

VIGILANCIA BIOMÉTRICA MASIVA, INTELIGENCIA ARTIFICIAL Y DERECHOS FUNDAMENTALES

FRANCISCO BALAGUER CALLEJÓN/ LEIRE ESCAJEDO SAN-EPIFANIO
Directores



Dykinson, S.L.



Colección
IA, Robots, y Bioderecho

**VIGILANCIA BIOMÉTRICA MASIVA,
INTELIGENCIA ARTIFICIAL
Y DERECHOS FUNDAMENTALES**

Colección IA, ROBOTS, Y BIODERECHO

Directores

FRANCISCO LLEDÓ YAGÜE
Catedrático de Derecho Civil de la Universidad de Deusto

IGNACIO BENÍTEZ ORTÚZAR
Catedrático de Derecho Penal de la Universidad de Jaén

CRISTINA GIL MEMBRADO
Profesora Titular de Derecho Civil de la Universidad de las Islas Baleares

ÓSCAR MONJE BALMASEDA
Profesor Titular de Derecho Civil de la Universidad de Deusto

Coordinadores

M^a JOSÉ CRUZ BLANCA
Profesor titular de Derecho Penal de la Universidad de Jaén

IGNACIO LLEDÓ BENITO
Profesor Derecho Penal de la Universidad de Sevilla. Profesor titular acreditado (ANECA)

Comité científico

LORENZO MORILLAS CUEVA
Catedrático de Derecho Penal de la Universidad de Granada

MANUEL MARCHENA GARCÍA
Presidente de la Sala Segunda del Tribunal Supremo

PILAR FERRER VANRELL
Catedrática de Derecho Civil de la Universidad de las Islas Baleares

JOSÉ ÁNGEL MARTÍNEZ SANCHIZ
Notario. Académico de “número” de la Real Academia de Legislación y Jurisprudencia

VICTORIO MAGARIÑOS BLANCO
Notario y miembro de la Comisión General de Codificación

PIERRE LLUIGI D'ELLOSO
Fiscal General de la República Emérito. Fiscal Nacional Antimafia (Italia)

ALICIA SÁNCHEZ SÁNCHEZ
Magistrado-Juez Registro Civil de Bilbao

LUCÍA RUGGERI
Professore ordinario di Diritto privato presso Università degli Studi di Camerino

CARMEN OCHOA MARIETA
Directora médica ura, Cer.Santander,S.L, Medicina de la reproducción

MARIAN M. DE PANCORBO
Catedrática de Biología Celular, Coordinadora Centro de Investigación Lascaray Ikergunea / Lascaray Research Center, Investigadora Principal Grupo biomics / biomics Research Group

LUIS MARTÍNEZ LÓPEZ
Catedrático de Lenguajes y Sistemas Informáticos de la Universidad de Jaén

HUMBERTO NICANOR BUSTINCE SOLA
Catedrático de Ciencias de la Computación e Inteligencia Artificial de la Universidad Pública de Navarra

**VIGILANCIA BIOMÉTRICA MASIVA,
INTELIGENCIA ARTIFICIAL
Y DERECHOS FUNDAMENTALES**

FRANCISCO BALAGUER CALLEJÓN/ LEIRE ESCAJEDO SAN-EPIFANIO

Directores

 *Dykinson, S.L.*

No está permitida la reproducción total o parcial de este libro, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sea este electrónico, mecánico, por fotocopia, por grabación u otros métodos, sin el permiso previo y por escrito del editor. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (art. 270 y siguientes del Código Penal).

Diríjase a Cedro (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra. Puede contactar con Cedro a través de la web www.conlicencia.com o por teléfono en el 917021970/932720407

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial
Para mayor información, véase www.dykinson.com/quienes_somos

Proyecto coordinado AI-BIOSURV, Biovigilancia mediante IA en la era post-COVID: corporeidad, identidad y derechos fundamentales (TED 2021 - 129975B-C21, MICINN), IPs. L. Escajedo San-Epifanio, F. Balaguer Callejón y E. Jacob Taquet.



© Copyright by
Los autores
Madrid, 2025

Imagen de cubierta: ©irstone/123RF.COM

Editorial DYKINSON, S.L. Meléndez Valdés, 61 - 28015 Madrid

Teléfono (+34) 91 544 28 46 - (+34) 91 544 28 69

e-mail: info@dykinson.com

<http://www.dykinson.es>

<http://www.dykinson.com>

ISBN: 979-13-7006-390-0

Depósito Legal: M-14207-2025

DOI: <https://doi.org/10.14679/4208>

ISBN electrónico: 979-13-7006-442-6

Preimpresión por:

Besing Servicios Gráficos S.L.

e-mail: besingsg@gmail.com

Reconocimientos:

Este trabajo se ha realizado en el marco del *Proyecto coordinado AI-BIO-SURV, Biovigilancia mediante IA en la era post-COVID: corporeidad, identidad y derechos fundamentales* (TED 2021 - 129975B-C21, MICINN), IPs. Leire Escajedo San-Epifanio, Francisco Balaguer Callejón y Eduardo Jacob Taquet. En su elaboración se han realizado dos estancias de investigación con cargo a dicho proyecto: Adoración Galera Victoria realizó una estancia de investigación de dos meses en *el Tribunal Europeo de Derechos Humanos* (Estrasburgo, Francia) y Leire Escajedo San-Epifanio realizó una estancia de investigación en *el Instituto Max-Planck de Estudio del Derecho, de la Seguridad y del Crimen* (Friburgo de Brisgovia, Alemania).



GIU24/007 *EU-Frames, Construcción de Marcos Regulatorios innovadores en la UE*, IPs L. Escajedo San-Epifanio/ I. Filibi.

Infraestructura Experimental mejorada para Investigación en 5G y 6G y servicios avanzados SN4E+ (Enhanced Smart Networks for Everything), e *Infraestructura Experimental para Investigación en 5G y 6G y servicios avanzados Smart-Nets4E* (Smart Networks for Everything), IP E. Jacob Taquet.

Secretaría Técnica:

Marta LUCENA PÉREZ. Contratada FPU del Departamento de Derecho Constitucional de la Universidad de Granada; con anterioridad investigadora contratada del proyecto Ai-Biosurv en el Departamento de Derecho Público y Ciencias Histórico-Jurídicas y del Pensamiento Político de la UPV/EHU.

María Eugenia IBÁÑEZ PÉREZ-ZAMACONA. Doctora en Antropología Biológica. Investigadora Contratada del Departamento de Derecho Público y Ciencias Histórico-Jurídicas y del Pensamiento Político de la UPV/EHU.

ÍNDICE

VIGILANCIA BIOMÉTRICA MASIVA MEDIANTE IA Y DERECHOS FUNDAMENTALES: RETOS JURÍDICO-CONSTITUCIONALES	21
<i>Leire Escajedo San Epifanio</i>	
I. BIOMETRÍAS AUTOMATIZADAS QUE AGUDIZAN EL CAPITALISMO DE VIGILANCIA Y LA SOCIEDAD RETICULAR: PLANTEAMIENTO DE LA CUESTIÓN Y CLARIFICACIÓN DE CONCEPTOS	22
II. EL DECEPCIONANTE TRATAMIENTO DE LA VIGILANCIA BIOMÉTRICA EN EL RIA Y EL RGPD	26
III. EL RECONOCIMIENTO BIOMÉTRICO ANTES DE LA IA. EN ESPECIAL, EL <i>BERTILLONAGE</i>	29
IV. CONTRA EL OLVIDO: LA PRIMERAS BIOMETRÍAS AUTOMATIZADAS Y LOS DISCURSOS CONTRA SU EXPANSIÓN A ESCENARIOS OPERATIVOS CIVILES. EL 11-S Y LA IMPOSICIÓN DEL PASAPORTE BIOMÉTRICO UE COMO PUNTOS DE INFLEXIÓN	31
V. DESAFÍOS JURÍDICOS EN LA FRONTERA ENTRE LO FÍSICO Y LO DIGITAL: RETOS PENDIENTES Y ABORDAJE DEL PROYECTO AI-BIOSURV	34
ABREVIATURAS Y ACRÓNIMOS DE USO FRECUENTE	39
ÍNDICE DE VOCES.....	45

I.- PERSPECTIVAS METODOLÓGICAS PARA EL ANÁLISIS CONSTITUCIONAL DE LA IA Y DE LA BIOVIGILANCIA AUTOMATIZADA

PERSPECTIVAS METODOLÓGICAS PARA EL ANÁLISIS CONSTITUCIONAL DE LA INTELIGENCIA ARTIFICIAL Y DE SU INCIDENCIA SOBRE LOS DERECHOS FUNDAMENTALES 55

Francisco Balaguer Callejón

INTRODUCCIÓN.....	55
I. LA TRANSFORMACIÓN DEL ENTORNO ANALÓGICO EN DIGITAL	58
II. LA CONSTRUCCIÓN DE LA SOCIEDAD DIGITAL Y LA INTELIGENCIA ARTIFICIAL GENERATIVA.....	61
III. LOS DERECHOS FUNDAMENTALES EN EL ENTORNO DIGITAL	62
CONCLUSIONES.....	65
REFERENCIAS BIBLIOGRÁFICAS	66

