, se trata según LAZCOS MORATINOS Y CASTILLO PARRILLA (2020) de un «sistema de procesado de datos en masa» con el objetivo de prevenir y combatir el fraude a la seguridad social. Según los mismos autores, el funcionamiento de SyRI se basa en la agregación (previa anonimización), triangulación y posterior análisis de grandes cantidades de datos (detallados en el párrafo 4.17 de la sentencia y de los que daremos cuenta más adelante) en poder de diversas administraciones públicas[12].

El sistema se basaba en la asignación del nivel de riesgo de que una determinada persona cometa fraude en los fondos públicos, en función de una serie de parámetros analizados y relacionados entre sí. El sistema se había configurado a partir de la denominada Ley de Organización de Implementación y Estructura de Ingresos (Wet structuur uitvoeringsorganisatie en inkomen, SUWI), cuyo artículo 65.2 permite la elaboración de informes de riesgos para evaluar el riesgo de que una persona física o jurídica haga un uso ilegal de fondos gubernamentales en el campo de la seguridad social y los esquemas relacionados con los ingresos públicos[13].

El sistema funcionaba del siguiente modo: si un organismo público (por ejemplo, los ayuntamientos, el banco de la Seguridad Social o la Agencia Tributaria) detectaba fraude con prestaciones, subsidios o impuestos en un barrio determinado, podía utilizar SyRI. SyRI determinaba qué residentes locales merecían una investigación más a fondo. Para calcular posibles irregularidades, los algoritmos enlazan todos los datos personales de sus residentes almacenados por instancias gubernamentales. La aplicación procesaba datos personales pseudoanonimizados, de todo tipo sobre el individuo, incluidos datos de endeudamiento, antecedentes penales, salud, etc., y de ella se extraían una serie de conclusiones sobre el nivel de riesgo de la persona[14]. Esos datos se comparan luego con el perfil de riesgo creado a partir de la información de otros ciudadanos que sí han delinquido. Observadas las similitudes, se confecciona una lista de nombres que las autoridades pueden conservar hasta dos años.

---

(12) LAZCOZ MORATINOS, G., & CASTILLO PARRILLA, J. A. (2020). Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI. Revista Chilena De Derecho Y Tecnología, 9(1), 207-225. https://doi.org/10.5354/0719-2584.2020.56843

(13) LLANO ALONSO, F. H. (Director). (2022). Inteligencia Artificial y Filosofía del Derecho. Murcia. España: Ediciones Laborum.

(14) GONZÁLEZ-ESPEJO, M. J., «Sector público y algoritmos: Transparencia o un poco más de paciencia», 19-2-2020 Diario la Ley, Consultado el 25 de junio de 2023. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyNDEyMTNTK0stKs7Mz7M1MjACCVqq5eWnpIa4ONuW5qWkpmXmpaaAlGSmVbrkJ4dUFqTapiXmFKeqpSbl52ejmBQPMwEAZnEi5GMAAAA=WKE

Esta práctica suscitó la oposición de la Autoridad Neerlandesa de Protección de Datos y del Consejo de Estado, que expresaron su preocupación por el derecho a la intimidad, así como por los derechos procesales, como la presunción de inocencia. Además, el sistema carecía de transparencia (ya que sus algoritmos no se publicaron y no se sometió a una auditoría técnica), y su selección de barrios desfavorecidos podría equivaler a una discriminación socioeconómica o por la condición de inmigrante. Además, SyRI se ha utilizado sobre todo en barrios de renta baja. Si el gobierno utiliza exclusivamente el análisis de riesgo de SyRI en barrios de alto riesgo, no es de extrañar que encuentre allí más personas de alto riesgo.

En 2020, el Tribunal de La Haya[15] ordenó la paralización inmediata de SyRI, al concluir que la legislación por la que se establecía proporcionaba una protección insuficiente contra la intromisión en la vida privada, debido a las medidas desproporcionadas adoptadas para prevenir y castigar el fraude en aras del bienestar económico. El tribunal concluyó que SyRI violaba el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH), que protege el derecho al respeto de la vida privada y familiar[16] por ausencia de proporcionalidad y transparencia.

Sobre esto último apunta COTINO (2020)[17] que a pesar de las muchas garantías que incluía el sistema, se consideran insuficientes, por no ir acompañadas de transparencia. En igual sentido, LAZCOS MORATINOS Y CASTILLO PARRILLA (2020) consideran que la Corte otorga el mayor peso de su argumentación al principio de transparencia. El sistema incluía garantías de anonimización, división funcional, borrado y de confidencialidad. En su artículo, COTINO describe las fases de reco-

(15) Nota de prensa de la sentencia por el Poder Judicial Holandés. Consultado el 25 de junio de 2023. Disponible en: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-wetgeving-in-strijd-met-het-Europees-Verdrag-voor-de-Rechten-voor-de-Mens.aspx
Sentencia Autoridad Tribunal de Distrito de La Haya 05-02-2020 ECLI:ES: RBDHA: 2020:865; Número de caso C-09-550982-HA SA 18-388; En inglés: ECLI:NL:RBDHA: 2020:1878. Consultado el 25 de junio de 2023. Disponible en: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:865

(16) DE LA ROSA Esteban, FERNANDO (Director), VERDEGAY GALDEANO José Luis, ZELEZNIKOW John, RUIZ RESA Josefa Dolores, MORAL SORIANO Leonor, FERNÁNDEZ-FÍGARES María José, VALLS PRIETO Javier, PELTA MOCHCOVSKY David Alejandro, CABRERA CUEVAS Marcelino, CASTILLO PARRILLA José Antonio, CORTÉS Pablo y VILALTA NICUESA Aura Esther, Justicia Digital. Guía para el diálogo sobre el diseño y uso eficiente, de calidad y ético de herramientas tecnológicas en la justicia civil, Madrid, Fundación Cotec para la Innovación – Universidad de Granada, 2022.
En el contexto de este procedimiento, el relator especial Philip Alston emitió un informe afirmando que tiene un efecto discriminatorio y estigmatizador. P. Alston, debido, entre otras razones, a la autoridad que se confiere a los algoritmos. «Brief by the United Nations Special Rapporteur on extreme poverty and human rights as amicus curiae before the District Court of The Hague on the case of NJCM c.s./De Staat der Nederlanden (SyRI), case No. C/09/550982/HA ZA 18/388», 2019, disponible en https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf

(17) COTINO HUESO, L. (2020). «SyRI, ¿a quién sanciono?»: Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020. La Ley privacidad, (4), 2020.

pilación, tratamiento y borrado de los datos. A pesar de todo ello el tribunal echa en falta «una revisión exhaustiva de antemano ni una revisión por un tercero independiente [...] con el fin de evaluar si es necesaria o no la restricción», esto es, la necesidad de una evaluación de impacto.

