Revista Jurídica

n.º 54 • 2024

Región de Murcia

Fundación Mariano Ruiz-Funes
ICAMUR Ilustre Colegio de la Abogacía de Murcia
Universidad de Murcia
Región de Murcia

Revista Jurídica Región de Murcia N.º 54 2024

PATRONATO DE LA FUNDACIÓN MARIANO RUIZ FUNES

PRESIDENTE

Excmo. Sr. Don Fernando López Miras, Presidente de la Comunidad Autónoma de la Región de Murcia.

VICEPRESIDENTA

Excma. Sra. Doña Maravillas Hernández López, Decana del Ilustre Colegio de la Abogacía de Murcia

VOCALES

Ilma. Sra. Doña María Caballero Belda, Secretaria General de la Consejería de Presidencia, Portavocía, Acción Exterior y Emergencias.

Ilma. Sra. Doña Ana María Tudela García, Directora de los Servicios Jurídicos de la Comunidad Autónoma de la Región de Murcia.

Ilma. Doña Cristina García López, Secretaria del Ilustre Colegio de la Abogacía de Murcia.

Ilma. Doña Daniela Rubio Riera, Bibliotecaria del Ilustre Colegio de la Abogacía de Murcia.

Doña María del Mar de la Peña Amorós, Directora de la Escuela de Práctica Jurídica de la Universidad de Murcia.

Don Fermín Gallego Moya, Directora de la Escuela de Relaciones Laborales de la Universidad de Murcia

DIRECTORA

Doña Teresa García Calvo, abogada colegiada del Ilustre Colegio de la Abogacía de Murcia.

SECRETARIA

Doña María Robles Mateo, Técnica Consultora de la Consejería de Presidencia, Portavocía, Acción Exterior y Emergencias.

CONSEJO DE REDACCIÓN DE LA REVISTA JURÍDICA DE LA REGIÓN DE MURCIA

DIRECCIÓN

Doña Teresa García Calvo. Abogada ICAMUR, especialista en Derecho penal, Derecho médico y salud y responsabilidad civil. Directora de la Fundación Mariano Ruíz-Funes.

COMPOSICIÓN DEL CONSEJO DE REDACCIÓN

1.- Doña Francisca María Ferrando García. Decana de la Facultad de Derecho de la Universidad de Murcia, Catedrática de Derecho del Trabajo y de la Seguridad Social.

2.- Doña Maravillas Hernández López. Abogada y Decana del Ilustre Colegio de la Abogacía de Murcia. Vicepresidenta de la Fundación Mariano Ruíz-Funes.

3.- Doña Esperanza Orihuela Calatayud. Profesora y catedrática de Derecho Internacional Público y Unión Europea, Universidad de Murcia.

4.- Doña María Ángeles Sánchez Jiménez. Profesora y Catedrática de Derecho Internacional Privado, Universidad de Murcia.

5.- Don Joaquín Atáz López. Profesor y Catedrático de Derecho Civil de la Universidad de Murcia.

6.- Don Faustino Cavas Martínez. Profesor y Catedrático de Derecho del Trabajo y de la Seguridad Social, Universidad de Murcia.

7.- Don Fermín Gallego Martínez. Profesor de Derecho del Trabajo y de la Seguridad Social, Universidad de Murcia.

8.- Doña María del Mar de la Peña Amorós. Profesora y Catedrática de Derecho Financiero y Tributario. Directora de la Escuela de Práctica Jurídica de la Universidad de Murcia.

9.- Don Julián Valero Torrijos. Profesor y Catedrático de derecho Administrativo de la Universidad de Murcia.

10.- Doña Maria José Verdú Canete. Profesora de Derecho Mercantil de la Universidad de Murcia Especialista en Derecho Concursal.

11.- Doña Elisa Pérez de los Cobos Hernández. Profesora y Doctora con mención internacional en Derecho Administrativo.

12.- Don Luís Gálvez Muñoz. Profesor y Catedrático de Derecho Constitucional de la Universidad de Murcia. Director del Aula de Debate y Director Académico de la Asociación Club de Debate Universitario.

13.- Don Francisco Martínez-Escribano Gómez. Abogado ICAMUR, con amplia experiencia en el mundo del Derecho especialista en procesos de Civil, Administrativo, Penal, Mercantil y Familia.

14.- Don Maximiliano Castillo González. Abogado ICAMUR, con amplia experiencia en el mundo del Derecho especialista en procesos de Civil, Administrativo, Penal, Mercantil y Familia.

15.- Doña Daniela Rubio Riera. Abogada ICAMUR con amplia y dilatada experiencia en Derecho de Familia. Bibliotecaria de ICAMUR.

16.- Don Andrés Arnaldos Cascales. Abogado ICAMUR, con amplia experiencia en el mundo del Derecho especialista en Mercantil, Societario, Civil, Penal, Económico, Administrativo, Laboral y Tributario. Especializado en el ámbito empresarial.

17.- Don Miguel Pardo Domínguez. Abogado ICAMUR, especialista en Derecho Penal.

18.- Doña Cristina García López. Abogada ICAMUR. Actualmente Secretaria del ICAMUR, especialista en Derecho en Civil, Penal, Contencioso y Social.

19.- Don Antonio García Montes. Abogado ICAMUR, especialista en Derecho Bancario, Mercantil, Civil y Mercantil.

20.- Doña Isabel María Rodríguez García. Abogada ICAMUR, especialista en Derecho Penal.

21.- Don Pedro Rivera Barrachina. Abogado ICAMUR, especialista en Derecho Civil e Inmobiliario.

22.- Doña Patricia Pérez García. Abogada ICAMUR, especialista en Derecho Financiero y Tributario.

23.- Doña Blanca Castillo Amorós. Abogada ICAMUR, especialista en Derecho de Extranjería y Violencia de Género.

24.- Don Idoia Azpetia Alonso. Abogada ICAMUR, especialista en Derecho Mercantil y Concursal.

25.- Don Alberto Pérez Quirós. Abogado ICAMUR, especialista en Derecho Civil, Sucesiones y Mercantil.

26.- Doña María Dolores Cantó Cánovas. Decana del del Ilustre Colegio de Procuradores y Tribunales de Murcia.

27.- Don Antonio Vicente Sempere Navarro. Magistrado del Tribunal Supremo, Presidente de la Sala IV. Catedrático de Derecho del Trabajo. Codirector de la Revista Española de Derecho del Trabajo y de la Revista de Derecho Laboral V-Lex, ha fundado y dirige la Revista de Jurisprudencia Laboral, editada por la AEBOE

28.- Don Miguel Angel Larrosa Amante. Magistrado y Presidente de la Audiencia Provincial de Murcia.