CONSTITUCIONALISMO Y PANÓPTICO DIGITAL ‘AMABLE’: BIOMETRÍAS AUTOMATIZADAS, PRIVACIDAD Y LIBERTAD COGNITIVA..... 69

Leire Escajedo San-Epifanio

I. LA VIGILANCIA CONTEMPORÁNEA “NO SÓLO” PERSIGUE CONTROLAR, SINO TAMBIÉN INFLUIR EN LOS COMPORTAMIENTOS DE LAS PERSONAS: RETOS CONSTITUCIONALES ANTE LA IA GENERATIVA	70
II. LA TOLERANCIA (O DIFICULTAD DE REACCIÓN) DEL ORDENAMIENTO JURÍDICO DE LA UE ANTE EL PANÓPTICO NEOLIBERAL	76
III. VIGILANCIA BIOMÉTRICA NO IDENTIFICANTE Y CAPTACIÓN DE ATENCIÓN EN EL REGLAMENTO EUROPEO DE IA: ¿NO ESTABAN EN LA AGENDA?	85
IV. BIOMETRÍAS (IDENTIFICANTES Y NO IDENTIFICANTES) Y MONITORIZACIÓN DE COMPORTAMIENTOS Y EMOCIONES: PRECISIONES CONCEPTUALES PARA UN ADECUADO TRATAMIENTO POLÍTICO-JURÍDICO	89
V. REWISEMOS CUANTO ANTES EL ESTATUTO JURÍDICO-CONSTITUCIONAL DE LA INFORMACIÓN BIOMÉTRICA Y LA PROTECCIÓN DE LA AUTONOMÍA ATENCIONAL	101
BIBLIOGRAFÍA	103

COMPETENCIA DE LA UNIÓN EUROPEA EN MATERIA DE INTELIGENCIA ARTIFICIAL Y DERECHOS FUNDAMENTALES..... 107

Augusto Aguilar Calahorra

I.	INTEGRACIÓN EUROPEA E INTELIGENCIA ARTIFICIAL.....	107
II.	LA MEJORA DEL MERCADO INTERIOR: UNA BASE JURÍDICA FIRME PARA REGULAR LA IA	111
III.	LA MEJORA DEL MERCADO INTERIOR: UNA BASE JURÍDICA DÉBIL PARA GARANTIZAR LOS DERECHOS.....	115
IV.	EL REGLAMENTO DE IA Y EL “ELEVADO NIVEL DE PROTECCIÓN” DE LOS DERECHOS FUNDAMENTALES	131
V.	LA BASE JURÍDICA DE LA IA PERMITE LA DESLEGALIZACIÓN DE LA MATERIA.....	136
	REFERENCIAS BIBLIOGRÁFICAS	143

**II. LA LUCHA GEOPOLÍTICA POR LIDERAR LA IA:
COMPARATIVA DE ESTRATEGIAS**

LA ESTRATEGIA DE LA UNIÓN EUROPEA PARA LIDERAR LA REGULACIÓN MUNDIAL DE IA CONFIABLE..... 147

Igor Filibi

I.	LA INTELIGENCIA ARTIFICIAL EN EL CONTEXTO DEL CAPITALISMO DIGITAL.....	148
II.	DE LA CARRERA POR LA IA A LA CARRERA POR REGULAR LA IA ..	150
III.	LA ESTRATEGIA DE LA UNIÓN EUROPEA.....	153
IV.	MÁS ALLÁ DE EUROPA: HACIA UNA REGULACIÓN MUNDIAL DE LA IA.....	171
V.	CONCLUSIONES	173
	REFERENCIAS.....	175
	ANEXO CRONOLOGÍA.....	178

EL DESAFÍO DE UNA IMPRESCINDIBLE REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL EN UN CONTEXTO GEOPOLÍTICO HOSTIL 189

Javier Uncetabarrenechea Larrabe

I.	INTRODUCCIÓN	190
II.	LA INFLUENCIA DEL MUNDO CORPORATIVO A LA HORA DE IMPULSAR LA CREACIÓN DE MARCOS DE REGULACIÓN FAVORABLES.....	192
III.	LA NUEVA GUERRA FRÍA ENTRE ESTADOS UNIDOS Y CHINA COMO OBSTÁCULO CLAVE A LA REGULACIÓN: EL PASO DE UNA RIVALIDAD TECNOLÓGICO-COMERCIAL A UN ENFRENTAMIENTO (CASI) TOTAL.....	200
IV.	LA DIFICULTAD A LA HORA DE ENCONTRAR UN MARCO DE COOPERACIÓN ADECUADO A ESCALA GLOBAL EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL	206
V.	LA APUESTA POR MARCOS MÁS REGIONALES DE COOPERACIÓN COMO INSTRUMENTO A LA HORA DE INFLUIR EN LA REGULACIÓN MÁS ALLÁ DE SU ÁMBITO TERRITORIAL: UNA MIRADA AL PAPEL CLAVE DE LA OCDE	216
	CONCLUSIONES.....	226
	BIBLIOGRAFÍA	228

UN ANÁLISIS DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL DESDE LA FORMA JURÍDICA DEL CONSTITUCIONALISMO ORDOLIBERAL (DIGITAL): EL TRINOMIO PODER SUPRANACIONAL DE MERCADO-DERECHO Y ESTADO REGULADOR 235

Ainhua Lasa López

I.	APROXIMACIONES PRELIMINARES A LA “PRESUNTA” DICOTOMÍA MATERIAL DEL RIA: ¿PRODUCCIÓN NORMATIVA DIGITAL ORIENTADA A LA COHABITACIÓN DERECHOS FUNDAMENTALES-MERCADO INTERIOR?.....	236
II.	EL ISOMORFISMO ESTRUCTURAL DEL CAPITAL DIGITAL Y SUS INTERRELACIONES CON EL PODER, EL ESTADO Y EL DERECHO ORDOLIBERAL.....	243
III.	EL RIA COMO CONCRECIÓN LEGAL-MATERIAL DE LA FORMA JURÍDICA ORDOLIBERAL: LA GOBERNANZA DEL MERCADO ÚNICO DIGITAL.....	248

IV.	LAS INTERRELACIONES DE LOS INTERES PÚBLICOS AXIALES, IUSFUNDAMENTALES Y DE LOS OBJETIVOS DE LA UNIÓN CON LA DECISIÓN DE SISTEMA DEL MERCADO INTERIOR.....	254
V.	CONCLUSIONES FINALES: EL ABORDAJE DE LA AUTONOMÍA PERSONAL Y EL CONTROL POLÍTICO DE LOS SISTEMAS DE IA DESDE EL CONSTITUCIONALISMO DE LOS CONFLICTOS	262
	BIBLIOGRAFÍA	263

III. INTELIGENCIA ARTIFICIAL E IDENTIFICACIÓN BIOMÉTRICA: EVOLUCIÓN REGULATORIA EN LA UE, EL COE Y EL TEDH

	INTELIGENCIA ARTIFICIAL, BIOMETRÍAS Y TUTELA DE DERECHOS A LA LUZ DEL CONVENIO MARCO DEL CONSEJO DE EUROPA Y LA JURISPRUDENCIA DEL TEDH	269
--	--	------------

Adoración Galera Victoria

I.	PREMISAS INICIALES	270
II.	BIOMETRÍAS Y DERECHOS FUNDAMENTALES.....	275
III.	EL CONVENIO MARCO SOBRE INTELIGENCIA ARTIFICIAL, DERECHOS HUMANOS, DEMOCRACIA Y ESTADO DE DERECHO.....	279
IV.	IDENTIFICACIÓN BIOMÉTRICA Y VIGILANCIA EN LA JURISPRUDENCIA DEL TEDH	287
V.	REFLEXIONES FINALES.....	296
	BIBLIOGRAFÍA	297

	EL RECONOCIMIENTO MEDIANTE BIOMETRÍAS EN EL NUEVO REGLAMENTO DE INTELIGENCIA ARTIFICIAL	301
--	--	------------

Marta Lucena Pérez

I.	INTRODUCCIÓN	302
II.	ANTECEDENTES AL REGLAMENTO DE INTELIGENCIA ARTIFICIAL EN LA UNIÓN EUROPEA.....	304
III.	REGLAMENTO UE DE INTELIGENCIA ARTIFICIAL	305
IV.	CONCLUSIONES	319
	BIBLIOGRAFÍA	322

**LA INTEGRACIÓN DEL PARADIGMA DE GESTIÓN DESCENTRALIZADA
EN LOS PROCESOS DE IDENTIFICACIÓN. UNA APROXIMACIÓN
CONSTITUCIONAL AL NUEVO ECOSISTEMA EUROPEO DE IDENTIDAD
DIGITAL..... 325**

Juan Francisco Rodríguez Gamal

I.	INTRODUCCIÓN	326
II.	LOS MODELOS DE GESTIÓN DE LA IDENTIDAD DIGITAL DESDE UNA PERSPECTIVA CONSTITUCIONAL: ACTORES E INCIDENCIA .	328
III.	LA DESCENTRALIZACIÓN EN LA GESTIÓN DE LA IDENTIDAD	333
IV.	BREVE APROXIMACIÓN AL EMERGENTE ECOSISTEMA EUROPEO DE IDENTIDAD DIGITAL	337
V.	CONSIDERACIONES FINALES	344
	REFERENCIAS BIBLIOGRÁFICAS	346

**TECNOLOGÍAS BIOMÉTRICAS Y AUTORIDADES DE PROTECCIÓN
DE DATOS..... 353**

Mónica Arenas Ramiro

I.	INTRODUCCIÓN	354
II.	EL TRATAMIENTO DE DATOS PERSONALES: LOS DATOS BIOMÉ- TRICOS.....	360
III.	LAS GARANTÍAS DEL TRATAMIENTO DE DATOS PERSONALES: LAS AUTORIDADES DE PROTECCIÓN DE DATOS	373
IV.	LOS PRONUNCIAMIENTOS DE LAS AUTORIDADES DE PROTEC- CIÓN DE DATOS.....	376
V.	A MODO DE REFLEXIÓN FINAL	397
	BIBLIOGRAFÍA	398