Si bien, la carencia más grave para la sentencia, y que lleva a considerar que las muchas garantías fueran insuficientes, son los problemas de caja negra y opacidad de SyRI, así como la falta de información a los interesados cuyos datos se tratan. El principio de transparencia es el principio rector de la protección de datos subyacente y consagrado en la Carta y el RGPD (6.87). El tribunal, en ausencia de normas europeas o nacionales que obliguen a desvelar el código fuente que permitieran un mejor control sobre el mismo, o que restrinjan estos usos de la informática en caso de que pueda sospecharse la existencia de estos riesgos, directamente acude al Convenio Europeo de Derechos Humanos (CEDH) y a la protección que el mismo hace sobre la intimidad de las personas para fundamentar la prohibición del uso de la herramienta (COTINO HUESO, 2020).

El tribunal considera que la normativa no responde al «justo equilibrio» que debe existir en virtud del CEDH entre el interés social al que sirve la legislación y la invasión de la vida privada que constituye la legislación para poder hablar de una invasión suficientemente justificada de la vida privada (6.7). Y es plausible que, en ausencia de una protección suficiente y transparente del derecho al respeto de la vida privada, se produzca un «efecto amedrentador» (6.5).

Respecto a la oscuridad y opacidad, la sentencia afirma que *«el modelo de riesgo que se está utilizando actualmente y los indicadores de riesgo que constituyen este modelo de riesgo son "secretos" [...] ni son conocidos por los interesados». (6.65). El sistema «de ninguna manera proporciona información sobre los datos fácticos que pueden demostrar la presencia de una determinada circunstancia [...] datos objetivos que pueden justificar la conclusión de que existe un mayor riesgo» (6.87). «El Estado no ha explicado en qué información objetivamente verificable se basan estos ejemplos». (6.88) y «no proporciona información sobre el funcionamiento del modelo de riesgo el tipo de algoritmos [...] ni [...] sobre el método de análisis de riesgos aplicado» (6.89). La legislación no establece la obligación de notificar a los interesados individualmente «puerta a puerta» (6.53). Además, quienes no son considerados perfil de riesgo, no pueden saber cómo se procesaron sus datos. La «transparencia, en aras de la verificabilidad» es necesaria frente a los peligros de «exclusión o discriminación injustificadas» (6.91). El tribunal considera que no puede probar la exactitud de la posición del Estado sobre qué es exactamente SyRI. El Estado no ha hecho público el modelo de riesgo y los indicadores que integran o pueden consistir en el modelo de riesgo. Tampoco proporcionó al tribunal información objetivamente verificable en este procedimiento para permitirle revisar la opinión del Estado sobre lo que es SyRI. La razón dada por el Estado para ello es que los ciudadanos pueden ajustar su comportamiento en consecuencia. Esta es una elección consciente del Estado. (6.49).*

Los residentes de vecindarios enteros fueron puestos bajo una lupa sin que ellos siquiera supieran qué datos sensibles a la privacidad tenía SyRI sobre ellos. Cada «indicación de riesgo» se registra en un archivo que los ciudadanos pueden consultar si lo solicitan. Pero los ciudadanos no son advertidos automáticamente si SyRI los señala por riesgo de fraude, y no pueden acceder a los motivos por los que han sido señalados[18].

El caso SyRI puede también valorarse como una muestra de la relevancia del control jurisdiccional como garantía frente al uso abusivo de la IA, pero, además, es necesario un control social por parte de la ciudadanía y para ello es imprescindible, por una parte, que dicha ciudadanía tenga formación adecuada en la materia y disponga de la información precisa[19] (PRESNO LINERA 2022).

El Tribunal de Justicia considera que, en cualquier caso, la legislación SyRI no contiene garantías suficientes para concluir que es necesaria en una sociedad democrática a la luz de los fines a los que sirve dicha legislación.

Por su parte en Australia, Robodebt, fue un polémico sistema automatizado de detección de fraudes del gobierno australiano.

El Departamento de Servicios Humanos de la Seguridad Social utilizó un algoritmo de comparación de datos para comparar los ingresos registrados en el registro de Centrelink de un cliente con los datos históricos de ingresos informados por el empleador de la Oficina de Impuestos de Australia y emitió notificaciones automáticas de aumento y recuperación de deudas cada vez que se detectaban deudas. El sistema reemplazó un proceso anterior en el que los funcionarios del departamento evaluaban las discrepancias, buscaban los registros del empleador y evaluaban la precisión antes de emitir notificaciones de deuda. En definitiva, carecía de supervisión humana, no tenía base legal adecuada y se descubrió que el sistema había emitido avisos de cobro de deudas por valor de millones de dólares a miles de beneficiarios de asistencia social basándose en datos personales inexactos e información laboral errónea. Además, invertía la carga de la prueba y eran los contribuyentes los que tenían que desvirtuar avisos de cobro de deudas que eran difíciles de entender y de refutar.

En 2020, tras la creciente presión pública y dos demandas perdidas, el Gobierno australiano declaró que Robodebt era ilegal, cerró el sistema y acordó condonar 470.000 deudas con reembolsos por un valor de 721 millones de dólares. En junio de 2021, un juez de un tribunal federal aprobó el acuerdo de una demanda colectiva de Robodebt por un valor de más de 1.700 millones de dólares en beneficios eco-

(18) Algorithm Watch. How Dutch activists got an invasive fraud detection algorithm banned. Consultado el 25 de junio de 2023. Disponible en: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2016:2454&keyword=%22ECLI:NL:HR:2016:2454%22 How Dutch activists got an invasive fraud detection algorithm banned – AlgorithmWatch

(19) PRESNO LINERA, Miguel Ángel. «Derechos fundamentales e inteligencia artificial en el Estado social, democrático y digital de Derecho». El Cronista del Estado Social y Democrático de Derecho, ISSN 1889-0016, N.º 100, 2022 (Ejemplar dedicado a: Inteligencia artificial y derecho), pp. 48-57.

nómicos para aproximadamente 430.000 personas. El propio juez calificó el episodio de: «el proceso ha puesto de manifiesto un capítulo vergonzoso en la administración del sistema de seguridad social de la Commonwealth y un fracaso masivo de la administración pública» [20], [21].