29.- Don José Guillermo Nogales Cejudo. Magistrado Titular del juzgado de Primera Instancia nº 13 de Murcia. Miembro de la Red Judicial Española para Asuntos Civiles y Mercantiles, de la Red Judicial Europea Civil y Mercantil y de la Red Iberoamericana de Cooperación Jurídica Internacional.

30.- Don Antonio Alcazar Fajardo. Magistrado-Juez del Juzgado de lo Penal nº 6 de Murcia

31.- Don Francisco Cano Marco. Magistrado-Juez de lo Mercantil Juzgado nº 2 de Murcia.

32.- Doña Gema Quintanilla Navarro. Magistrada de la Sala de lo Contencioso Administrativo del TSJ.

33.- Doña Carmen Rodriguez Pérez. Decana del Ilustre Colegio de Notarios de Murcia

34.- Don Jorge López Fernández. Registrador de la Propiedad, Registro nº 1 de Murcia

35.- Doña Ana Maria Tudela García. Directora de los Servicios Jurídicos de la Comunidad Autónoma de la Región de Murcia.

36.- Don Manuel Pino Smilg. Letrado Subdirector de los Servicios Jurídicos de la Comunidad Autónoma de la Región de Murcia.

37.- Don Manuel M. Contreras Ortiz. Letrado-Secretario General del Consejo Jurídico de la Región de Murcia.

38.- Doña Caridad de la Hera Orts. Directora de la Escuela de Formación e Innovación de Administración Pública de la Región de Murcia.

39.- Don Pablo Vigueras Paredes. Jefe de Servicio de la Asesoría Jurídica del Hospital Clínico Universitario Virgen de la Arrixaca y Profesor Asociado de la Universidad de Murcia. .

EDITA:

Consejería de Presidencia, Portavocía, Acción Exterior y Emergencias.
Palacio San Esteban
Calle Acisclo Díaz, s/n
30005 Murcia
ISSN: 0213-4799
Depósito legal: MU-329-1985
Producción: O. A. Boletín Oficial de la Región de Murcia

Sumario

CRITERIOS DE CALIDAD. LATINDEX

CARACTERÍSTICAS BÁSICAS (PRERREQUISITOS PARA EVALUAR LA REVISTA)

1. Mención del cuerpo editorial: se debe mencionar la existencia de un consejo editorial, de redacción o responsable científico.
2. Contenido científico para calificar positivamente al menos el 40% de los documentos publicados en los fascículos a evaluar, estará constituido por: a) artículos originales; b) artículos técnicos: c) comunicaciones en congresos; d) cartas al director o artículos breves) artículos de revisión, estados del arte, etc.) .
3. Antigüedad mínima de un año; para ser analizada una publicación deberá haber comenzado a editarse al menos 12 meses antes del momento de hacer el análisis.
4. Identificación de los autores. Los trabajos deben estar firmados por los autores con nombre y apellidos o declaración de autor institucional.
5. Lugar de edición: Deben hacerse constar en lugar visible el lugar de edición de la revista.
6. Entidad editora: Debe hacerse constar en lugar visible la entidad o institución editora de la publicación
7. Mención del Director: en la revista deberá constar el nombre del director de la publicación.
8. Mención de la dirección de la revista: Deberá aportarse en lugar visible la dirección postal o de correo electrónico de la administración de la revista a efectos de solicitud de suscripciones, canje, etc.

PARÁMETROS RELATIVOS A LA PRESENTACIÓN DE LAS REVISTAS

9. Páginas de presentación (Cubierta/portada) : Deberán incluir título completo, ISSN, volumen, número, fecha y membrete bibliográfico.
10. Mención de periodicidad: Es condición inexcusable que la revisa exprese o mencione su periodicidad o, en su defecto, el número de fascículos que editar al año.
11. Tabla de contenido: Califica positivamente cuando existe en cada fascículo tabla de contenido, índice o sumario en los que consten los datos del título, autor y al menos página inicial.
12. Membrete bibliográfico al inicio del artículo: Califica positivamente si el membrete bibliográfico aparece al inicio de cada artículo e identifica la fuente.
13. Membrete bibliográfico en cada página: Califica positivamente si el membrete que identifica la fuente aparece en cada página de los artículos publicados.
14. Miembros del Comité Editorial o Consejo de Redacción: Califica positivamente si aparecen los nombres de los miembros del Comité Editorial o Consejo de Redacción de la Revista.
15. Afiliación institucional de los miembros del Comité editorial o Consejo de Redacción: Califica positivamente si se proporcionan los nombres de las instituciones a las que están adscritos los miembros del Comité editorial (a no confundir con el Consejo Asesor o Comité Científico, cuyos miembros también deberán ir a acompañados de sus lugares de trabajo) . No basta que se indique solo el país.
16. Afiliación de los autores: Deberá proporcionarse al menos el nombre de la institución de trabajo del autor o autores de cada artículo. Esta información podrá encontrarse tanto al principio como al final de cada artículo, así como en las "listas de colaboradores" o "información sobre los autores" que aparecen entre las primeras o entre las últimas páginas de cada fascículo.

PARÁMETROS RELATIVOS A LA GESTIÓN Y LA POLÍTICA EDITORIAL

17. Fecha de recepción y aceptación de originales: Califica positivamente solo si se indican ambas fechas.
18. ISSN: Califica positivamente la existencia de código ISSN.
19. Definición de la revista: Califica positivamente si en la revista se menciona el objetivo, cobertura temática y/o público al que va dirigida.
20. Sistemas de arbitraje: en la revista deberá constar el procedimiento empleado para la selección de los artículos a publicar.
21. Evaluadores externos: Califica positivamente si el sistema de arbitraje recurre a evaluadores externos a la entidad o institución editora de la revista.
22. Autores externos: Califica positivamente si al menos el 50% de los trabajos publicados provienen de autores externos a la entidad editora de la revista. En el caso de revistas editadas por asociaciones se considerarán autores pertenecientes a la entidad editora los que formen parte de la directiva de la asociación o figuren en el equipo de la revista.
23. Apertura editorial: Califica positivamente si al menos una tercera parte del Comité editorial o Consejo de Redacción es ajena a la entidad editora de la revista.
24. Servicios de información: Califica positivamente si la revista está incluida en algún servicio de indización, resúmenes, directorios o bases de datos. Este campo califica positivamente tanto si la base de datos es mencionada por la propia revista, como si lo agrega el calificador (a partir de la búsqueda hecha para tal fin) .
25. Cumplimiento de la periodicidad: Califica positivamente si la revista edita al año el número de fascículos correspondientes con la periodicidad expresada.