**LA REPERCUSIÓN DE LA INTELIGENCIA ARTIFICIAL Y LA
BIOVIGILANCIA DESDE LA PERSPECTIVA DEL CONTROL DE LA
ACTIVIDAD LABORAL DE LAS PERSONAS TRABAJADORAS 401**

J. Eduardo López Ahumada

I.	INTRODUCCIÓN	402
II.	EL DESARROLLO PARALELO DE LA IA Y LAS NUEVAS POSIBILIDA- DES DE BIOVIGILANCIA EN EL TRABAJO	402

III.	LOS RIESGOS DE LAS NUEVAS MANIFESTACIONES DE VIGILANCIA Y CONTROL DEL TRABAJO DE LA EMPRESA EN LOS DERECHOS DE LAS PERSONAS TRABAJADORAS.....	405
IV.	DECISIONES AUTOMATIZADAS, CONTROL BIOMÉTRICO Y SALVAGUARDA DE LOS DERECHOS Y LIBERTADES DE LAS PERSONAS TRABAJADORAS	410
V.	SISTEMAS DE CONTROL BIOMÉTRICO Y BIOVIGILANCIA EN EL TRABAJO: CONTROLES DE ACCESO Y REGISTRO DE JORNADA.....	412
VI.	LA ESPECIAL LIMITACIÓN DE LA MONITORIZACIÓN DE LOS DATOS DE SALUD DE LOS TRABAJADORES	423
VII.	LA PROBLEMÁTICA DEL USO DE LOS DISPOSITIVOS DIGITALES Y LA DESCONEXIÓN DIGITAL: LOS PROBLEMAS DE UN CONTROL GENÉRICO.....	424
VIII.	LA VIDEOVIGILANCIA Y GRABACIÓN DE SONIDOS: GARANTÍA DE PROPORCIONALIDAD E INTERVENCIÓN MÍNIMA.....	426
IX.	LÍMITES A LA GEOLOCALIZACIÓN PRESERVANDO LA PRIVACIDAD DE LAS PERSONAS TRABAJADORAS	429
X.	REFLEXIONES FINALES.....	432
	BIBLIOGRAFÍA	434

REFLEXIONES CONCEPTUALES SOBRE LA TRANSPARENCIA ALGORÍTMICA APLICADAS A LAS PLATAFORMAS DIGITALES PARA LA PROTECCIÓN DE LOS DERECHOS Y LA DEMOCRACIA 437

Eloísa Pérez Conchillo

I.	UNA VISIÓN PANORÁMICA DE CONTEXTO. ¿POR QUÉ LA TRANSPARENCIA ALGORÍTMICA?.....	438
II.	REFLEXIONES CONCEPTUALES: IA, ALGORITMOS Y TRANSPARENCIA ALGORÍTMICA.....	444
III.	UNA VISIÓN DE CONJUNTO SOBRE LA NORMATIVA EUROPEA EN MATERIA DE TRANSPARENCIA ALGORÍTMICA APLICABLE A LAS PLATAFORMAS DIGITALES	455
IV.	CONCLUSIONES	459
	BIBLIOGRAFÍA	461

V.- BIODETERMINACIÓN, PERFILADO Y DISCRIMINACIÓN ALGORÍTMICA

LA RESPONSABILIDAD CIVIL DERIVADA DE LOS EFECTOS DISCRIMINATORIOS EN EL PERFILADO DE LAS PERSONAS 467

María Victoria Jiménez Martínez

INTRODUCCIÓN.....	468
I. DELIMITACIÓN DE CONCEPTOS	471
II. LAS DECISIONES AUTOMATIZADAS Y EL PERFILADO DE LAS PERSONAS	474
III. LOS DAÑOS PROVOCADOS POR LA INTELIGENCIA ARTIFICIAL Y LA RESPUESTA DE LA UNIÓN EUROPEA: LA REGULACIÓN DE LA RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL EN EL ÁMBITO DE LA INTELIGENCIA ARTIFICIAL	482
IV. LA RESPONSABILIDAD CIVIL CONTRACTUAL POR DISCRIMINACIÓN ALGORÍTMICA EN EL ÁMBITO EMPRESARIAL	494
V. CONCLUSIONES	501
BIBLIOGRAFÍA	502

LA PROHIBICIÓN DE LOS SISTEMAS QUE EVALÚAN Y CLASIFICAN A LAS PERSONAS CON EFECTOS DISCRIMINATORIOS EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL 507

Miguel Ángel Presno Linera

I. INTRODUCCIÓN	508
II. EL SISTEMA DE CRÉDITO SOCIAL CHINO	512
III. EL DESARROLLO DE LOS SISTEMAS DE CALIFICACIÓN COMO UNA VÍA DE EXPANSIÓN DEL CAPITALISMO DE VIGILANCIA.....	514
IV. LA PROHIBICIÓN DE DETERMINADOS SISTEMAS QUE EVALÚAN O CLASIFICAN A LAS PERSONAS FÍSICAS	519
BIBLIOGRAFÍA	523

VI.- IDENTIFICACIÓN BIOMÉTRICA EN ESPACIOS PÚBLICOS Y CONTROL DE FRONTERAS

LA IDENTIFICACIÓN BIOMÉTRICA, LA INTELIGENCIA ARTIFICIAL Y EL EFECTO DESALIENTO EN REUNIONES Y MANIFESTACIONES..... 527

Juan Francisco Sánchez Barrilao

I.	INTRODUCCIÓN: LA DESMOVILIZACIÓN Y EL DESALIENTO AL RESPECTO DEL EJERCICIO DE DERECHOS FUNDAMENTALES EN LA SOCIEDAD DIGITAL	528
II.	LA IDENTIFICACIÓN Y VIDEOVIGILANCIA DE PERSONAS EN REUNIONES Y MANIFESTACIONES	532
III.	PROPUESTA EUROPEA DE REGULACIÓN DE LA IDENTIFICACIÓN BIOMÉTRICA MEDIANTE INTELIGENCIA ARTIFICIAL EN LUGARES DE ACCESO PÚBLICO	536
IV.	LA DESMOVILIZACIÓN COMO SENTIMIENTO Y OBJETO CONSTITUCIONAL.....	542
V.	¿HACIA UN CAMBIO DE PARADIGMAS?	546
VI.	CODA: EL RÉGIMEN DE LA IDENTIFICACIÓN BIOMÉTRICA EN LUGARES DE ACCESO PÚBLICO CONFORME EL RIA	548
	BIBLIOGRAFÍA	555

LA INTELIGENCIA ARTIFICIAL EMOCIONAL EN EL ÁMBITO MIGRATORIO Y SUS RIESGOS PARA LOS DERECHOS FUNDAMENTALES: ¿HACIA LA BIODETERMINACIÓN DE LA CREDIBILIDAD? 561

Andrea Romano

I.	INTRODUCCIÓN	562
II.	LA IA EMOCIONAL	564
III.	LA EXPERIMENTACIÓN DE LA IA EMOCIONAL EN EL CAMPO DE LA MIGRACIÓN: <i>IBORDERCTRL</i> Y PROYECTOS SIMILARES	568
IV.	EL RECONOCIMIENTO DE EMOCIONES EN EL REGLAMENTO SOBRE INTELIGENCIA ARTIFICIAL Y SU RELEVANCIA EN EL ÁMBITO MIGRATORIO	570
V.	EL RECONOCIMIENTO DE EMOCIONES Y LOS DERECHOS FUNDAMENTALES DE LOS MIGRANTES	574
VI.	CONCLUSIONES	576
	BIBLIOGRAFÍA	578

SISTEMAS EUROPEOS DE IDENTIFICACIÓN BIOMÉTRICA**EN DEFENSA, SEGURIDAD Y FRONTERAS:****SU SITUACIÓN TRAS LA APROBACIÓN DEL RIA 581**

*María Eugenia Ibáñez Pérez-Zamacona, Aline Jelenkovic,
Alaitz Poveda Zabala, Esther M. Rebato Ochoa,
Eduardo Jacob Taquet, Ixone Alonso Sanz
Leire Escajedo San-Epifanio*

I.	LOS SISTEMAS UE QUE CONTIENEN INFORMACIÓN BIOMÉTRICA Y LA ELABORACIÓN DEL RIA. EN ESPECIAL EL CONTROL DE FRONTERAS	582
II.	PREVISIONES DEL ART. 111 Y EL ANEXO X DEL RIA RESPECTO A LOS GRANDES SISTEMAS INFORMÁTICOS.....	584
III.	LOS REGLAMENTOS DE INTEROPERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN DE FRONTERAS Y DE COOPERACIÓN JUDICIAL, POLICIAL, ASILO E INMIGRACIÓN	586
IV.	SISTEMAS CON COMPONENTES BIOMÉTRICOS PREVIOS A LOS REGLAMENTOS DE INTEROPERABILIDAD: SIS, EURODAC Y VIS....	589
V.	SISTEMAS IMPULSADOS JUNTO CON LOS REGLAMENTOS DE INTEROPERABILIDAD: SES, ETIAS Y ECRIS-TCN.....	598
VI.	CONEXIONES CON OTROS SISTEMAS DE INFORMACIÓN (EUROPOL, INTERPOL, WAPIS, FRONTEX)	604
VII.	COMPONENTES QUE SERÁN NECESARIOS PARA UNA INTEROPERABILIDAD EFECTIVA Y MECANISMOS DE GARANTÍA	606
	BIBLIOGRAFÍA	609

**VII. BIOMETRÍAS EN EL ÁMBITO PENAL Y PROTECCIÓN
DE LOS DERECHOS DE LOS MENORES**

LA UTILIZACIÓN DE SISTEMAS DE BIOMETRÍA**EN EL ÁMBITO PENAL: UN ANÁLISIS DESDE LA****PERSPECTIVA DEL DERECHO CONSTITUCIONAL 615**