C) Otros (Proyecto Sensing, HessenDATA, Edward Bridges v. South Wales Police; Glukhin v. Rusia; «iBorderCtrl: Intelligent Portable Border Control System»; Patel v. Facebook; Clearview, Uber; Deliveroo, Chatgpt y otros)

En cuanto a otras resoluciones judiciales en las que se ha realizado control judicial sobre algoritmo, podemos mencionar el Proyecto Detección de Países Bajos, analizado también hace unos cuantos años en el libro «El derecho y la inteligencia artificial» [22].

El ***Proyecto Detección (Sensing,*** en inglés) está diseñado para prevenir y detectar delitos contra la propiedad cometidos por lo que se conoce como «bandidaje móvil» en la localidad de Países Bajos, Roermond. Sin embargo, Amnistía Internacional solicitó una evaluación previa a su uso sobre la afectación a los derechos humanos y consideran que el programa tiene sesgos discriminatorios raciales automáticos de actuación policial que se reflejan en el algoritmo. Con cámaras y otros sensores, la policía vigilaba sistemáticamente a todas las personas que circulan en automóvil en Roermond y sus alrededores, reuniendo información sobre vehículos y patrones de movimiento. Los datos recogidos se procesaban después con un modelo algorítmico que calcula una «puntuación de riesgo» para cada vehículo, dato que la policía cree que informa de la probabilidad de que quien conduce y quienes viajan en el vehículo cometan un delito contra la propiedad. Uno de los indicadores usados para hacer esta valoración es si las personas a bordo del vehículo son de Europa Oriental.

El artículo 160 de la Ley de Tráfico holandesa autoriza la detención y el control de personas en cualquier lugar y en cualquier momento, sin previo aviso y sin posibilidad real de elegir si someterse o no al procedimiento. Sin embargo, dicho artículo es discutible que sea destinado a prevenir delitos, ya que esta disposición otorga a

(20) COTINO HUESO, L. (Coord.). (2024). Guía práctica: ¿Cómo abrir los algoritmos públicos? Recomendaciones para la implantación de registros de algoritmos públicos (Versión 1.0). José Manuel Calabuig, Lorenzo Cotino, Antonia Ferrer Sapena, y Enrique Alfonso Sánchez Pérez.

(21) BALLANTYNE, N. (2023, agosto 7). The harm that data do: The case of Robodebt. Medium. Consultado el 8 de julio de 2024. Disponible en: https://medium.com/@neilballantyne/the-harm-that-data-do-the-case-of-robodebt-33bb080c970b y enlace al acuerdo aprobado por el Juez Murphy, Prygodicz contra Commonwealth of Australia (n.º 2) [2021] FCA 634 (11 de junio de 2021) Consultado el 8 de julio de 2024. Disponible en: http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2021/634.html?context=1;query=Prygodicz%20v%20Commonwealth%20of%20Australia;mask_path=

(22) VV. AA., HERRERA TRIGUERO, Francisco; PERALTA GUTIÉRREZ, Alfonso; TORRES LÓPEZ, Leopoldo Salvador Uso policial de sistemas de inteligencia artificial en el ámbito comparado. El derecho y la inteligencia artificial. 2022. 24/10/2022. Editorial Universidad de Granada. 978-84-338-7049-0

la policía poderes para un objetivo diferente: controlar el cumplimiento de las normas de tráfico. Las infracciones penales objeto del proyecto Sensing no guardan relación alguna con las normas de seguridad vial. Los seguimientos del proyecto Detección, que consisten en paradas y controles basados en puntuaciones de riesgo elaboradas por el sistema policial predictivo interfieren, por tanto, en el derecho a la intimidad. Así, los hurtos a personas y en tiendas no están penados por la Ley de Tráfico, sino por el Código Penal por lo que el uso de dicha norma como cobertura frente a una injerencia puede suponer un grave abuso de poder y una interpretación problemática.

Cuando un vehículo es identificado como de alto riesgo, la policía intentará interceptarlo y comprobar los documentos de identidad de la persona que conduce y de las que viajan con ella. La legislación neerlandesa carece de salvaguardias legales adecuadas para prevenir dar el alto y registrar de forma arbitraria y discriminatoria[23]. El Tribunal Supremo de Holanda (Hoge Raad)[24] ha establecido que este proyecto que produce paradas y controles preventivos señalando sus coches por matrículas de países de Europa del Este supone una distinción basada en la nacionalidad o el origen étnico de los pasajeros, lo cual es un tratamiento desigual o discriminatorio, cuando no hay ninguna razón objetiva para parar el coche, aparte de coincidir con el perfil de nacionalidad.

Otros casos relativos al ámbito policial eran la plataforma para el «análisis» de datos ***(Hesse, plataforma «hessenDATA») o una «evaluación» de datos (Hamburgo)*** por la policía de ambos territorios y que fueron declarados inconstitucionales por la Primera Cámara del Tribunal Constitucional Federal en sentencia de 16 de febrero de 2023 (1 BvR 1547/19, 1 BvR 2634/20[25]).

La ley de Seguridad y Orden Público de Hesse y la de Procesamiento de Datos de Hamburgo autorizan a la policía a procesar los datos personales almacenados mediante análisis de datos automatizados (Hesse) o interpretación de datos automatizados (Hamburgo).

En ambas el Tribunal Constitucional ha determinado que vulneran el derecho de la personalidad en cuanto a protección de datos y autodeterminación informativa por falta de límites de la injerencia en su redacción demasiado amplia.

---

(23) AMNISTÍA INTERNACIONAL. Países Bajos: Pongan fin a los peligrosos experimentos policiales de vigilancia masiva. 29 de septiembre de 2020. En línea. [Consultado 7 de febrero de 2021]. Disponible en: https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/paises-bajos-pongan-fin-a-los-peligrosos-experimentos-policiales-de-vigilancia-masiva/

(24) Tribunal Supremo de los Países Bajos, 1 de noviembre de 2016, ECLI:NL:HR:2016:2454. Consultado el 25 de junio de 2023. Disponible en: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2016:2454&keyword=%22ECLI:NL:HR:2016:2454%22

(25) Sentencia de la Cámara Primera del Tribunal Constitucional Federal de 16 de febrero de 2023 – 1 BVR 1547/19 – – 1 BVR 2634/20 – Consultado el 25 de junio de 2023. Disponible en: https://www.bundesverfassungsgericht.de/e/rs20230216_1bvr154719.html

De conformidad con ambas leyes, los datos pueden ser objeto de un tratamiento posterior que no se ajuste a la finalidad original, así como de un tratamiento con cambio de finalidad distinta a la de su recogida, si bien se exigen disposiciones suficientemente claras para el cumplimiento del principio de limitación de la finalidad.