PARÁMETROS RELATIVOS A LAS CARACTERÍSTICAS DE LOS CONTENIDOS

26. Contenido original: Califica positivamente si al menos el 40% de los artículos son trabajos de investigación, comunicación científica o creación originales.
27. Instrucciones a los autores: Califica positivamente si aparecen las instrucciones a los autores sobre el envío de originales y resúmenes en cada fascículo.
28. Elaboración de las referencias bibliográficas: En las instrucciones a los autores deberán indicarse las normas de elaboración de las referencias bibliográficas para calificar positivamente.
29. Exigencia de originalidad: Califica positivamente si en la presentación de la revista o en las instrucciones a los autores se menciona esta exigencia para los trabajos sometidos a publicación.
30. Resumen: Califica positivamente si todos los artículos van acompañados de un resumen en el idioma original del trabajo.
31. Resumen en dos idiomas: Califica positivamente si se incluyen resúmenes en el idioma original del trabajo y en un segundo idioma.
32. Palabras clave: Califica positivamente si se incluyen palabras clave en el idioma original del trabajo.
33. Palabras clave en dos idiomas: Califica positivamente si se incluyen palabras clave en el idioma original del artículo y en otro idioma.

RESH. Evaluación de Revistas de Ciencias Sociales y Humanidades Revistas Españolas de Ciencias Sociales y Humanas: Valoración integrada e índice de citas CSIC Ministerio de Ciencia e Innovación.

I.- PRESENTACIÓN

El actual panorama internacional, marcado por una situación general convulsa donde se suceden acontecimientos catastróficos y guerras como la de Ucrania y conflictos como los de África y Próximo Oriente, no deja de generar momentos de incertidumbre política. Una tendencia que se ve confirmada tras las recientes elecciones en Estados Unidos o la situación en Venezuela, por citar algunos ejemplos. A esta situación se suma también la acción de los fenómenos climáticos con consecuencias como la reciente DANA que ha azotado principalmente a Valencia y a otras zonas de Albacete y Andalucía, causando enormes daños personales y materiales que tenemos bien presentes, y cuyas víctimas cuentan con toda nuestra solidaridad y apoyo.

En el año 2022 se lanzaba el número 53 de la Revista Jurídica de la Región de Murcia, en un momento en el que España empezaba a salir de la enorme crisis sanitaria que supuso la pandemia internacional ocasionada por el Covid-19, que paralizó multitud de actividades a nivel global, tanto económicas, como intelectuales, oficios, servicios privados y públicos… La prioridad fue entonces enfocar los esfuerzos sólo en aquellos aspectos que fuesen esenciales y exclusivos para paliar los efectos de la pandemia. Hoy, dos años después, la Revista Jurídica de la Región de Murcia resurge con más fuerza que nunca, y lo vuelve hacer en un escenario de preocupación y notable inestabilidad nacional e internacional, por lo que es necesario reconocer el mérito y el esfuerzo de quienes, al margen de sus puestos de responsabilidad en diferentes instituciones y empresas, han dedicado tiempo a conformar y publicar

el que es ya el número 54 de la Revista Jurídica de la Región de Murcia, en su edición de 2024.

Distintas reorganizaciones de la Administración Regional han afectado a la composición del Patronato de la Fundación Mariano Ruiz-Funes, a lo que se ha sumado la necesidad de actualizar la composición del Consejo de Redacción de la Revista. Esto se ha conseguido en el primer semestre de 2024, naciendo así un renovado Consejo en el que siguen participando importantes consejeros, integrantes del mismo desde sus orígenes en 1985, y al que se incorporan nuevos miembros de reconocido prestigio y trayectoria profesional de distintas ramas como la abogacía, procuraduría, judicatura, notaría, registros, función pública…

Este Consejo de redacción está integrado por un extenso número de personas relevantes en el ámbito jurídico, lo que demuestra el interés real y vigente por mantener viva la edición y publicación de la Revista Jurídica de la Región de Murcia, así como por aunar sus esfuerzos y conseguir no sólo que perdure su publicación, sino que se sitúe y consolide como revista de prestigio y valor añadido dentro de las publicaciones existentes en el sector.

Los nuevos patronos, con el Presidente de la Comunidad Autónoma de la Región de Murcia al frente, abogan firmemente por esta puesta en valor de la Revista. De ello es prueba la incorporación de su nueva directora, Teresa García Calvo, que fue discípula de Felipe Ortega, responsable de la Revista desde sus comienzos hasta 2016, y que continuará con este legado que, sin duda, cosechará grandes éxitos y será de enorme utilidad en el ámbito jurídico.

La revista surgió, en un principio, con afán científico y divulgativo, teniendo como propósito evitar la inseguridad jurídica en una época en la que la tecnología distaba mucho de la actual y ni siquiera las bases de datos de jurisprudencia eran fácilmente accesibles. Con la colaboración de la entonces Consejería de Presidencia y actualmente Consejería de Presidencia, Portavocía, Acción Exterior y Emergencias, el Ilustre Colegio de la Abogacía de Murcia y la Universidad de Murcia, a través de la Facultad de Derecho, fue posible elaborar esta publicación que serviría de altavoz a abogados y juristas en la Región, que se hacían eco así de la más novedosa actualidad jurídica y jurisprudencial.

Por ello, este número de la revista cobra un valor significativo dado que ha cambiado el paradigma en el que se originó el nacimiento de la misma, cuando estamos siendo testigos de un momento histórico crucial en el que está en ple-

no auge el fenómeno de la Inteligencia Artificial, siendo así que la publicación actual consiste en un número monográfico dedicado a este asunto tan crucial para nuestro presente y futuro, la famosa IA, la Inteligencia Artificial.

Con sus defensores y sus detractores, la IA marca un hito del que la Revista Jurídica debía hacerse eco, como así lo ha hecho la Fundación durante este año 2024, en el que ha dedicado unas Jornadas y un Congreso a abordar este tema; Congreso en el que, además, se ha explicado la importancia y valor que cobran los datos en el contexto al que nos referimos.

La Inteligencia Artificial es ya una realidad y, por tanto, es preciso conocer tanto sus ventajas como inconvenientes; aquello en lo que nos puede ayudar y, cómo no, en el contexto que nos ocupa, la regulación jurídica de la misma.