Amalia Lozano España

I.	INTRODUCCIÓN	616
II.	LA UTILIZACIÓN DE LA BIOMETRÍA EN EL ÁMBITO DE LA INVESTIGACIÓN Y PREVENCIÓN DE DELITOS.....	620
III.	LA DELIMITACIÓN DEL OBJETO, FUNCIONES Y OBJETIVOS LOS SISTEMAS BIOMÉTRICOS EN EL ÁMBITO PENAL	621

IV.	EL MARCO JURÍDICO SUPRANACIONAL DE REGULACIÓN DE LOS SISTEMAS DE RECONOCIMIENTO FACIAL PARA SU USO EN LAS INVESTIGACIONES Y PREVENCIÓN DE DELITOS.....	624
V.	LA REGULACIÓN DE LOS SISTEMAS BIOMÉTRICOS DE INVESTIGACIÓN, DETECCIÓN Y PREVENCIÓN DE LOS DELITOS DE RECONOCIMIENTO FACIAL EN ESPAÑA	632
	CONCLUSIONES.....	635
	BIBLIOGRAFÍA	637

	LOS MENORES FRENTE A LA INTELIGENCIA ARTIFICIAL: ALGO MÁS QUE ESPECIAL VULNERABILIDAD.....	639
--	---	------------

Luis Fernando Martínez Quevedo

I.	INTRODUCCIÓN	640
II.	PREMISA: ¿POR QUÉ “ALGO MÁS QUE” ESPECIAL VULNERABILIDAD?	642
III.	LAS PERSONAS DE MENOR EDAD Y LA INTELIGENCIA ARTIFICIAL: RIESGOS ESPECÍFICOS.....	644
IV.	CONCLUSIONES	660
	BIBLIOGRAFÍA	662

LA PROHIBICIÓN DE LOS SISTEMAS QUE EVALÚAN Y CLASIFICAN A LAS PERSONAS CON EFECTOS DISCRIMINATORIOS EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

MIGUEL ÁNGEL PRESNO LINERA

*Catedrático de Derecho Constitucional de la Universidad de Oviedo¹. ORCID:
0000-0002-0033-6159*

SUMARIO: I.- Introducción. II. El sistema de crédito social chino. III. El desarrollo de los sistemas de calificación como una vía de expansión del capitalismo de vigilancia. IV.- La prohibición de determinados sistemas que evalúan o clasifican a las personas físicas. Bibliografía.

El reciente Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (la llamada “Ley de Inteligencia”) muestra su preocupación por los sistemas de inteligencia artificial (IA en lo sucesivo) que permiten a agentes públicos o a entidades privadas realizar una puntuación ciudadana de las personas físicas atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos enteros de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente o desemboque en un trato perjudicial o desfavorable que sea injustificado o desproporcionado con respecto al com-

¹ Este trabajo es uno de los resultados del Proyecto PID2022-136548NB-I00 “Los retos de la inteligencia artificial para el Estado social y democrático de Derecho”, financiado por el Ministerio de Ciencia e Innovación en la Convocatoria Proyectos de Generación de Conocimiento 2022.

portamiento social o la gravedad de éste. Estos resultados discriminatorios menoscaban el derecho a la no discriminación y los valores de igualdad y justicia propios de un Estados social y democrático de Derecho. El ejemplo más acabado de los efectos perversos de estas herramientas es el bien conocido sistema de “crédito social chino”, que se articula sobre un régimen de recompensas y castigos (en forma de “listas rojas” y “listas negras”) mantenido por organismos gubernamentales. La inclusión en una lista puede implicar diversos beneficios (facilidades para el alquiler de una vivienda o la obtención de un préstamo), mientras que entrar en una lista negra lleva aparejadas restricciones de derechos (por ejemplo, para acceder a determinados medios de transporte).

Sin estar pensando en la introducción en la Unión Europea de sistemas similares al descrito, sí se advierte del altísimo riesgo de que se produzcan consecuencias discriminatorias, por lo que tras la entrada en vigor del Reglamento estos sistemas quedarán prohibidos en la Unión Europea, y tampoco podrán exportarse a otros países.

I. INTRODUCCIÓN

El reciente 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 incluye un considerando 31 en el extenso Preámbulo donde explica que “los sistemas de IA que permiten a agentes públicos o privados llevar a cabo una puntuación ciudadana de las personas físicas pueden tener resultados discriminatorios y abocar a la exclusión a determinados grupos. Pueden menoscabar el derecho a la dignidad y a la no discriminación y los valores de igualdad y justicia. Dichos sistemas de IA evalúan o clasifican a las personas físicas o a grupos de estas sobre la base de varios puntos de datos relacionados con su comportamiento social en múltiples contextos o de características personales o de su personalidad conocidas, inferidas o predichas durante determinados períodos de tiempo. La puntuación ciudadana resultante de dichos sistemas de IA puede dar lugar a un trato perjudicial o desfavorable de determinadas personas físicas o grupos enteros en contextos sociales que no guardan relación con el contexto donde se generaron o recabaron los datos originalmente, o a un trato perjudicial desproporcionado o injustificado en relación con la gravedad de su comportamiento social. Por lo tanto, deben prohibirse los sistemas de IA que impliquen esas prácticas inaceptables de puntuación y den lugar a esos resultados perjudiciales o desfavorables [...]”.

En otras palabras, estamos hablando de que tras la entrada en vigor del Reglamento quedarán prohibidos en el ámbito de la Unión Europea, y tam-

poco podrán exportarse a otros países, sistemas de IA que generen calificaciones o jerarquizaciones sociales de las personas derivadas de sus comportamientos o de sus características y que puedan dar lugar a situaciones discriminatorias y, por tanto, vulneradoras de los principios de dignidad e igualdad.

Se trata de una cuestión de extraordinaria importancia porque están en juego elementos esenciales del Estado social y democrático de Derecho que quedarían seriamente menoscabados si se permitieran sistemas, como los apuntados, dirigidos a condicionar la conducta de la ciudadanía y capaces de generar, cuando menos, daños sociales y económicos, cuando no físicos y psíquicos².

En las siguientes páginas desarrollaremos la hipótesis del riesgo cierto que suponen los sistemas que nos ocupan³ y el acierto que, a nuestro juicio, constituye su introducción en el Reglamento Europeo como una forma de hacer frente a una de las manifestaciones crecientes de, en palabras de Shoshana Zuboff, el “capitalismo de vigilancia”⁴.

Como es obvio, no se trata de excluir cualquier tipo de “puntuación” personal que persiga modificaciones conductuales, puesto que hay sistemas no solo posibles sino, seguramente, necesarios; así, por ejemplo, el permiso de circulación por puntos sería un buen y conocido ejemplo: en palabras de la Dirección General de Tráfico su objetivo “es modificar los comportamientos y actitudes de los conductores infractores, sensibilizarlos sobre las graves consecuencias humanas, económicas y sociales que se derivan de los acci-

² Véase al respecto el trabajo de F. PASQUALE y D. KEATS CITRON “The Scored Society: Due Process for Automated Predictions”, *Washington Law Review*, vol. 89, 2014, pp. 1-33.

³ Sobre el riesgo algorítmico D. SAN MARTÍN SEGURA, *La intrusión jurídica del riesgo*, CEPC, Madrid, 2023, p. 271 y ss.

⁴ “Capitalismo de la vigilancia, m. 1. Nuevo orden económico que reclama para sí la experiencia humana como materia prima gratuita aprovechable para una serie de prácticas comerciales ocultas de extracción, predicción y ventas. 2. Lógica económica parasítica en la que la producción de bienes y servicios se subordina a una nueva arquitectura global de modificación conductual. 3. Mutación inescrupulosa del capitalismo caracterizada por grandes concentraciones de riqueza, conocimiento y poder que no tienen precedente en la historia humana. 4. El marco fundamental de una economía de la vigilancia. 5. Amenaza tan importante para la naturaleza humana en el siglo XXI como lo fue el capitalismo industrial para el mundo natural en los siglos XIX y XX. 6. Origen de un nuevo poder instrumental que impone su dominio sobre la sociedad y plantea alarmantes contradicciones para la democracia de mercado. 7. Movimiento que aspira a imponer un nuevo orden colectivo basado en la certeza absoluta. 8. Expropiación de derechos humanos cruciales que perfectamente puede considerarse como un golpe desde arriba: un derrocamiento de la soberanía del pueblo”, *La era del capitalismo de vigilancia*, Paidós, Barcelona, 2022, 2ª edición, p. 9.

dentes de tráfico y hacerles ver la implicación que sus conductas tienen en los accidentes”⁵.

En otros contextos los sistemas no estarán prohibidos pero sí serán calificados como de “alto riesgo”; así, “... los sistemas de IA que se utilizan en los ámbitos del empleo, la gestión de los trabajadores y el acceso al autoempleo, en particular para la contratación y la selección de personal, para la toma de decisiones que afecten a las condiciones de las relaciones de índole laboral, la promoción y la rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales y para la supervisión o evaluación de las personas en el marco de las relaciones contractuales de índole laboral, dado que pueden afectar de un modo considerable a las futuras perspectivas laborales, a los medios de subsistencia de dichas personas y a los derechos de los trabajadores. Las relaciones contractuales de índole laboral deben incluir, de manera significativa, a los empleados y las personas que prestan servicios a través de plataformas, como indica el programa de trabajo de la Comisión para 2021. Dichos sistemas pueden perpetuar patrones históricos de discriminación, por ejemplo, contra las mujeres, ciertos grupos de edad, las personas con discapacidad o las personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, durante todo el proceso de contratación y en la evaluación, promoción o retención de personas en las relaciones contractuales de índole laboral. Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden socavar sus derechos fundamentales a la protección de los datos personales y a la intimidad” (Considerando 57 del Reglamento Europeo).