Asimismo, por una injerencia en derechos fundamentales considera el tribunal que debe cumplirse que estén legalmente justificables y por lo tanto la existencia de un peligro identificable y los datos de dicho peligro, esto es, un posible hecho delictivo o la sospecha de este, en cuanto a su comisión de predicción. Sin embargo, se considera que no se centra en ello, faltando la ausencia de un peligro específico requerido o un peligro identificable basados ambos en hechos suficientemente concretos y apenas habiéndose restringido el análisis y evaluación de los datos.

No obstante, ello no significa que la inconstitucionalidad sea por una prohibición absoluta, sino que «no se cumplen los requisitos constitucionales porque el concepto de práctica de Hessen no apunta desde el principio a la identificación de al menos un peligro concreto y los datos adecuados para evitar. Sin embargo, esto es necesario debido al diseño de método y datos abiertos de la autorización en la Sección 25a HSOG y la Sección 49 HmbPolDVG». De esta forma, lo que se censura, según COTINO (2023), es que las leyes de Hamburgo y Hesse permiten un uso prolongado y no específico del sistema (párr. 167), además de que se permite el uso con la finalidad de adquirir conocimientos para futuras investigaciones y procedimientos de investigación, sin un peligro concreto o particular.

En general, el Tribunal Constitucional Federal (TCF) admite el *«propósito legítimo de aumentar la eficacia de la prevención de actos delictivos graves en el contexto de la evolución de las tecnologías de la información mediante la obtención de indicios de delitos graves inminentes que, de otro modo, pasarían desapercibidos en la base de datos de la policía. [...] Las autoridades policiales se enfrentan a un volumen de datos en constante crecimiento y cada vez más heterogéneo en términos de su calidad y formato [y el conocimiento] difícilmente podría obtenerse manualmente, especialmente bajo presión de tiempo»* (párr. 52). (COTINO 2023 [26]).

Como bien explica este autor, hay que tener en cuenta diversos criterios para determinar la mayor o menor intensidad de la injerencia (párrs. 76 y ss.). Así, se distinguen elementos respecto del rastreo y análisis de datos: la mayor o menor duración del rastreo, si incluyen datos de rastreo espaciales o geográficos, si derivan perfilados de la personalidad, si se obtiene información que sirva como punto de partida para otras medidas no relacionadas con lo que motivó la intervención inicial, si hay tecnología de reconocimiento automatizado, si hay riesgos específicos de

(26) COTINO HUESO, Lorenzo. Los requisitos del Tribunal Constitucional alemán para el análisis automatizado de datos o con inteligencia artificial, que no se cumplen en España. 12 de abril de 2023. Consultado el 25 de junio de 2023. Disponible en: https://eapc-rcdp.blog.gencat.cat/2023/04/12/los-requisitos-del-tribunal-constitucional-aleman-para-el-analisis-automatizado-de-datos-o-con-inteligencia-artificial-que-no-se-cumplen-en-espana-lorenzo-cotino-hueso/

discriminación (párr. 78). También se distinguen las variantes según la «naturaleza y alcance de los datos» (párrs. 78 y ss.): la cantidad, variedad, relevancia, el origen de estos o si hay datos de redes sociales. Se recuerda que hay que ser más estrictos respecto del análisis de datos obtenidos a través de la vigilancia de domicilios particulares o registros remotos de sistemas informáticos (párr. 81). Asimismo, el TCF diferencia los impactos y restricciones según los métodos que se empleen.

Si, por el contrario, la autoridad se definiera de manera más estricta con respecto al tipo y alcance de los datos y los métodos de procesamiento permitidos y la intensidad potencial de la intervención se redujera hasta tal punto que un umbral de intervención más bajo sería constitucionalmente suficiente.

Por último, llama poderosamente la atención a COTINO (2023) que el Tribunal Constitucional impone la prohibición de sistemas de autoaprendizaje y se añaden garantías técnicas y organizativas («en cualquier caso, el principio de proporcionalidad se traduce en exigencias de transparencia, tutela jurídica individual y control de supervisión» (& 103)[27].

Allá por 2020 en el Caso ***Edward BRIDGES v. South Wales Police***[28], Ed Bridges fue el primero que desafió al uso público del reconocimiento facial en vivo o a tiempo real por parte de la policía de Gales del Sur, alegando que estaba violando los derechos a la privacidad, las leyes de protección de datos y las leyes de igualdad.

El funcionamiento cuando se implementa AFR (Reconocimiento facial automatizado) Locate, SWP (South Wales Police – Policía del Sur de Gales) el cual monta cámaras de CCTV en vehículos policiales, o en postes, sería para capturar imágenes del rostro de cualquier persona que pase dentro del alcance de la cámara. Como hemos descrito anteriormente, las imágenes digitales de los rostros de los miembros

(27) COTINO HUESO, Lorenzo. Una regulación legal y de calidad para los análisis automatizados de datos o con inteligencia artificial. Los altos estándares que exigen el tribunal constitucional alemán y otros tribunales, que no se cumplen ni de lejos en España. Revista General de Derecho Administrativo 63 (2023). Proyecto «Derecho, Cambio Climático y Big Data», Grupo de Investigación en Derecho Público y TIC; MICINN Retos «Derechos y garantías frente a las decisiones automatizadas...» (RTI2018-097172-B-C21); «La regulación de la transformación digital ...» grupo de investigación de excelencia Generalitat Valenciana «Algoritmic law» (Prometeo/2021/009, 2021-24); «Transición digital de las Administraciones públicas e inteligencia artificial» (TED2021-132191B-I00) y «Algorithmic Decisions and the Law: Opening the Black Box» (TED2021-131472A-I00), del Plan de Recuperación, Transformación y Resiliencia. Estancia Generalitat Valenciana CIAEST/2022/1.

(28) Neutral citation number: [2020] ewca civ 1058; Case No: C1/2019/2670; Court Of Appeal (Civil Division) on Appeal from the High Court of Justice Queen's Bench Division (Administrative Court) Cardiff District Registry; 11/08/2020; Edward Bridges Appellant- and - The Chief Constable of South Wales Police – and The Secretary of State for the Home Department - and the Information Commissioner the Surveillance Camera Commissioner (2) The Police and Crime Commissioner for South Wales (3) consultado el 25 de junio de 2023. Disponible en: https://www.judiciary.uk/wp-content/uploads/2020/08/r-bridges-v-cc-south-wales-ors-judgment.pdf Toda la documentación del caso puede consultarse aquí: https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/

del público se toman de las transmisiones de CCTV (circuito cerrado de televisión) y se procesan en tiempo real para extraer información biométrica facial. Luego, esa información se compara con la información biométrica facial de las personas en una lista de vigilancia preparada para el propósito de ese despliegue específico (12). AFR Locate es capaz de escanear 50 caras por segundo (aunque eso no significa necesariamente 50 personas diferentes). Más allá de esas limitaciones técnicas, no hay límite en la cantidad de personas a las que se les pueden capturar sus datos biométricos faciales durante un despliegue determinado. La intención de la Policía del Sur de Gales durante cada implementación es permitir que AFR Locate procese a tantas personas como sea posible. Está claro que el número de personas procesadas es muy grande. Durante los 50 despliegues que se llevaron a cabo en 2017 y 2018, es posible que se hayan escaneado alrededor de 500 000 rostros. La gran mayoría de las personas cuyos datos biométricos son capturados y procesados por SWP utilizando AFR Locate no son sospechosas de ningún delito, no son de interés para la policía y se habría obtenido sin su consentimiento (16).