No hay que olvidar que la Fundación Mariano Ruiz-Funes se integra en el Sector Público Regional, y dentro de su actividad de divulgación del conocimiento científico, y de su objetivo de acercar el mundo del derecho a la ciudadanía, es más que oportuno explicar la producción normativa que está surgiendo en esta materia, la casuística real que se está generando y la protección que tenemos y debemos tener los ciudadanos en uno de los bienes más preciados que poseemos y más codiciados por los mercados en la actualidad : "los datos".

Nos encontramos ante un escenario en el que el acceso a la información pública, la transparencia, la colaboración y la participación del conjunto de la sociedad, son pilares fundamentales. Es por ello que el concepto de Administración abierta se ha convertido en eje central para que las políticas públicas del gobierno sean más efectivas e inclusivas. La sociedad reivindica transparencia, rendición de cuentas, participación ciudadana, inclusión y colaboración de las Administraciones con el conjunto de la población. Para ello, es fundamental disponer de datos. Y es básico y necesario tanto que las Administraciones Públicas velen por la protección de los mismos como que los pongan a disposición con todas las garantías.

Las nuevas tecnologías y la inteligencia artificial suponen un reto, al tiempo que pueden facilitar y contribuir a mejorar muchos trabajos, reduciendo márgenes de error y disminuyendo tiempos de producción, siendo de gran utilidad siempre que sean usadas con las debidas garantías y límites. Por otro lado, las Administraciones Públicas son grandes bancos de datos de información pública que se acumula durante el proceso de implantación de las políticas que

se aplican, y con las diferentes interacciones de servicio al ciudadano y en sus relaciones con el sector privado y la sociedad civil.

Por ello, los datos son un recurso público cuya explotación a través de las nuevas tecnologías consigue una mayor eficiencia en la aplicación de los servicios públicos y en la implantación de políticas de calidad siendo, además, un recurso imprescindible para ponerlos a disposición del tejido empresarial y productivo como herramienta para el desarrollo de la economía y la sociedad en su conjunto.

Siendo conscientes de esta situación, el número 54 de la Revista Jurídica de la Región de Murcia está expresamente dedicado a la Inteligencia Artificial. Con la selección de cinco artículos, tres estudios doctrinales y dos artículos divulgativos que nos ilustrarán sobre la regulación realizada a nivel europeo en relación con la Inteligencia Artificial, la posible confrontación entre la protección de los derechos fundamentales y el uso de la IA, en especial la protección del derecho a la salud, a la privacidad e intimidad de las personas, a la propiedad intelectual o industrial e incluso a la propia vida. Por ello, también veremos como el Derecho Penal no puede estar alejado de la protección de estos derechos de los ciudadanos ante el uso y automatización masiva de estas tecnologías que, de forma genérica, se utilizan ya por los poderes públicos.

Para concluir, me gustaría trasladar desde el Gobierno de la Región de Murcia mi felicitación y agradecimiento a la nueva Directora de la Fundación Mariano Ruiz-Funes, Doña Teresa García Calvo, que ha conseguido renovar y reunir al Consejo de Redacción de la Revista Jurídica en un tiempo récord desde su toma de posesión el pasado mes de enero y, así mismo, hacer extensivo este agradecimiento a todo el Consejo de Redacción de la Revista Jurídica y a su Comité Ejecutivo, que, con su implicación y dedicación, han conseguido elaborar un número de calidad, rigurosidad y brillantez digno de esta publicación que es ya un referente consolidado en el ámbito jurídico de la Región de Murcia.

Marcos Ortuño Soto

Consejero de Presidencia, Portavocía, Acción Exterior y Emergencias.

Vicepresidente de la Fundación Mariano Ruiz-Funes.

II.- EDITORIAL

La última Revista editada en el año 2022 supuso la superación de la época COVID 2019 con un importante contenido de artículos.

Este año 2024 hemos retomado con gran ilusión el propósito de contribuir a la Sociedad y al Derecho desde la Revista, esta vez con un tema monográfico de enorme actualidad, con implicaciones presentes en nuestra vida diaria, como es la Inteligencia Artificial.

Con éste número se publican artículos que realizan un estudio sobre esta realidad, sus bondades, usos, e incluso los posibles efectos adversos, que supone un antes y después de la vida misma a nivel mundial.

Todos los autores/as de nuestra revista han tenido un espíritu altruista y colaborador, por lo que son merecedores de la difusión de este significativo esfuerzo.

Quiero agradecer a todo el equipo que conforma el Consejo de Redacción de la Revista su trabajo, apoyo humano y calidad profesional al haber llevado a cabo un arduo estudio de los artículos presentados, seleccionando aquéllos que han considerado de mayor calidad y trascendencia jurídica en un tema novedoso, tratado monográficamente desde distintas perspectivas. Todas ellas oportunas.

El Consejo de Redacción integrado por anteriores y nuevas incorporaciones desde la Administración Pública, Abogacía, Procura, Magistratura, Docencia, Investigación Universitaria, Notaría y Registro de la Propiedad, con la aporta-

ción de nuevos artículos de envergadura jurídica, participará sobre otros temas en próximos números. Propiciando una Revista en la que convivirán artículos jurídicos muy técnicos y otros más divulgativos de indudable interés también para la sociedad.

Además de todos aquéllos autores externos al Consejo de Redacción que quieran aportar sus artículos y enriquecer la revista con sus colaboraciones, como viene siendo habitual.

Deseo dar las gracias a quienes han seguido la Revista en sus muchas ediciones. Y a quiénes la hicieron posible luchando por ella, como el abogado Felipe Ortega Sánchez. A cuantos nos sigan actualmente y en el futuro.

Nos proponemos elevar su calidad jurídica, sin perder su función de aproximación a la ciudadanía.

Bienvenidos a todos/as, y deseo que puedan disfrutar escribiendo y leyendo. Nuestro objetivo es estar abiertos a sus reflexiones, comentarios, y artículos.

Y ser útiles desde el Derecho a la Sociedad.

Teresa García Calvo

Directora de la Fundación Mariano Ruíz Funes.

III. SECCIÓN DE ESTUDIOS DOCTRINALES

DERECHOS FUNDAMENTALES Y DERECHO PENAL FRENTE AL USO DE LA IA Y OTRAS TECNOLOGÍAS EN CIENCIAS DE LA SALUD[1].