Igualmente, “el acceso a determinados servicios y prestaciones esenciales, de carácter público y privado, necesarios para que las personas puedan participar plenamente en la sociedad o mejorar su nivel de vida, y el disfrute de dichos servicios y prestaciones, es otro ámbito en el que conviene prestar especial atención a la utilización de sistemas de IA. En particular, las personas físicas que solicitan a las autoridades públicas o reciben de estas prestaciones y servicios esenciales de asistencia pública, a saber, servicios de asistencia sanitaria, prestaciones de seguridad social, servicios sociales que garantizan

⁵ “El saldo de puntos puede cambiar: ser un buen conductor y/o realizar cursos de sensibilización te hacen ganar puntos. Cometer infracciones te resta, hasta llegar a cero. Si llegaras a esa situación, se procederá a tramitar la pérdida de vigencia de tu permiso y no podrás conducir ningún vehículo, aunque antes de que esto suceda, puedes recuperar puntos”, disponible en

<https://www.dgt.es/nuestros-servicios/permisos-de-conducir/tus-puntos-y-tus-permisos/como-funciona-el-permiso-por-puntos/> (a 15 de junio de 2024).

una protección en casos como la maternidad, la enfermedad, los accidentes laborales, la dependencia o la vejez y la pérdida de empleo, asistencia social y ayudas a la vivienda, suelen depender de dichas prestaciones y servicios y, por lo general, se encuentran en una posición de vulnerabilidad respecto de las autoridades responsables. La utilización de sistemas de IA para decidir si las autoridades deben conceder, denegar, reducir o revocar dichas prestaciones y servicios o reclamar su devolución, lo que incluye decidir, por ejemplo, si los beneficiarios tienen legítimamente derecho a dichas prestaciones y servicios, podría tener un efecto considerable en los medios de subsistencia de las personas y vulnerar sus derechos fundamentales, como el derecho a la protección social, a la no discriminación, a la dignidad humana o a la tutela judicial efectiva y, por lo tanto, deben clasificarse como de alto riesgo” (Considerando 58).

Como es sabido, y como se explica con más detalle en otros apartados de esta obra colectiva, la calificación de un sistema como de alto riesgo implica una serie de obligaciones; entre otras,

“Los sistemas de IA de alto riesgo irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue” (artículo 13.2);

“1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas. 2. El objetivo de la vigilancia humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible...” (artículo 14.1 y 2);

“Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida” (artículo 15.1);

“... Los sistemas de IA de alto riesgo que continúan aprendiendo tras su introducción en el mercado o puesta en servicio se desarrollarán de tal modo que se elimine o reduzca lo máximo posible el riesgo de que información de salida que puede estar sesgada influya en la información de entrada de futuras operaciones («bucles de retroalimentación») y se garantice que dichos bucles se subsanen debidamente con las medidas de reducción de riesgos oportunas” (artículo 15.4.3).

II. EL SISTEMA DE CRÉDITO SOCIAL CHINO

El sistema de puntuación social del que más se ha venido hablando, y que comenzó a desarrollarse incluso antes de la eclosión actual de la IA, es el de crédito social chino (CSCH en lo sucesivo); como explican Lauren Yu-Hsin Lin y Curtis J. Milhaupt⁶, la planificación de un programa integral de crédito social que complementara el débil sistema jurídico de China comenzó en la década de 1990 con el objetivo más ambicioso de hacer frente al fraude generalizado en la transición del país de la planificación central a una incipiente economía de mercado. Esos esfuerzos culminaron en 2014 con la publicación conjunta por el Comité Central del Partido Comunista Chino y el Consejo de Estado chino del *Esquema de planificación para la construcción de un sistema de crédito social (2014-2020)*, un programa integral para evaluar el crédito social de individuos, empresas, entidades gubernamentales y otras organizaciones.

En la actualidad, el sistema de crédito social es también la pieza central de la estrategia de gobernanza digital de China, que marca un cambio hacia un mercado autorregulado, es decir, en el que se presiona o incentiva a los agentes para que ajusten su comportamiento a las normas del partido-Estado más allá de los canales ordinarios de la ley y la regulación.

Por su parte, y en el ámbito privado, ya en 2015 Alibaba presentó su propio sistema de calificación crediticia personal, *Sesame Credit*, para recopilar información sobre la identidad personal, el historial crediticio, la fiabilidad contractual y los comportamientos y relaciones sociales. A partir de esta información, a los participantes se les asignan puntuaciones de crédito social visibles para los demás y a quienes las tienen altas se les ofrecen ventajas, como la aprobación más rápida de un préstamo⁷.

⁶ “China’s Corporate Social Credit System: The Dawn of Surveillance State Capitalism?”, *The China Quarterly*, Cambridge University Press, 2023, pp. 1-19; en particular, pp.2-4; disponible, a 15 de junio de 2024, en <https://www.cambridge.org/core/journals/china-quarterly/article/chinas-corporate-social-credit-system-the-dawn-of-surveillance-state-capitalism/EC80AC0CC9AE60D3D3C631A707A5CE54> (a 18 de febrero de 2024); véase también R. CREEMERS “China’s Social Credit System: An Evolving Practice of Control”, 9 de mayo de 2018, en <https://ssrn.com/abstract=3175792> y <http://dx.doi.org/10.2139/ssrn.3175792> (a 15 de junio de 2024).

⁷ En su página web *Sesame Credit* explica: “The concept of a credit score may feel complicated, but in essence it looks simply at your payment history, amount of debt, how long you have had debt and how many recent applications you have made for credit accounts. Information about these items are reported to the three credit bureaus, Experian, Trans-Union and Equifax, who compile your credit report. The information on your credit report is used to calculate your credit score. Your three-digit credit score captures your experiences with credit and debt and can help you track changes in your financial history over time, from the very first debt you encounter-such as the credit card you opened in college-up to

Zuboff explica que el sistema *Sesame Credit* genera una valoración «holística» del «carácter» de una persona por medio de un aprendizaje algorítmico que asimila mucho más que el hecho de que esta pague a tiempo sus facturas y los préstamos que contrata. Los algoritmos evalúan y clasifican compras (por ejemplo, el hecho de que sean videojuegos en vez de libros para niños), títulos educativos, y cosas como la cantidad y la «calidad» de las amistades. Los individuos bien puntuados reciben distinciones y recompensas de los clientes de *Sesame Credit* en sus mercados de futuros conductuales. Pueden así alquilar un coche sin pagar fianza, o recibir unos términos más favorables en ese préstamo o en ese alquiler de piso que soliciten, o ver acelerados los trámites para la obtención de visado, o ser objeto de una exposición más destacada en las aplicaciones de citas, etcétera. Sin embargo, algunos testimonios apuntan a que los privilegios asociados a una reputación personal elevada pueden tornarse súbitamente en penalizaciones por motivos en absoluto relacionados con el comportamiento de la persona en su faceta como consumidor: basta, por ejemplo, con que haya hecho trampa en un examen en la universidad⁸.

Volviendo al CSCH, tiene dos características principales: la primera es la recopilación de datos a escala nacional procedentes de un amplio abanico de organismos reguladores, Gobiernos centrales y locales, el Poder Judicial y plataformas privadas. Cuando esté plenamente operativo, el sistema recopilará dos tipos básicos de información: la crediticia pública, generada por las interacciones de una empresa con órganos gubernamentales y agencias reguladoras (multas, sentencias, licencias comerciales...), y la información

the present. Credit score is a powerful tool that signals to prospective lenders your ability to make payments in a timely manner. This number is unique to you but publicly available under federal law to lenders considering you as a borrower. Your score can be a point of personal pride for good financial management and a point of public documentation. A credit score is an easy way to explain to another person or prospective lender that you can honor your commitment to make timely payments on outstanding debts. In turn, higher scores might lead a lender to extend interest rates lower than they would for consumers with less-favorable credit scores. You can get your credit score as part of a request for a credit report or independently of a credit report. A comprehensive solution is to open a free Credit Sesame account. This provides you with fast access to everything you need to know about your credit history, including your credit score. It includes helpful supporting information that makes sense of your score and report...

Legally, a variety of entities and people can request a copy of your creditreport, which is the information that feeds into your credit score. According to the Consumer Financial Protection Bureau (CFPB), this list includes: Businesses to whom you owe money, Government agencies, Landlords, Employers, Insurance providers, Banks and financial providers, Legal entities (in the event of court orders, for example), Others you have authorized in writing to receive a copy"; disponible, a 15 de junio de 2024, <https://www.creditsesame.com/knowledge-hub/what-is-credit-score/>

⁸ *Op. cit.*, p. 520 y 521.

crediticia de mercado, generada por las interacciones de una empresa con otros agentes del mercado (reclamaciones de consumidores, datos generados por agencias de calificación de créditos...). Los datos se utilizarán en sistemas de puntuación gestionados por las administraciones locales, la mayoría de los cuales están en fase de construcción.

El segundo elemento principal del CSCH es un régimen de recompensas y castigos (en forma de “listas rojas” y “listas negras”) mantenido por organismos gubernamentales. Algunas listas tienen un amplio alcance, como el incumplimiento de sentencias judiciales, mientras que otras se aplican a sectores específicos de la economía, como la alimentación o la medicina.

La inclusión en una lista roja o negra es pública; en el primer caso puede implicar diversos beneficios, que van desde la ampliación del acceso a los préstamos hasta una reducción de la frecuencia de las inspecciones o el aumento de las oportunidades en los procesos de contratación pública y acceso a la financiación, sobre todo para las pequeñas y medianas entidades. La inclusión en una lista negra origina barreras de mercado, como restricciones para obtener autorizaciones gubernamentales, mayor frecuencia de inspecciones y prohibiciones para obtener financiación. Cuando una entidad es incluida en una lista negra, su representante legal y las personas directamente responsables de la infracción también se incluirán en la lista⁹.