El uso de la tecnología de reconocimiento facial automático implica la recopilación, el procesamiento y el almacenamiento de una amplia gama de información, incluidas (1) imágenes faciales; (2) rasgos faciales (es decir, datos biométricos); (3) metadatos, incluidos el tiempo y la ubicación, asociados con el mismo; y (4) información sobre coincidencias con personas en una lista de vigilancia (21).

En el primer desafío legal del mundo contra el uso policial de esta tecnología se argumentó que la fuerza estaba violando los derechos a la privacidad, las leyes de protección de datos y las leyes de igualdad.

En agosto de 2020, el Tribunal de Apelación revocó la decisión de septiembre de 2019 del Tribunal Superior y consideró que el uso de la tecnología de reconocimiento facial por parte de la Policía de Gales del Sur infringe los derechos de privacidad, las leyes de protección de datos y las leyes de igualdad debido a «deficiencias fundamentales» en el marco legal.

En cuanto al marco legal suficiente, se considera una excesiva discrecionalidad. Asimismo, se considera que la DPIA (Data Protection Impact Assestment, evaluación de impacto de protección de datos) no contenía una evaluación de la privacidad (evaluación de impacto, evaluación de riesgos y mitigación de estos), los datos personales y las garantías. Respecto a las deficiencias, la Evaluación de impacto no consideró adecuadamente los riesgos para los derechos y libertades de los interesados y no abordó las medidas previstas para valorar los riesgos derivados de las deficiencias. Por último, se estimó que la Evaluación de impacto de igualdad de la Policía del Sur de Gales era obviamente inadecuada y se basaba en un error de derecho (no reconocer el riesgo de discriminación indirecta) y el enfoque posterior para la evaluación de la posible discriminación indirecta derivada del uso de AFR es defectuoso.

Para una mayor profundización en materia de reconocimiento facial y búsqueda entrecruzada e inteligente datos, COTINO realiza un análisis en profundidad men-

cionando creo que la totalidad de casos alrededor del mundo de estos sistemas que han acabado ante las autoridades de control o tribunales (Alemania, Brasil, Argentina, Italia, Suecia, etc.)[29].

Continuando con reconocimiento facial, ya podemos encontrar una sentencia en el Tribunal de Derechos Humanos de Estrasburgo, que aborda esta temática, el caso **GLUKHIN contra Rusia**, solicitud no. 11519/20 de 4 de julio de 2023.

El asunto se refiere a la condena administrativa del demandante por su no notificar a las autoridades su intención de celebrar una manifestación en solitario utilizando un «objeto rápidamente (des)montado» (una figura de cartón). Durante la investigación, la policía utilizó tecnología de reconocimiento facial para tratar los datos personales del demandante. Desde 2017 y 2018 se llevan instalando cámaras tanto en Moscú como en el metro de dicha ciudad. Para el 1 de septiembre de 2020, todas las cámaras de CCTV de Moscú —había ya unas 175.000 y más de 220.000 en 2022— estaban equipadas con tecnología de reconocimiento facial en directo.

El 12 de agosto de 2019 un activista político, el Sr. Konstantin Kotov, fue detenido y acusado de infracción administrativa reiterada de las normas sobre «actos públicos» por viajar en el metro de Moscú con una figura de cartón a tamaño real del Sr. Kotov sosteniendo una pancarta que decía: *«debes estar de coña. Soy Konstantin Kotov. Me enfrento a cinco años [de cárcel] en virtud del [artículo] 212.1 por protestas pacíficas»*. Unos días después habría sido arrestado en virtud del uso de reconocimiento facial en el metro. El demandante fundamenta su queja en que las actividades de búsqueda que se utilizaron de reconocimiento facial no tienen un soporte legal para el caso de infracciones administrativas pues únicamente se permiten para delitos graves, desaparecidos o prófugos y motivos de seguridad nacional, así como una vulneración de la libertad de expresión y alegación de detención ilegal. También recabaron y almacenaron del canal de Telegram del demandante imágenes y vídeos de dicha protesta para posteriormente utilizarlas en el sistema de reconocimiento facial. De igual manera sostiene que no hay decisión judicial que autorice la recolección, almacenamiento y uso de sus imágenes para la detención y para su validez como prueba.

El Tribunal recuerda que la grabación o filmación de una persona en lugares públicos no tiene por qué ser necesariamente una injerencia en la vida privada, existen casos anteriores donde se ha recogido y almacenado datos personales por autoridades y se ha declarado una vulneración de derechos. En el presente caso el tribunal debido a la dificultad probatoria de uso de reconocimiento facial por el demandante, así como la ausencia de explicación de detención en tan corto tiempo y un reconocimiento implícito de la Federación rusa del uso de dicha tecnología, se

(29) VVAA Francisco BALAGUER CALLEJÓN y Lorenzo COTINO HUESO, DERECHO PÚBLICO DE LA INTELIGENCIA ARTIFICIAL. Colección: Obras Colectivas 27. Editado por la Fundación Manuel Giménez Abad. Zaragoza, 2023. ISBN: 978-84-127016-0-9. COTINO HUESO, Lorenzo. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos.

considera que se ha utilizado el reconocimiento facial para la detención y que ello supone una injerencia en la vida privada. Así, la utilización de reconocimiento facial, en un primer lugar para la identificación a partir de fotografías y vídeos tomados de Telegram, y en segundo lugar para su localización y detención se considera vulnerador de los derechos humanos.

En el contexto de la recogida y el tratamiento de datos personales, por tanto, es esencial disponer de normas claras y detalladas que regulen el alcance y la aplicación de las medidas, así como salvaguardias mínimas relativas, entre otras cosas, a la duración, el almacenamiento, el uso, el acceso de terceros y los mecanismos para preservar la integridad y confidencialidad de los datos y los procedimientos para su destrucción, proporcionando garantías suficientes contra el riesgo de abuso y arbitrariedad (véanse S. y Marper, antes citada, § 99, y P.N. c. Alemania, no. 74440/17, § 62, 11 de junio de 2020).