María Ángeles Cuadrado Ruiz

Premio San Raimundo de Peñafort

Lema: "Salud para todos"

Resumen: *Las tecnologías emergentes y otros sistemas inteligentes como la Inteligencia Artificial son herramientas cada vez más utilizadas en ámbitos médicos y relativos a ciencias de la salud con la finalidad de mejorar la atención de los pacientes, la eficiencia de los hospitales o los ensayos clínicos, entre otros, pero que no están exentos de crear riesgos y comprometer derechos fundamentales como la vida, la salud, la privacidad e intimidad de las personas o la propiedad intelectual o industrial. El Derecho penal no puede estar alejado de la protección de estos derechos de los ciudadanos ante el uso y automatización masiva de estas tecnologías, que de forma genérica, se utilizan ya desde por los poderes públicos y la Administración sanitaria para la protección de la salud.*

Palabras clave*: Derechos humanos, Derecho penal, tecnologías emergentes, Inteligencia Artificial, salud pública, bioética, Medicina 5.0.*

Abstract: *Emerging technologies and other intelligent systems such as Artificial Intelligence are*

---

1 El presente trabajo de investigación se ha elaborado en el marco del Proyecto de Investigación "El Derecho Penal ante los retos actuales de la Biomedicina" (DERPEBIO, Ref. PID2022-136743OB-I00), financiado por MCIN, AEI y por FEDER Una manera de hacer Europa y de la estancia de investigación "Salvador de Madariaga" en la Facultad de Derecho de la Universidad de Siena, "La responsabilidad penal de las empresas y laboratorios farmacéuticos en el ámbito de la Biomedicina y el Bioterrorismo".

tools that are increasingly used in medical fields and health sciences in order to improve patient care, the efficiency of hospitals or clinical trials, among others, but they are not exempt from creating risks and compromising fundamental rights such as life, health, privacy and intimacy of individuals or intellectual or industrial property. Criminal law cannot be far from the protection of these rights of citizens in the face of massive use and automation of these technologies, which in a generic way, are already used by public authorities and health administration for the protection of health.

Key words*: Human rights, Criminal Law, emerging technologies, artificial intelligence, public health, bioethics, Health 5.0.*

I. INTRODUCCIÓN

Los avances de la ciencia y de la técnica, en la medida en que colaboran a un mejor orden de la sociedad humana y a acrecentar la libertad de las personas contribuyen a su vez a la transformación del mundo. Los progresos de la informática y el desarrollo de las tecnologías digitales en los últimos decenios ya han comenzado a producir profundas transformaciones en la sociedad global. Los nuevos instrumentos digitales están cambiando el rostro de las comunicaciones, de la administración pública, de la educación, de la justicia, del consumo, de las interacciones personales y de otros innumerables aspectos de la vida cotidiana[2]. La Medicina así como otras ciencias de la salud no han estado ajenas a los avances tecnológicos; de hecho, gracias a muchos de ellos, se ha mejorado la atención a las personas. Lo que ha venido a denominarse Medicina 5.0 o Salud 5.0 se configura como "una transformación a distintos niveles que implica un cambio cultural, científico, regulatorio y organizativo capaz de poner a la persona y su bienestar en el centro del sistema. Está conformado por las tecnologías de la información y la comunicación (TIC), los dispositivos basados en inteligencia artificial, la robótica médica y las aplica-

2 Francisco, *Inteligencia artificial y paz*, vid. 1. El progreso de la ciencia y de la tecnología como camino hacia la paz; 2. El futuro de la inteligencia artificial entre promesas y riesgos. Vaticano, 8 de diciembre de 2023.

ciones biomédicas y enmarca la necesidad de un nuevo enfoque en la gestión de la salud. El nuevo modelo de Medicina 5.0 se centra en la transición de un paradigma basado en el desarrollo tecnológico a un replanteamiento de la tecnología para el ser humano, enfatizando el papel activo y participativo del sujeto en la planificación y evaluación"[3].

La ex ministra de Justicia de España, Pilar Llop, en octubre 2023, en el marco del seminario "Servicios Públicos de Justicia en tiempos de transformación", organizado por el Ministerio de Justicia en colaboración con la Comisión Europea señaló en su intervención que "no podemos renunciar a la tecnología, porque sería renunciar a nuestro propio futuro", y advirtió que "debemos unir esfuerzos para eliminar los abusos, sesgos y brechas sociales que pueda generar". Según la ex ministra, "los derechos humanos y la ética deben ser el marco de referencia para la aplicación de la Inteligencia Artificial" (IA)[4].

Por ello, urge considerar los aspectos teóricos, prácticos, sociales, éticos y jurídicos de este nuevo escenario post pandemia COVID 19, (puesto que desde las disciplinas científicas y técnicas el estado del arte es otro). Los desafíos jurídicos y éticos[5] que estas tecnologías, y en concreto, la Inteligencia Artificial han traído consigo son inconmensurables para diferentes sectores y agentes. Es por lo que debemos preocuparnos por todos aquellos motivos por los que se puede originar un impacto negativo en los derechos fundamentales o que, cuanto menos, son proclives a ser analizados minuciosamente desde el

---

3 Bertolaso, M., responsable del proyecto *Healthcare 5.0: New perspectives in healthcare innovation and assessment* (octubre 2022-marzo 2024), de la Università Campus Bio-Medico di Roma, cuyos objetivos a abordar son: la caracterización del concepto Healthcare 5.0;la relación entre Medicina 4.0 y 5.0; el análisis del papel del paciente en la Sanidad 5.0 desde perspectivas éticas, epistemológicas y teóricas; los factores sociales y económicos relacionados con el paciente inteligente; la redefinición del concepto de medicina personalizada; las implicaciones sociales, políticas, económicas y jurídicas del paradigma emergente Sanidad 5.0: implicaciones para la gestión sanitaria y las JCI; implicaciones del paciente físico-digital en la gestión de datos y los derechos humanos. Además de enmarcar la Medicina 5.0 en el desarrollo sostenible y el enfoque ecológico. **¿El modelo 5.0 aporta un paradigma más sostenible a la atención sanitaria?**

4 Vid infra. competencias de la Agencia Española de Supervisión de Inteligencia Artificial, en España.

5 Vid. Urzúa Infante, C., "Inteligencia Artificial y los problemas éticos", en Arellano Toledo, V. (Dir.) *Derecho, Ética e Inteligencia Artificial* , Valencia 2023, pp. 369 y ss.

Derecho, pero también desde el punto de vista ético. No deberíamos olvidar aquellos aspectos que afectan a la esfera pública, puesto que los asuntos vinculados a ésta, y en concreto todo lo relacionado con la Administración sanitaria, los registros de datos de pacientes, la relación médico-paciente, el diagnóstico o la asistencia médica así como los cuidados por parte de enfermería u otro personal sanitario etc. se verán afectados por el uso de estas nuevas tecnologías, la IA, IoT, la telemedicina o la ciencia de datos, entre otras, que como señalaré más adelante, están construyendo una nueva forma de atención a los pacientes.