III. EL DESARROLLO DE LOS SISTEMAS DE CALIFICACIÓN COMO UNA VÍA DE EXPANSIÓN DEL CAPITALISMO DE VIGILANCIA

En una nota al principio de estas páginas recogimos las definiciones de “capitalismo de vigilancia” que propone Zuboff¹⁰ y las dos primeras acepciones, con algunas puntualizaciones, parecen englobar prácticas como las que caracterizan el sistema de crédito social chino: serían, en primer lugar, parte de un nuevo orden económico-político que reclama para sí la experiencia humana como materia prima gratuita aprovechable para una serie de prácticas políticas, sociales y comerciales ocultas de extracción, predicción y ventas; en segundo término, estarían presididas por una lógica parasítica en la que la producción de bienes y servicios se subordina a una nueva arquitectura global de modificación conductual.

No parece que la previsión del Reglamento de Inteligencia Artificial prohibiendo los sistemas de IA que proporcionan calificaciones sociales de per-

⁹ Y.-H. LIN y C. J. MILHAUPT, *op. cit.*, p. 3-4; con más amplitud, K. SCHAEFER, “China’s social credit system: context, competition, technology and geopolitics.” *Trivium China*, 16 de noviembre de 2020, disponible, a 15 de junio de 2024, en https://www.uscc.gov/sites/default/files/2020-12/Chinas_Corporate_Social_Credit_System.pdf.

¹⁰ S. ZUBOFF, *La era del capitalismo de vigilancia*, Paidós, 2020, *passim*.

sonas físicas para su uso con fines generales esté pensando en la implantación o el uso en Europa de sistemas como el del crédito social chino: en los países de la Unión Europea y en otros Estados democráticos la vida privada y los datos personales gozan de un elevado nivel de protección jurídica y existe mayor grado de preocupación social por las amenazas que herramientas de esta naturaleza suponen para esos derechos y para el propio libre desarrollo de la personalidad individual; como resultado no se han desarrollado prácticas propias de sociedades totalitarias como el llamado “*dang'an*”, el expediente personal de múltiples y variados aspectos de cada uno de los cientos de millones de habitantes urbanos que se va actualizando desde su infancia y durante el resto de sus vidas. Este «sistema de la era Mao para el registro de los más íntimos detalles de la vida» se nutre de la información actualizada que suministran los profesores, los funcionarios del Partido Comunista y los empleadores. Los ciudadanos no tienen derecho alguno a revisar el contenido de sus propios ficheros ni, menos aún, a impugnarlo”¹¹.

No obstante estas diferencias entre el “ecosistema” europeo y el chino, debe tenerse en cuenta para matizarlas que, en primer lugar, entre nosotros está presente la llamada “paradoja de la privacidad”: mientras los individuos se declaran preocupados por su privacidad y le otorgan una valoración importante, sus decisiones son significativamente incoherentes con la valoración que confiesan, puesto que hacen poco o, esencialmente, nada para proteger sus datos personales y, por lo tanto, su privacidad¹².

Y, en segundo lugar, aunque no parezca próxima en Europa la consolidación de un capitalismo de vigilancia estatal autoritario como el chino no quiere decir que no haya ya prácticas de capitalismo de vigilancia empresarial que, parafraseando de nuevo a Zuboff, se valen de la experiencia humana como materia prima gratuita aprovechable para una serie de prácticas comerciales y laborales ocultas de extracción, predicción y ventas presididas por una lógica parasítica en la que la producción de bienes y servicios y las relaciones laborales poco a poco se van subordinando a una nueva arquitectura global de modificación conductual.

En palabras de CREEMERS, esta “tendencia a la ingeniería social y a ‘empujar’” a los individuos hacia un comportamiento ‘mejor’ también forma

¹¹ *Op. cit.*, p. 524.

¹² M. ARTIGOT GOLOBARDES, “Mercados digitales, inteligencia artificial y consumidores”, *El Cronista El Cronista del Estado social y democrático de Derecho*, n° 100, 2022, pp. 130 y 131; de manera más extensa, S. BARTH y M. DE JONG, “The privacy paradox –Investigating Discrepancies between expressed privacy concerns and actual online behavior –A sytematic literature review”, *Telematics and Informatics*, 34(7) (2017); P. A. NORBERG; D. R. HORNE, y D. A. HORNE (2007), “The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors”, *Journal of Consumer Affairs*, 41 (1): 100-126.

parte del enfoque de Silicon Valley, que sostiene que los problemas humanos pueden resolverse de una vez por todas mediante el poder perturbador de la tecnología. Los seres humanos se reducen a un conjunto de números que indican su rendimiento en escalas preestablecidas, en sus hábitos alimentarios, por ejemplo, o en su régimen de ejercicio físico, que luego se les reta a mejorar. El mero hecho de que exista información significa que las empresas y los gobiernos tratarán de aprovecharla para sus propios fines, ya sean políticos o comerciales. En ese sentido, quizá el elemento más chocante de la historia no sea la agenda del gobierno chino, sino lo similar que es al camino que está tomando la tecnología en otros lugares”¹³.

Y para mencionar un ejemplo concreto en España de la utilización de datos que una empresa ha venido empleando con el objetivo de evitar las exigencias derivadas de una relación laboral dependiente y al tiempo para “empujar” conductualmente a los trabajadores a estar disponibles el mayor tiempo posible para conseguir más encargos y, en suma, mayor retribución, cabe recordar, aunque resulte un poco extenso, lo dicho por la Sala de lo Social del Tribunal Supremo español en su sentencia de 25 de septiembre de 2020 que resolvió sobre la condición de trabajadores por cuenta ajena de los repartidores de GLOVO:

“*Antecedente de hecho 7*- La Empresa tiene establecido un sistema de puntuación de los ‘glovers’, clasificándolos en tres categorías: principiante, junior y senior. Si un repartidor lleva más de tres meses sin aceptar ningún servicio, la Empresa puede decidir bajarle de categoría. (Cláusula cuarta del contrato de prestación de servicios). El sistema de ranking utilizado por GLOVO ha tenido dos versiones diferentes: la versión *fidelity*, que se utilizó hasta julio de 2017, y la versión *excellence*, utilizada desde dicha fecha en adelante. En ambos sistemas la puntuación del repartidor se nutre de tres factores: La valoración del cliente final, la eficiencia demostrada en la realización de los pedidos más recientes, y la realización de los servicios en las horas de mayor demanda, denominadas por la Empresa ‘horas diamante’. La puntuación máxima que se puede obtener es de 5 puntos. Existe una penalización de 0,3 puntos cada vez que un repartidor no está operativo en la franja horaria previamente reservada por él. Si la no disponibilidad obedece a una causa justificada, existe un procedimiento para comunicarlo y justificar dicha causa, evitando el efecto penalizador[...]. Los repartidores que tienen mejor puntuación gozan de preferencia de acceso a los servicios o recados que vayan entrando[...].

FJ 18.- [...] En la práctica este sistema de puntuación de cada repartidor condiciona su libertad de elección de horarios porque si no está disponible

¹³ *China’s chilling plan to use social credit ratings to keep score on its citizens*, CNN, 27 de octubre de 2015, <https://edition.cnn.com/2015/10/27/opinions/china-social-credit-score-creemers/index.html> (a 15 de junio de 2024).

para prestar servicios en las franjas horarias con más demanda, su puntuación disminuye y con ella la posibilidad de que en el futuro se le encarguen más servicios y conseguir la rentabilidad económica que busca, lo que equivale a perder empleo y retribución. Además, la empresa penaliza a los repartidores, dejando de asignarles pedidos, cuando no estén operativos en las franjas reservadas, salvo causa justificada debidamente comunicada y acreditada.

La consecuencia es que los repartidores compiten entre sí por las franjas horarias más productivas, existiendo una inseguridad económica derivada de la retribución a comisión sin garantía alguna de encargos mínimos, que propicia que los repartidores intenten estar disponibles el mayor período de tiempo posible para acceder a más encargos y a una mayor retribución.

FJ 21.- Glovo no es una mera intermediaria en la contratación de servicios entre comercios y repartidores. No se limita a prestar un servicio electrónico de intermediación consistente en poner en contacto a consumidores (los clientes) y auténticos trabajadores autónomos, sino que realiza una labor de coordinación y organización del servicio productivo. Se trata de una empresa que presta servicios de recadería y mensajería fijando el precio y condiciones de pago del servicio, así como las condiciones esenciales para la prestación de dicho servicio. Y es titular de los activos esenciales para la realización de la actividad[...]. La empresa ha establecido instrucciones que le permiten controlar el proceso productivo. Glovo ha establecido medios de control que operan sobre la actividad y no solo sobre el resultado mediante la gestión algorítmica del servicio, las valoraciones de los repartidores y la geolocalización constante[...]. Para prestar estos servicios Glovo se sirve de un programa informático que asigna los servicios en función de la valoración de cada repartidor, lo que condiciona decisivamente la teórica libertad de elección de horarios y de rechazar pedidos. Además, Glovo disfruta de un poder para sancionar a sus repartidores por una pluralidad de conductas diferentes, que es una manifestación del poder directivo del empleador. A través de la plataforma digital, Glovo lleva a cabo un control en tiempo real de la prestación del servicio, sin que el repartidor pueda realizar su tarea desvinculado de dicha plataforma[...].”