En el presente caso el tribunal tiene serias dudas de la calidad de la ley y de dichas normas que sean claras y suficientemente detalladas. De igual manera se considera que afectando a la libertad ideológica lo que es un dato especialmente sensible, y no constituyendo infracción penal, el principio de necesidad decae en cuanto que no se trata de una injerencia necesaria en la sociedad democrática. De esta manera, no se trata de censurar el uso de esta tecnología de identificación y localización en supuestos de crimen organizado o terrorismo, sino si el uso de esta tecnología en este caso concreto fue proporcionado. Tratándose de unas tecnologías tan intrusivas se requiere un nivel muy alto de justificación debiendo valorar la naturaleza y gravedad de los hechos.

Por todo ello, se considera que la utilización de estas tecnologías puede tener un efecto amedrentador en la libertad de expresión y manifestación y no es compatible en este caso con una sociedad democrática.

Hay que recordar que, si bien la Federación rusa se salió del convenio el 16 de septiembre de 2022, a la vista de que los hechos ocurrieron con anterioridad el Tribunal de Estrasburgo es competente para conocer.

El caso «**iBorderCtrl: Intelligent Portable Border Control System**»[30] aborda la aplicación de sistemas inteligentes en control de fronteras, algo que en el futuro reglamento europeo se contempla como ***prohibido*** *si es para deducir las emociones de una persona física en los ámbitos de la gestión de fronteras y que se considerará* ***de alto riesgo*** *si es para evaluar un riesgo, incluido un riesgo de seguridad, un riesgo de gestión de fronteras o para supervisar, vigilar o tratar datos en el contexto de las actividades de gestión de fronteras así como para la previsión o predicción de tendencias relacionadas con los movimientos migratorios y el cruce de fronteras*.

La Agencia Ejecutiva Europea de Investigación (REA) subvencionó el proyecto iBorderCtrl como destinado a experimentar con aquellas nuevas tecnologías en los

(30) Sentencia del Tribunal General (Sala Décima) de 15 de diciembre de 2021. Patrick Breyer contra Agencia Ejecutiva Europea de Investigación. Asunto T-158/19

escenarios de gestión controlada de fronteras («controlled border management scenarios») que podrían incrementar la eficacia de la gestión de las fronteras exteriores de la Unión Europea, así como garantizar la gestión más rápida de los viajeros de buena fe y una detección más rápida de las actividades ilegales. El 5 de noviembre de 2018, el demandante, el Sr. Patrick Breyer, presentó solicitud de acceso a la documentación del proyecto, concediéndose acceso por la Agencia a un documento, parcial a varios y denegándose a otros. Así, el fondo del asunto es la transparencia y el acceso a la documentación del sistema inteligente de control de fronteras, algo bien parecido al caso BOSCO, planteado por Civio ante la Audiencia Nacional y que posteriormente analizaremos. En la decisión impugnada, para fundamentar la denegación de acceso a los documentos en cuestión, la REA invocó la protección de los intereses comerciales y el Tribunal de Luxemburgo considera que alguno de los documentos no tiene propiamente una plusvalía o el valor comercial que se aduce, no constituye información comercial sensible, de modo que su divulgación no puede conferir una ventaja a los competidores de los miembros del consorcio ni explica cómo la divulgación podría perjudicar concreta y efectivamente a la reputación de los miembros del consorcio. Asimismo, tampoco se justifica el no poder acceder al currículum vitae detallado del consejero de ética externo y su escrito de aceptación de las tareas encomendadas por el consorcio, sin que se haya ofrecido la posibilidad de su acceso incluso de manera anonimizada ni por qué no se puede acceder a dicha información.

En igual sentido el TJUE considera que la REA no justifica la denegación de acceso a la elaboración de la metodología de las investigaciones o la metodología de evaluación de los datos obtenidos de este modo y las conclusiones que se extrajeron tratándose los procedimientos de vigilancia de fronteras de un asunto público. Tampoco queda justificada la denegación de acceso a las soluciones tecnológicas, a las técnicas, tecnologías o la arquitectura global del sistema. Tampoco se justifica el carácter sensible de la documentación relativa a un plan de comunicación y divulgación.

Sí que por el contrario se considera que puede afectar a los intereses comerciales la información relativa al plan de gestión de calidad, el documento que describe con detalle, en particular, la estructura de la gestión de la calidad del proyecto y el reparto de las responsabilidades entre distintas personas y órganos del consorcio, las metodologías, los criterios y los procedimientos diseñados para evaluar la calidad de los resultados del proyecto por lo que respecta a sus distintos componentes, como los indicadores clave de rendimiento, la gestión de riesgos, la estrategia desarrollada por los miembros del consorcio para realizar el proyecto en cuestión, incluida la descripción minuciosa de las tareas llevadas a cabo en el correspondiente período y el reparto de las tareas entre los miembros, así como las metodologías diseñadas para seguir ese estado de progreso.

Habida cuenta de lo anterior, procede por el Tribunal estimar la primera parte del primer motivo en la medida en que se refiere a la denegación de acceso íntegro

al documento D 1.3, a la denegación de acceso parcial a los documentos D 1.1,D 1.2, D 2.1, D 2.2 y D 2.3, y a un acceso más amplio a los documentos D 3.1, D 7.3 y D 7.8, y desestimarla por lo que respecta a la denegación de acceso a los documentos D 8.1, D 8.3, D 8.4, D 8.5 y D 8.7. No obstante, procede recordar que no corresponde al Tribunal actuar en lugar de la REA e indicar concretamente las partes de los documentos a las que debería haberse concedido acceso parcial, sino que la agencia está obligada, al ejecutar la presente sentencia a tomar en consideración los motivos expuestos al respecto en esta resolución.

Asimismo, el Tribunal considera, al igual que el demandante, que existe interés del público en participar en un debate público, crítico y democrático acerca de si unas tecnologías de control como las controvertidas son deseables y deben ser financiadas con fondos públicos, y que ese interés debe salvaguardarse debidamente. Habida cuenta de que, no obstante, el proyecto iBorderCtrl no es más que un proyecto de investigación en desarrollo, es perfectamente posible mantener ese debate público crítico sobre los diferentes aspectos de que se trata sobre la base de los resultados de esas investigaciones divulgadas de conformidad con el Programa Horizonte 2020.