II. ¿A QUÉ NOS REFERIMOS CUANDO HABLAMOS DE TECNOLOGÍAS EMERGENTES (TES)?

Las tecnologías emergentes son innovaciones que incorporan mejoras a desarrollos que se encuentran en etapas todavía tempranas, o incluso pueden referirse a una mejora continua de una tecnología ya desarrollada y tienen el potencial de crear un impacto muy significativo en diversos campos de la sociedad. En ciencias de la salud estas tecnologías[6] están revolucionando la forma en cómo se diagnostican, tratan y gestionan las enfermedades, la forma de interacción entre gestores, médicos y pacientes. ¿Cuál es el papel de las tecnologías emergentes ante los retos sanitarios de los próximos años, como, por ejemplo, la gestión de enfermedades crónicas o la gestión de enfermedades degenerativas?[7] Aunque son aún muchos los interrogantes, se podría afirmar que estas tecnologías de alguna manera favorecen y mejoran la atención médica, en general. Tal resultado positivo sólo será posible si somos capaces de actuar de forma responsable y de respetar los derechos humanos fundamentales.

---

6 Izquierdo Alonso, J. L., Almonacid Sánchez, C., "Nuevas tecnologías en medicina", en *RIECS: Revista de Investigación y Educación en Ciencias de la Salud,* Vol. 7, Nº. 1, 2022, pp.69-82.

7 de Miguel Beriain, I., Lazcoz Moratinos, G., "Inteligencia artificial, personas mayores y biomedicina: la vulnerabilidad en el debate ético-jurídico" en Alkorta Idiakez, I. (dir.), Atienza Macías, E., (coord.) *Soluciones tecnológicas para los problemas ligados al envejecimiento: cuestiones éticas y jurídicas* / 2020, pp. 115-137.

Las tecnologías más destacadas en este campo son:

1. Inteligencia Artificial (IA):

Tradicionalmente lo que ha caracterizado al ser humano es precisamente el poseer inteligencia y voluntad. Inteligencia y voluntad son las facultades más específicas de la persona, y como tales modulan lo mejor de su vida, su obrar y su fin. Permiten conocer la verdad y amar el bien. Son la esencia humana. Podemos afirmar por ello, que inteligencia y voluntad están en el núcleo de la historia de la filosofía[8].

Es verdad que también nos referimos a la inteligencia de los animales y algunos autores plantean que sus acciones pudieran hacer dudar a cualquiera de la superioridad intelectual de la que el género humano hace gala a la hora de hablar de sus conocimientos[9].

La inteligencia se ha definido de muchas maneras[10], pero acudiendo al Diccionario de la Real Academia española[11] podemos decir que se trata de la capacidad de entender o comprender, de la capacidad de resolver problemas, del conocimiento, la comprensión, o el acto de entender, también es inteligencia el sentido en que se puede tomar una proposición, un dicho o una expresión, o la habilidad, destreza y experiencia, entre otras acepciones.

---

8 Congreso Internacional Inteligencia y Voluntad en Tomás de Aquino, Universidad de Navarra, Pamplona, 26-27 de abril de 2018.

9 Pouydebat, E., *Inteligencia animal: cabeza de chorlitos y memoria de elefantes*, 2018. Esta bióloga e investigadora francesa Emmanuelle Pouydebat ha recogido en un libro sus estudios sobre la inteligencia animal. Actualmente, varias investigaciones científicas en animales cuestionan si la inteligencia es una característica exclusiva de seres humanos. Si bien los seres humanos tenemos una capacidad de pensamiento abstracto que nos distingue de otros animales, se ha demostrado que el uso de herramientas, el razonamiento y la capacidad de aprendizaje no son exclusividad de los humanos. Para llegar a esta conclusión se han analizado algunas especies animales que demuestran niveles de inteligencia avanzados. Evidentemente los más conocidos son los primates, pero hay otras especies como las aves que pueden dar nuevas luces sobre la inteligencia de los animales.

10 Vid. al respecto, Díaz Fernández, A. M. (dir.), *Conceptos fundamentales de inteligencia*, 2016.; el mismo, Díaz Fernández (dir.), *Diccionario LID Inteligencia y seguridad*: *estructuras de inteligencia, fuentes, análisis, diseminación y operaciones encubiertas*, Ministerio de Defensa, Centro de publicaciones, 2013.

11 23ª ed. *Diccionario de la Real Academia española*, disponible en https://dle.rae.es/.

Como ha destacado Rozenwurcel, "la inteligencia puede ser muchas cosas. Sherman Kent escribió que la inteligencia tiene tres definiciones separadas: es conocimiento (la información que uno debe tener para tomar decisiones adecuadas), es una institución (refiriéndose a las organizaciones físicas de personas que persiguen cierto tipo de conocimiento) y es actividad (las acciones de dirección, reunión, análisis y difusión). Si bien las tres son necesarias para el éxito institucional, la inteligencia se describe mejor como un proceso analítico que evalúa la información recopilada de diversas fuentes; integra la información relevante en un paquete lógico; y produce una conclusión, estimación o pronóstico sobre un fenómeno utilizando el enfoque científico para la resolución de problemas"[12]. "La ciencia y la tecnología manifiestan de modo particular esta cualidad fundamentalmente relacional de la inteligencia humana, ambas son producto extraordinario de su potencial creativo"[13]. De las múltiples definiciones de "análisis de Inteligencia" ofrecidas por los autores puede concluirse que se trata de una actividad intelectual y no mecánica destinada a interpretar información más allá de los hechos aparentes, a la luz de la experiencia y mediante distintas herramientas, para exponerla de una forma clara y convincente al que la solicita. (…) En definitiva el análisis de inteligencia es nada más y nada menos que la identificación de la información clave (esto es: de las pruebas), relevante para un problema y la determinación de las conclusiones lógicas que pueden ser extraídas de esa información; la inteligencia es la quintaesencia del negocio del conocimiento"[14].

Si todo esto es Inteligencia, **¿Qué es la Inteligencia Artificial**? Podríamos acercarnos a este concepto señalando que es la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico[15]. Y se aplica a todos los campos[16].

---

12 Rozenwurcel, P., *Seguridad y prevención de la criminalidad: el mapeo de los delitos y de la percepción de seguridad (aplicado a la Ciudad Autónoma de Buenos Aires)*, Universidad de Granada, 2023, disponible en URI: https://hdl.handle.net/10481/85092, p. 370.