Cabe mencionar otros ejemplos en el ámbito laboral; así, Todolí Signes explica, en una cita también extensa, que “el trabajo en un *Call center* es uno de los más afectados por este alto nivel de monitorización. Los algoritmos controlan el número de llamadas atendidas, la duración de las mismas, las pausas, incluso el contenido de la llamada a través de la detección de palabras clave, el tono de voz y la entonación[...]. La empresa CallMiner anuncia que su software puede evaluar y poner nota –y hacer un ranking entre los trabajadores– en profesionalidad, cortesía y empatía en la atención mostrada durante las llamadas[...]. En el mismo sentido, en los supermercados se contabiliza cómo de rápido cada cajero escanea los productos de la cesta de

la compra pudiendo compararlos con el resto de trabajadores a efectos de retribuciones, asignación de turnos de trabajo, despidos de los menos rápidos y para hacer competir entre sí a los cajeros para que aceleren el ritmo de trabajo. El trabajo con ordenadores, sea en oficina o teletrabajo, es otro de los que están sujetos a un control absoluto de los tiempos de trabajo y una posterior evaluación del mismo mediante algoritmos a través de índices de productividad. La empresa Crossover ofrece una herramienta llamada *Work-Samart* para monitorizar ordenadores. Este programa cuenta las pulsaciones del teclado y el ratón, la pantalla del ordenador, los emails enviados e incluso realiza una foto cada diez minutos a través de la webcam del ordenador. De esta forma, cada segundo de inactividad con el ordenador –que no significa que el trabajador no esté pensando o trabajando con una libreta– se penaliza[...].

Los trabajos presenciales no se libran de este tipo de controles y rankings de productividad. Existen en el transporte, la limpieza, la hostelería, etc. El ejemplo más conocido es el control que realiza Amazon a los mozos de almacén midiendo el número y velocidad de cajas empaquetadas, los pasos dados en un día dentro de los almacenes, las pausas para ir al baño o socializar, etc. Así, mediante pulseras inteligentes o chips en las botas se realiza un exhaustivo recuento del trabajo prestado y junto otras variables se elabora un índice de productividad que es usado para generar avisos automáticos (la pulsera vibra o se le envía un mensaje a la misma) o se despiden de forma automatizada a las personas que no alcanzan una mínima productividad. De acuerdo con los datos, el 10% de los trabajadores de almacén de Amazon en los EEUU han sido despedidos por el índice de productividad¹⁴.

Finalmente, y por acercarnos de manera breve un ámbito diferente como es el de los contratos de seguro, un ejemplo clásico es el uso de la calificación crediticia de los asegurados para fijar la prima en los seguros de automóvil, que como recuerda María Luisa Muñoz Paredes, dio lugar a un movimiento de rechazo en Estados Unidos, tras la averiguación hecha por la Asociación Consumer Reports en el año 2015 de que se atendía más a ese factor que a otros más influyentes en el riesgo, como es el historial de conducción del asegurado¹⁵. A este respecto, en el Considerando 37 del Reglamento euro-

¹⁴ “La inteligencia artificial no te robará tu trabajo, sino tu salario. Retos del Derecho del Trabajo frente a la dirección algorítmica del trabajo”, *El Cronista del Estado social y democrático de Derecho*, n° 100, 2022, pp. 155 y 156; de manera más extensa, y del mismo autor, *Algoritmos productivos y extractivos. Cómo regular la digitalización para mejorar el empleo e incentivar la innovación*, Aranzadi, 2023.

¹⁵ “Big Data, IA y seguro: riesgos de inasegurabilidad y discriminación entre asegurados”, *El Cronista del Estado social y democrático de Derecho*, n° 100, 2022, p. 122; de manera más extensa, y de la misma autora, “‘Big Data’ y contrato de seguro: los datos generados por los asegurados y su utilización por los aseguradores”, en A. HUERGO LORA (dir.):

peo de IA se recuerda que los sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas para los seguros de salud y de vida también pueden tener un impacto significativo en los medios de vida de las personas y, si no se diseñan, desarrollan y utilizan debidamente, pueden vulnerar sus derechos fundamentales y acarrear graves consecuencias para la vida y la salud de las personas, incluida la exclusión financiera y la discriminación.

Con las previsiones contenidas en el Reglamento, algunas de estas herramientas, como ya se ha apuntado antes, serán consideradas sistemas de “alto riesgo” si los datos que se usan provienen del propio contexto en el que se aplican los resultados de las evaluaciones y podrán prohibirse en el supuesto de que provengan de contextos diferentes y generen discriminaciones.

IV. LA PROHIBICIÓN DE DETERMINADOS SISTEMAS QUE EVALÚAN O CLASIFICAN A LAS PERSONAS FÍSICAS

El apartado 1.c del artículo 5 del Reglamento ha tenido el siguiente desarrollo desde la propuesta de la Comisión de 21 de abril de 2021 a la redacción definitiva, pasando antes por la Posición común (“enfoque general”) del Consejo Europeo sobre la Ley de IA, del 6 de diciembre de 2022, y por las enmiendas formuladas por el Parlamento Europeo el 14 de junio de 2023.

Quedan prohibidas las siguientes prácticas de IA:

La regulación de los algoritmos, Aranzadi, Cizur Menor, 2020, pp. 129-162; “El ‘Big Data’ y la transformación del contrato de seguro”, en A. B. VEIGA: *Dimensiones y desafíos del seguro de responsabilidad civil*, Cizur Menor (Aranzadi), 2021, pp. 1017-1051; sobre el empleo en los contratos de seguro de lo que Caty O’NEIL llama “armas de destrucción matemática” véase su libro del mismo título, Capitán Swing, Madrid, 2017, pp. 199 ss.

Comisión	Consejo Europeo	Parlamento	Reglamento
La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA por parte de las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas, de forma que la clasificación social resultante provoque una o varias de las situaciones siguientes:	La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA con el fin de evaluar o clasificar a las personas físicas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:	La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA con el fin de evaluar o clasificar a las personas físicas o grupos de ellas a efectos de su calificación social durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:	La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA con el fin de evaluar o clasificar a las personas físicas o grupos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las siguientes situaciones:
i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;	i) un trato perjudicial o desfavorable hacia determinadas personas físicas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;	i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;	i) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos enteros de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;
ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de éste”.	ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos de personas físicas que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de éste”.	ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos de personas físicas que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de éste”.	ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de éste”.

Cuadro de elaboración propia.

Aunque no estamos ante uno de los preceptos que haya experimentado más cambios entre la propuesta de la Comisión, las enmiendas aprobadas por el Parlamento y el texto definitivo resultante de los “trílogos”, sí cabe destacar los realizados y, en primer lugar, uno de los más importantes es el relativo al sujeto al que se le prohíbe introducir estos sistemas: mientras que en la propuesta de la Comisión se mencionaba a “las autoridades públicas” o a quien actuara “en su representación”, la posición común del Consejo, así como la enmienda del Parlamento y la redacción final resultante del acuerdo interinstitucional suprimen esa concreción y la prohibición afectará tanto a las autoridades públicas como a sujetos particulares, físicos o jurídicos, incluyendo, por tanto, a las empresas.

Esta modificación parece muy positiva porque los riesgos que se tratan de combatir pueden provenir tanto de sujetos públicos como de particulares y, como ya hemos visto, encontramos ejemplos de utilización de sistemas de puntuación por parte de empresas muy relevantes.

En segundo lugar, la propuesta de la Comisión se refería a la evaluación o clasificación de “la fiabilidad” de personas físicas mientras que la posición común del Consejo, la enmienda del Parlamento y el texto definitivo hablan de “evaluar o clasificar a las personas físicas o a grupos de personas”, es decir, el análisis no se circunscribe a la “confianza” que puede generar una persona sino que alcanza a la persona como tal y, además, a partir de la enmienda del Parlamento se incluye a las personas “o grupos de personas” (piénsese, por ejemplo, en colectivos de consumidores, trabajadores, asegurados...).

En tercer lugar, los textos de la Comisión y del Consejo aunque no son idénticos -en el primer caso se atiende “a su conducta social o a características personales o de su personalidad” y en el segundo “a su comportamiento social o a características personales o de su personalidad”- aluden a características “conocidas o predichas”; la enmienda del Parlamento y la redacción final del Reglamento también incluyen las “inferidas”, algo relevante porque las inferencias son conclusiones que se obtienen a partir del tratamiento de datos y esa es una de las propiedades de los sistemas de IA: la capacidad de extraer de los datos existentes nuevas informaciones.

En cuarto lugar, mientras la propuesta de la Comisión habla de “clasificación social” el Consejo y el Parlamento utilizan la expresión “puntuación ciudadana”, que será la incluida finalmente en el Reglamento”, aunque no parece que la idea a la que se refieren sea distinta: la jerarquización de las personas a partir de los datos conocidos, predichos o inferidos.

Como quinta cuestión a comentar está la relativa a la generación de una o varias de las situaciones que se describen a continuación y que son las que justificarían la prohibición; la primera de ellas es que resulte un trato per-

judicial o desfavorable para concretas personas o colectivos enteros en contextos sociales que no guarden relación con aquéllos donde se generaron o recabaron los datos originalmente. Se está pensando en que la puntuación resultante del tratamiento de los datos provoque una discriminación o, en palabras de los textos examinados, un “trato perjudicial o desfavorable”.

A este respecto, y como hemos visto al principio, la redacción final del Considerando 31 explica que “los sistemas de IA que permiten a agentes públicos o privados llevar a cabo una puntuación ciudadana de las personas físicas pueden tener resultados discriminatorios y abocar a la exclusión a determinados grupos. Pueden menoscabar el derecho a la dignidad y a la no discriminación y los valores de igualdad y justicia”.