Asimismo, según la jurisprudencia, el interés público en la transparencia no tiene el mismo peso cuando se trata de la actividad administrativa de la institución de que se trate, en cuyo marco se inscriben, en el caso de autos, los documentos solicitados, que cuando se trata de su actividad legislativa y procede anular la decisión impugnada en la medida en que la REA no se pronunció sobre la solicitud de acceso del demandante a los documentos relativos a la autorización del proyecto iBorderCtrl y denegó el acceso íntegro al documento D 1.3 y el acceso parcial o un acceso más amplio a los documentos D 1.1,D 1.2, D 2.1, D 2.2, D 2.3, D 3.1, D 7.3 y D 7.8, y desestimar el recurso en todo lo demás.

Debemos mencionar en materia de decisiones judiciales sobre inteligencia artificial y más aún reconocimiento facial, aunque en un ámbito privado, uno de los primeros casos, en el año 2019, el denominado ***Patel v. Facebook*** [(31)]. Según Global Expression Freedom[(32)], en 2010, Facebook comenzó a utilizar la tecnología de reconocimiento facial para desarrollar su función de sugerencias de etiquetas, sin el consentimiento previo y por escrito de los usuarios, y sin un cronograma de conservación de la información biométrica. La tecnología que aplicó Facebook escaneaba las fotografías y a partir del análisis de los puntos fundamentales biométricos,

(31) United States Court of Appeals for the Ninth Circuit, Nimesh Patel, Individually and on Behalf of All Others Similarly Situated; Adam Pezen; Carlo Licata, Plaintiffs-Appellees, v. FACEBOOK, INC., Defendant-Appellant.No. 18-15982 D.C. No. 3:15-cv-03747-JD. Consultado el 25 de junio de 2023. Disponible en: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/11/Patel-v-Facebook.pdf Toda la documentación puede consultarse aquí:
https://epic.org/documents/patel-v-facebook/

(32) Global Expression Freedom. Columbia University. Consultado el 25 de junio de 2023. Disponible en: https://globalfreedomofexpression.columbia.edu/cases/patel-v-facebook/?lang=es

y su comparación en la base de datos, sugería etiquetar a ese usuario en particular en la fotografía.

Tres usuarios de Facebook en Illinois presentaron una demanda en 2015, alegando que la tecnología de reconocimiento facial invadía su privacidad, en cuanto que Facebook recopiló los datos biométricos de los usuarios en secreto y sin consentimiento.

Así, la sección 15(b) de la Ley de Privacidad de la Información Biométrica (BIPA, por sus siglas en inglés) establece que ninguna entidad privada puede recopilar, capturar, comprar, recibir u obtener de otra manera, el identificador o información biométrica de una persona o cliente, a menos que se informe por escrito al sujeto sobre la recopilación o almacenamiento, así como deberá informarse de un propósito específico y el plazo.

El Tribunal describió las amenazas a la privacidad planteadas por la tecnología de reconocimiento facial de Facebook y señaló que invade los asuntos privados e intereses concretos de un individuo y la tecnología le permite a Facebook identificar a usuarios individuales, sus ubicaciones y sus amigos, y que en el futuro esto podría permitir la identificación de personas a partir de fotografías de vigilancia. Ello se considera por el tribunal como un perjuicio concreto e identificable.

El Tribunal confirmó la decisión del Tribunal de Distrito de los Estados Unidos para el Distrito Norte de California, al considerar que la tecnología de reconocimiento facial de Facebook afectó la privacidad y los asuntos personales de los usuarios y señaló el impacto que los avances tecnológicos pueden tener en la privacidad.

Otro ámbito privado de uso de reconocimiento facial es el de la empresa ***Clearview. AI.*** El 10 de febrero de 2022, el Garante Italiano de Privacidad[33] impuso a esta empresa norteamericana una prohibición de cualquier recopilación posterior, mediante técnicas de web scraping, de imágenes y metadatos relevantes relacionados con personas en el territorio italiano y de un procesamiento posterior de los datos estándar y biométricos que son manejados por la compañía a través de su sistema de reconocimiento facial y para personas en territorio italiano; ordenó la supresión de los datos, incluidos los datos biométricos, procesados por su sistema de reconocimiento facial con respecto a personas que se encuentran en el territorio italiano, sujeto a la obligación de responder oportunamente a dichas solicitudes para el ejercicio de los derechos previstos en los artículos 15 a 22 del Reglamento y ordenó a la sociedad designar un representante en el territorio de la Unión Europea así como una multa récord de 20 millones de euros. El procedimiento se inició a raíz de informes de prensa y cuatro denuncias de particulares y 2 informes de asociaciones de privacidad. Y como veremos no es el único, ya que autoridades de privacidad de 5 países europeos abrieron expedientes, así como Canadá. Si bien analizaremos some-

(33) Ordinanza ingiunzione nei confronti di Clearview AI – 10 de febrero de 2022 [9751362]. Consultado el 25 de junio de 2023. Disponible en: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362

ramente todas ellas, no obstante, nos centraremos más en las decisiones y transacciones judiciales al respecto que se han producido.

Clearview es un motor de búsqueda de reconocimiento facial con una base de datos —que afirman— de más de 10 mil millones de imágenes faciales que mediante técnicas de web scraping, han sido extraídas de redes sociales (por ejemplo, Twitter o Facebook), blogs, medios de comunicación, webs de fichas policiales y, en general, de sitios web como vídeos de YouTube, las procesa algorítmicamente con técnicas biométricas para determinar su coincidencia y cuando un cliente consulta la base de datos y envía una imagen para buscar, se compara con las recopiladas. Una vez verificada la correspondencia entre las imágenes, el cliente recibe el resultado junto con una serie de metadatos y geolocalización y Clearview logra su propósito comercial al ofrecer la correspondencia entre imágenes previamente sometidas a un proceso de hashing.

Un periodista español[(34)] comprobó la base de datos ejercitando el derecho de acceso y la empresa americana le facilitó 22 fotografías y fotogramas suyos.

Por su parte la empresa norteamericana alega cumplir su legislación nacional, no someterse a la jurisdicción italiana y al RGPD y no prestaría servicios en dicho país pues no es posible el uso del servicio mediante geoblocking con inhibición de IPs europeas y ausencia de clientes en nuestro continente si bien a los europeos el ejercicio de derechos de acceso sobre sus datos. Se trataría además de un servicio destinado a fuerzas y cuerpos de seguridad de los Estados y servicios de inteligencia principalmente. Sin embargo, por ejemplo, el uso de la herramienta por la policía sueca ha sido detectado y prohibido.