13 Francisco, *op. cit*, 1. El progreso de la ciencia y de la tecnología como camino hacia la paz.

14 Rozenwurcel, P., *op. cit.* p. 371.

15 23ª ed. Diccionario de la *Real Academia española*, disponible en https://dle.rae.es/

16 *I Congreso de Inteligencia Artificial de Andalucía*, que se llevó a cabo los días 22 y

Según se describe en la Propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial y se modifican determinados actos legislativos de la Unión[17]: "la Inteligencia Artificial es una familia de tecnologías de rápida evolución que requiere nuevas formas de vigilancia regulatoria y un espacio seguro para la experimentación, así como que se garantice la innovación responsable y la integración de salvaguardias y medidas de reducción del riesgo adecuadas. Para conseguir un marco jurídico que favorezca la innovación, resista el paso del tiempo y sea resiliente a las perturbaciones, conviene animar a las autoridades nacionales competentes de uno o varios Estados miembros a que establezcan espacios controlados de pruebas para la Inteligencia Artificial que faciliten el desarrollo y la prueba de sistemas de IA innovadores bajo una estricta vigilancia regulatoria antes de su introducción en el mercado o puesta en servicio".

La IA también se utiliza para el análisis de datos médicos, Big Data[18], el diagnóstico y la predicción de enfermedades, como ayuda a la práctica asistencial, pero también en la investigación clínica.

Los algoritmos de aprendizaje profundo pueden analizar imágenes médicas, como radiografías y escáneres, con gran precisión, y pueden ayudar a identificar patrones y tendencias en grandes conjuntos de datos de pacientes[19].

---

23 de noviembre en el Palacio de Congresos de Granada. También, el proyecto IA4TES de aplicación de la Inteligencia Artificial para la Transición Energética Sostenible, un programa pionero en España y de referencia internacional, que supone un importante impulso a la incorporación de las últimas tecnologías inteligentes a la gestión del sistema eléctrico. El proyecto, liderado por Iberdrola España, aspira a establecer las bases de la investigación para la aplicación de la tecnología IA en el sector eléctrico. Igualmente, tendrá en cuenta los aspectos **éticos**, de diversidad e inclusión y de privacidad de la Inteligencia Artificial.

17 COM(2021) 206 final 2021/0106 (COD), parágrafo (71).

18 Martínez García, Dalgo Flores, Herrera López, Jiménez, Velasco Acurio, "Avances de la inteligencia artificial en salud", en Revista *Dominio de las Ciencias,* Vol. 5, núm. 2, julio 2019, pp.603-613. El régimen para la utilización de datos personales con fines de investigación biomédica, fue aprobado en diciembre de 2018 mediante una nueva Ley Orgánica, la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD) que tiene por objetivo adaptar el Derecho interno español al Reglamento General de Protección de Datos que se hizo efectivo en mayo de ese mismo año.

19 Cfr. de Miguel Beriain, I., "Medicina personalizada, algoritmos predictivos y uti-

Como han señalado Izquierdo Alonso y Almonacid Sánchez, "la IA y el Big data permiten dar respuestas, casi en tiempo real a preguntas que han surgido en un contexto excepcional, pero preguntas igualmente importantes también las tenemos enfrente de nosotros en nuestra práctica clínica habitual. Además, en muchas ocasiones el perfil de pacientes que vemos en nuestras consultas o en las salas de un hospital tienen una complejidad muchísimo mayor que la que podemos observar en los ensayos clínicos, donde se tiende a seleccionar pacientes relativamente "puros" evitando aquellos cuya mayor complejidad pueda interferir de los resultados finales del estudio. Esta pobre validez externa de muchos ensayos clínicos hace que sus conclusiones, frecuentemente, no sirvan para establecer la efectividad de una determinada medida terapéutica, limitando su aplicabilidad a la vida real. Los pacientes atendidos con una determinada patología en un entorno hospitalario, sobre todo pacientes complejos, pluripatológicos, solo se podrían entender desde una aproximación personalizada que tenga en cuenta todas las variables que influyen en el estado de salud de ese paciente, y eso difícilmente se podrá evaluar de una forma integral con los ensayos clínicos actuales"[20]. Sin embargo, estas nuevas tecnologías permiten aproximaciones que pueden dar mejores respuestas que con la investigación tradicional.

La Medicina 5.0 se centra en la colaboración entre profesionales de la salud y sistemas de Inteligencia Artificial (IA) avanzados, una tecnología clave para analizar imágenes médicas, como radiografías, resonancias magnéticas y tomografías computarizadas, con el fin de detectar patrones y ayudar a los médicos a realizar diagnósticos más precisos y tempranos. La IA permite, además, un mejor monitoreo y seguimiento del paciente por su capacidad para procesar los datos de los dispositivos médicos conectados y, de esta forma, generar un sistema de alertas para que los facultativos puedan actuar rápidamente ante urgencias.

lización de sistemas de decisión automatizados en asistencia sanitaria. Problemas éticos", en Revista *Dilemata*, Nº. 30, 2019 (Ejemplar dedicado a: Ética, robótica y tecnologías asistenciales), págs. 96-99 y ss.

20 Izquierdo Alonso, J. L., Almonacid Sánchez, C., "Nuevas tecnologías en medicina", en *RIECS: Revista de Investigación y Educación en Ciencias de la Salud,* Vol. 7, Nº. 1, 2022, págs.69-82.

2. Telemedicina:

La telemedicina[21] permite la consulta médica y el seguimiento de enfermos a distancia a través de videoconferencias y herramientas *on line*. Esto es especialmente útil para pacientes que viven en áreas rurales o tienen dificultades para trasladarse o acceder a atención médica. Y en tiempos de pandemia y confinamiento se ha venido utilizando para citas médicas. Pero también se abren retos en cuanto a la comunicación. **¿Cómo modifica la salud físico-digital la relación médico-paciente?** ¿Puede cambiar el concepto de salud y enfermedad con el nuevo modelo de asistencia sanitaria?

3. Genómica:

La secuenciación del ADN ha avanzado enormemente, lo que permite la identificación de mutaciones genéticas y, por tanto, la personalización de tratamientos y medicamentos para pacientes con base en su perfil genético. La medicina genómica nos permite usar la información disponible en los genes para poder obtener resultados que permitan tratar enfermedades[22]. La terapia genómica introduce material genético en las células del paciente para corregir defectos genéticos específicos, potenciar su sistema inmunitario y como tratamiento o vacunas frente a enfermedades infecciosas. La metodología que se emplea en estas terapias es muy diversa y algunas de ellas ya están aprobadas para el tratamiento de ciertas enfermedades. Se pueden usar virus modificados para introducir un gen específico o ARN mensajero para que se produzca la proteína deseada. Ambas estrategias han sido utilizadas para las vacunas frente a la COVID-19.