Una matización significativa, a la que ya nos hemos referido con anterioridad, es que los datos que generan ese trato desfavorable deben haberse obtenido en contextos diferentes al de aquel en el que provocarían ese perjuicio pero nada impediría su uso en el contexto de origen; a este respecto, parece que sí se podrían emplear datos conseguidos en el seno de una relación laboral para llevar a cabo una puntuación de quienes trabajan en esa empresa o datos obtenidos en una relación contractual de prestación de servicios (por ejemplo, el suministro eléctrico) para establecer una jerarquía de precios diferentes a clientes en situaciones distintas porque una cosa es la diferencia de precios y otra la discriminación; en esta línea, la Ley 3/1991, de 10 de enero, de Competencia Desleal, en artículo 16.1 establece que “el tratamiento discriminatorio del consumidor en materia de precios y demás condiciones de venta se reputará desleal, a no ser que medie causa justificada”, es decir, no sería desleal aquel trato diferente para el que exista justificación ni la mera diferencia de precios¹⁶.

Ahora bien, la no existencia de discriminación o trato perjudicial contrario a la prohibición del artículo 5.1.c no excluye que los datos empleados lo sean sin conocimiento o, incluso, sin consentimiento de la persona afectada, lo que puede situarle en una posición de especial vulnerabilidad en los mercados digitales. Por este motivo, “es necesario crear los mecanismos para evitar que dicha vulnerabilidad se materialice en una expropiación de excedente contractual que el consumidor esperaba obtener de la transacción y que solo con instrumentos puramente contractuales no podrá recuperar”¹⁷.

¹⁶ Véase al respecto, M. L. MUÑOZ PAREDES: “Big Data, IA y seguro: riesgos de inasegurabilidad y discriminación entre asegurados”, *El Cronista del Estado social y democrático de Derecho...*, p. 123.

¹⁷ ARTIGOT GOLOBARDES, M.: “Mercados digitales, inteligencia artificial y consumidores”, *El Cronista del Estado social y democrático de Derecho...*, p. 135.

Por otra parte, y como también se ha apuntado más arriba, que el sistema en cuestión no sea objeto de prohibición no excluye que pueda ser calificado como de “alto riesgo” en los términos ya vistos.

Finalmente, y como ya se ha apuntado, lo que no cabría es la utilización de los datos de alguien para llevar a cabo evaluaciones o clasificaciones en un contexto diferente al de su generación u obtención y que le supongan un perjuicio o trato desfavorable¹⁸; así, por ejemplo, la mayor o menor calificación crediticia de una persona no debería ser un condicionamiento para un ascenso dentro de una empresa¹⁹.

La segunda situación que justificaría la prohibición de un sistema de IA es que genere “un trato perjudicial o desfavorable hacia determinadas personas físicas o grupos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este”. Aquí lo que se tiene en cuenta es la manera en que una persona física interactúa con otras personas físicas o con la sociedad e influye en ellas y de ahí se deriva un trato desfavorable que o bien no está justificado o las consecuencias son desproporcionadas a su gravedad; por ejemplo, que las opiniones políticas o manifestaciones ideológicas, religiosas, sociales o culturales expresadas en una red social impliquen, con carácter general, una causa de exclusión para que una persona sea contratada o su expulsión de un centro educativo o que las calificaciones sobre amabilidad de un trabajador llevadas a cabo por los clientes supongan causa suficiente para su despido o para una sanción económica desmedida.

BIBLIOGRAFÍA

- ARTIGOT GOLOBARDES, M. “Mercados digitales, inteligencia artificial y consumidores”, *El Cronista El Cronista del Estado social y democrático de Derecho*, n° 100, 2022, pp. 130 y 131.
- BARTH, S. y DE JONG, M. “The privacy paradox –Investigating Discrepancies between expressed privacy concerns and actual online behavior –A systematic literature review”, *Telematics and Informatics*, 34(7) (2017).
- CREEMERS, R. “China’s Social Credit System: An Evolving Practice of Control”, 9 de mayo de 2018, en <https://ssrn.com/abstract=3175792> y <http://dx.doi.org/10.2139/ssrn.3175792> (a 15 de junio de 2024).

¹⁸ Como es obvio, sí pueden tener repercusión en la relación laboral comentarios o comportamientos que supongan una transgresión de la buena fe contractual o sean ofensivos para el empleador (54.2 c) y d) del Estatuto de los Trabajadores).

¹⁹ Cathy O’NEIL ofrece numerosos ejemplos de los resultados perversos derivados del uso, entre otros, de criterios de calificación crediticia en el ámbito laboral y en el del consumo en *Armas de destrucción matemática. Cómo el big data aumenta la desigualdad y amenaza la democracia...*, pp. 181 ss.

- CREEMERS, R. *China's chilling plan to use social credit ratings to keep score on its citizens*, CNN, 27 de octubre de 2015, <https://edition.cnn.com/2015/10/27/opinions/china-social-credit-score-creemers/index.html> (a 15 de junio de 2024).
- MUÑOZ PAREDES, María Luisa. “‘Big Data’ y contrato de seguro: los datos generados por los asegurados y su utilización por los aseguradores”, en A. HUERGO LORA (dir.): *La regulación de los algoritmos*, Aranzadi, Cizur Menor, 2020, pp. 129-162.
- MUÑOZ PAREDES, María Luisa. “Big Data, IA y seguro: riesgos de inasegurabilidad y discriminación entre asegurados”, *El Cronista del Estado social y democrático de Derecho*, n° 100, 2022, 122 y ss.
- MUÑOZ PAREDES, María Luisa. “El ‘Big Data’ y la transformación del contrato de seguro”, en A. B. VEIGA: *Dimensiones y desafíos del seguro de responsabilidad civil*, Cizur Menor (Aranzadi), 2021, pp. 1017-1051.
- NORBERG, P. A.; HORNE, D. R. ; y HORNE, D. A. . (2007), “The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors”, *Journal of Consumer Affairs*, 41 (1): 100-126.
- O'NEIL, C. *Armas de destrucción matemática. Cómo el big data aumenta la desigualdad y amenaza la democracia*, Capitan Swing, Madrid, 2017.
- PASQUALE, F. y KEATS CITRON, D. “The Scored Society: Due Process for Automated Predictions”, *Washington Law Review*, vol. 89, 2014, pp. 1-33.
- SAN MARTÍN SEGURA, D. *La intrusión jurídica del riesgo*, CEPC, Madrid, 2023.
- SCHAEFER, K. “China's social credit system: context, competition, technology and geopolitics.” *Trivium China*, 16 de noviembre de 2020, disponible, a 15 de junio de 2024, en https://www.uscc.gov/sites/default/files/2020-12/Chinas_Corporate_Social_Credit_System.pdf.
- TODOLÍ SIGNES, A. “La inteligencia artificial no te robará tu trabajo, sino tu salario. Retos del Derecho del Trabajo frente a la dirección algorítmica del trabajo”, *El Cronista del Estado social y democrático de Derecho*, n° 100, 2022, pp. 155 y 156.
- TODOLÍ SIGNES, A. *Algoritmos productivos y extractivos. Cómo regular la digitalización para mejorar el empleo e incentivar la innovación*, Aranzadi, 2023.
- YU-HSIN LIN, L. y CURTIS J. Milhaupt, CURTIS J. “China's Corporate Social Credit System: The Dawn of Surveillance State Capitalism?”, *The China Quarterly*, Cambridge University Press, 2023, pp. 1-19.
- ZUBOFF, S. *La era del capitalismo de vigilancia*. Paidós, 2020.

Los mecanismos jurídico-constitucionales existentes se revelan insuficientes ante la arquitectura de mediación informática que se impone a escala global. Como advirtió Shoshana Zuboff, esta estructura avanza con fuerza y sin oposición, basada en sofisticados mecanismos de extracción de información de todo tipo. Esta obra se centra, en particular, en la recolección masiva de datos biométricos de las personas, orientada a la captación de comportamientos, emociones y perfilado, en un contexto marcado por la expansión del llamado capitalismo de la vigilancia.

La evolución de la economía de datos ha dejado claro que el viejo paradigma regulador —centrado en la protección frente a la acumulación de archivos y dosieres— ha quedado obsoleto ante el despliegue del big data. Hoy, el objetivo de las grandes plataformas va mucho más allá: no se limita a registrar nuestras acciones, sino que busca captar nuestra atención de forma constante y, en última instancia, modular nuestro comportamiento. En este nuevo entorno, nos hemos convertido en objetos del Internet del Todo (Internet of Everything), monitorizadas de forma ubicua, incluso sin saberlo, más allá de los escenarios clásicos de vigilancia como los policiales o de control fronterizo.

El problema es que esta vigilancia se presenta de forma seductora, casi invisible. Más que percibirla como una amenaza, la ciudadanía se siente halagada por la creciente personalización de los servicios y estímulos que la rodean. Sin advertirlo, se entrega complacida a esta lógica, convertida —como ya intuyó Tocqueville— en una masa dócil, pastoreada por algoritmos que giran en torno a sus datos.

Frente a este escenario, esta obra colectiva reúne las aportaciones de una veintena de expertas y expertos que analizan en detalle las posibilidades y los límites del marco normativo europeo. Se examina especialmente el potencial del Reglamento General de Protección de Datos (RGPD) para afrontar los desafíos de la vigilancia biométrica masiva, en diálogo con otras normas clave del paquete digital europeo, como el recién aprobado Reglamento (UE) 2024/1689 de Inteligencia Artificial. Asimismo, se presta atención al Convenio Marco sobre IA del Consejo de Europa, a las estrategias impulsadas por actores internacionales como la OCDE, a los desarrollos doctrinales de las autoridades de protección de datos y a la jurisprudencia nacional, comunitaria y europea, en constante conversación con la literatura comparada.