La autoridad italiana recuerda en primer lugar que la disponibilidad pública de datos en Internet no implica, por el mero hecho de su carácter público, la legitimidad de su recogida por terceros. Que la recopilación y tratamiento de datos personales aún en fuentes abiertas requiere una base legal adecuada y que incluso la publicación de datos personales en Internet por parte del sujeto al que se refieren, por ejemplo, en el contexto de una red social, no implica, en sí misma, una condición suficiente para legitimar su libre reutilización por parte de terceros. Más aun cuando con el scraping los interesados suelen desconocer la utilización de sus datos o cuando las propias redes sociales suelen prohibir estas prácticas expresamente en sus términos del servicio.

El garante italiano desestima la ausencia de sujeción al reglamento europeo debido a prácticas comerciales dirigidas a Europa, derecho de acceso a ciudadanos europeos, transferencias internacionales de datos y clientes europeos, al igual que desestima la no consideración de la empresa como responsable del tratamiento, la

(34) PEREZ COLOMÉ, Jordi. 2021. La empresa que almacena fotos suyas en Internet para identificarle. 16 de junio de 2020. El País. Consultado el 1 de julio de 2023. Disponible en: https://elpais.com/tecnologia/2020-06-16/la-empresa-que-almacena-fotos-tuyas-en-internet-para-identificarte.html

ausencia de interés legítimo y le señala las violaciones del RGPD supra mencionadas imponiéndole la multa récord de 20 millones de euros.

A su vez, la autoridad sueca [35] de protección de datos reprocha a las autoridades policiales suecas haber utilizado Clearview sin garantizar su constitucionalidad, sin cumplir el principio estricto de necesidad, ni realizar evaluación de impacto. Por ello se impone una multa de 2.5 millones de coronas suecas y las obligaciones de informar a los interesados y eliminar sus datos antes del 15 de septiembre de 2021.

A su vez se abrieron expedientes en Francia, Reino Unido [36], Australia [37], Grecia o Canadá [38]. En el caso de Grecia [39], se impuso una multa de 20 millones de dólares, la más alta hasta ese momento, y 7.5 millones en Reino Unido.

La CNIL [40] determinó que se habían cometido dos infracciones del RGPD al realizar tratamientos de datos biométricos sin una base jurídica pues no podría basarse en el interés legítimo de la compañía, dado que el tratamiento resulta «particularmente intrusivo». Por otra parte, la CNIL determinó que se habían infringido también los arts. 12, 15 y 17 del RGPD, ya que había decidido limitar el derecho de acceso a la información recabada durante los doce meses anteriores a la fecha de la solicitud, así como la restricción del ejercicio de este derecho a dos veces al año, sin justificación ni motivación alguna.

En su decisión, la Autoridad Francesa de Protección de Datos no impone una sanción económica, pero ordena a la empresa que, en el plazo de dos meses, cese en la recogida y uso de datos personales en territorio francés y que facilite de forma completa los ejercicios de derechos que le han sido solicitados por parte de los interesados.

(35) Decisión de la autoridad sueca de protección de datos de 10 de febrero de 2021. 2719/2020 Consultado el 1 de julio de 2023. Disponible en: https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf

(36) PETERSON, A. (2022, May 23). UK data authority fines Clearview AI more than £7.5m, orders UK data deleted. Government Briefs. The record. Consultado el 1 de julio de 2023. Disponible en: https://therecord.media/clearview-ai-ico-fine-uk-data-delete

(37) Clearview AI breached Australians' privacy. 3 de noviembre de 2021. Consultado el 1 de julio de 2023. Disponible en: https://www.oaic.gov.au/newsroom/clearview-ai-breached-australians-privacy

(38) Clearview AI ordered to comply with recommendations to stop collecting, sharing images. 14 diciembre de 2021. Consultado el 1 de julio de 2023. Disponible en: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/

(39) Decisión autoridad helénica protección datos 35/22 de 13 de julio. Consultado el 1 de julio de 2023. Disponible en: https://www.homodigitalis.gr/wp-content/uploads/2022/07/HellenicDPA_ClearviewDecision_13.7.2022_.pdf

(40) Décision n.º MED-2021-134 du 26 noviembre 2021 CLEARVIEW AI. Consultado el 1 de julio de 2023. Disponible en: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044499030?init=true&page=1&query=CLEARVIEW&searchField=ALL&tab_selection=

La inteligencia artificial ya está transformando la justicia, y este libro ofrece una mirada integral, rigurosa y comparada sobre ese cambio.

Desde un enfoque comparado y global, **analiza tanto el control judicial de algoritmos como una ruta global de herramientas tecnológicas incorporadas a los distintos sistemas judiciales del mundo.**

A través del estudio de jurisprudencia internacional, el lector descubrirá cómo los tribunales están respondiendo al reto de garantizar derechos y libertades frente a algoritmos potencialmente discriminatorios, sesgados o carentes de control humano, especialmente en aquellos ámbitos de alto riesgo. En este contexto, se subraya el papel esencial del Poder Judicial en su papel de garante del estado democrático y de derecho frente a los desafíos que plantean las decisiones automatizadas, en un contexto en el que la gobernanza algorítmica y el compliance tecnológico se convierten en exigencias ineludibles.

La obra aborda la necesidad de evolucionar hacia una verdadera inteligencia de negocio en la justicia y el potencial de las políticas de datos abiertos. Se introduce el concepto de «análisis de contexto» y se propone un modelo estructurado para abordar con éxito los procesos de transformación digital en la justicia y aplicable a cualquier sector.

Pero este libro no se detiene en el diagnóstico, el análisis, el estudio o la comparación. Propone. **Con una marcada vocación práctica, se formulan 40 soluciones rupturistas de mejora de transformación digital de justicia, construidas a partir de la experiencia práctica tan singular del autor** —como magistrado en activo— y al mismo tiempo miembro de la CEPEJ del Consejo de Europa, consultor de la UNESCO, experto de la Comisión Europea o formador de jueces y magistrados de poderes judiciales de medio mundo (Unión Europea, Iberoamérica, Oriente Próximo y África).

Con una clara vocación práctica, esta obra aspira a convertirse en un manual de referencia para jueces, fiscales, abogados y operadores jurídicos, sobre la denominada «jurisprudencia algorítmica» y anticipando los retos que, de forma creciente, llegarán a los tribunales en los próximos años.

Si existe una obra para transformar y revolucionar la Justicia en España y en el mundo iberoamericano, es esta.

En definitiva, **un libro que busca construir una justicia más eficiente, transparente y sólida, al servicio de un Estado de Derecho reforzado en la era digital.**

ISBN: 979-13-88078-39-2

LA LEY