---

21 En Andalucía (España) se implantó el "Sistema integral de Telemedicina" en el año 1989, siendo una de las Comunidades Autónomas pioneras en su implementación. El Sistema Integral de Telemedicina de Andalucía permitió, a través de la transmisión de información e imágenes en tiempo real, que los ciudadanos de las áreas rurales pudieran ser diagnosticados y tratados en su propia localidad por los profesionales de los hospitales de referencia, en aquellas patologías que no podían ser abordadas en sus respectivos centros de salud. Vid. Martínez Saporta, E., "Telemedicina y responsabilidad patrimonial de la Administración sanitaria", en *DS* Vol. 16, Número 1, Enero-Junio 2008, pp.110-111.

22 Cfr. Traversi, D., "Genomica in Sanità Pubblica Evidenze scientifiche e prospettive di integrazione nella pratica della prevenzione", en *Journal of Preventive Medicine and Hygiene*, 2023 Mar; 63(3 Suppl 2): E1–E29. Publicado online el 13 enero 2023.

Otras tecnologías usadas son los oligonucleótidos antisentido y los ARN interferentes, que se diseñan para que se unan a un ARN mensajero determinado y así bloquear o disminuir la producción de una proteína o de una enzima que es perjudicial. En este ámbito una de las estrategias más prometedoras es la conocida como "edición genómica" que se realiza directamente en las células del paciente y corrige de forma permanente la información genética que se asocia a una enfermedad. Esto se consigue usando la tecnología CRISPR-Cas9 que se dirige a la zona del gen que deseamos modificar, corta esa secuencia de ADN e inserta nuevo ADN con la información correcta y también se plantean cuestiones éticas importantes[23].

Actualmente hay múltiples ensayos clínicos que se están realizando para el tratamiento de numerosas patologías utilizando esta novedosa tecnología, y esto seguramente generará en los próximos años una revolución en la Medicina clínica que mejorará la vida de las personas.

4. Medicina regenerativa:

La medicina regenerativa se enfoca en la reparación y regeneración de tejidos y órganos dañados. Tecnologías como la terapia génica y la terapia de células madre están siendo investigadas para tratar una variedad de enfermedades. La Medicina Regenerativa, o Terapia Celular, conoce los tratamientos, terapias o técnicas que emplean material biológico como las células madre o tejidos del mismo paciente para curar, mejorar, curar o regenerar órganos. Es decir, se utilizan las propias células del cuerpo de la persona enferma para mejorar y auto-curar algunos tejidos, órganos y zonas dañadas.

5. Impresión en 3D de órganos y tejidos:

La impresión en 3D es una tecnología emergente que se ha utilizado para la creación de objetos reales a partir de modelos creados por ordenador, desde juguetes y joyas, hasta automóviles incluso alimentos.

La impresión en 3D y las tecnologías 3D aplicadas a la Medicina son un ámbito donde los avances salvan vidas. Las impresoras 3D y escáneres 3D ayudan a los médicos, investigadores y fabricantes de equipos médicos a vi-

23 De Miguel Beriain, I., "Retos éticos y jurídicos que plantea la edición genética embrionaria a la luz del marco legal vigente en el ámbito europeo: una mirada crítica", en *AFD,* 2019 (XXXV), pp. 71-92.

sualizar procedimientos, probar ideas rápidamente y personalizar la atención médica como nunca antes. Se utiliza también para crear órganos y tejidos a partir de materiales bio-compatibles. Las primeras aplicaciones en Medicina regenerativa de impresiones en 3D se hicieron con prótesis sólidas creadas con materiales plásticos, cerámicos o de titanio. La tecnología permite ajustar exactamente las piezas a las necesidades de cada paciente, con un grado de personalización inviable en la producción industrial. Sin embargo, estas piezas artificiales, si bien se integran mejor que las convencionales, no están exentas de presentar complicaciones.

La evolución lógica de la impresión en tres dimensiones en el ámbito de la Medicina es fabricar estructuras con la capacidad biológica de integrarse en el cuerpo del receptor. De ahí que se avance hacia la bio-impresión. El método consiste en utilizar materiales biocompatibles, que no sean rechazados por el organismo, y poblados por células del paciente para evitar, también, posibles rechazos. Los biomateriales ejercerían de receptáculo para las células que, una vez implantado el órgano, se irían reproduciendo hasta ocupar el espacio que les corresponda. Hoy en día existen dos técnicas de impresión de órganos: la más utilizada es generar una estructura a base de polímeros que posteriormente es repoblada con células, en un biorreactor. La otra imprime los órganos capa a capa; es decir, que el producto que sale de la máquina ya incluye el cultivo celular. Actualmente existen varios Proyectos de bioimpresión de órganos y tejidos impresos en 3D[24]: desde una córnea -un grupo de investigación en Hyderabad, India, ha completado con éxito el desarrollo de la primera córnea bioimpresa en 3D; la insuficiencia renal es una enfermedad que afecta a muchas personas en todo el mundo, pero no hay muchas opciones de tratamiento. Por este motivo, la empresa Trestle Biotherapeutics ha estado trabajando en el desarrollo de tejido que puede implantarse en pacientes con enfermedad renal terminal. En concreto, se trata de tejido renal funcional, destinado a sustituir y complementar las funciones renales y también complementar las funciones renales pérdidas anteriormente. Según Trestle Biotherapeutics, esta nueva terapia funciona integrando la biología de las células madre con la bioimpresión en 3D; un equipo de investigación de la Universidad de Boston ha utilizado la tecnología de impresión 3D para desarrollar una réplica en miniatura de un

24 M., Alicia, "Proyectos de bioimpresión: órganos y tejidos impresos en 3D" en https://www.3dnatives.com/es/proyectos-bioimpresion-organos-tejidos-impresos-3d-070420202/ Publicado el 2 febrero, 2023.

corazón humano. El dispositivo se creó utilizando una combinación de células cardiacas derivadas de células madre humanas y piezas acrílicas impresas en 3D a microescala. Y en 2022, un grupo de científicos del Hospital Tongi, de China desarrolló un ovario artificial impreso en 3D. Todo esto, sin duda, revolucionará la cirugía de trasplantes, ya que podría eliminar la necesidad de donantes y acortar los tiempos de espera.

6. Wearables y dispositivos de seguimiento:

Los dispositivos como los relojes inteligentes y las pulseras de actividad pueden recopilar datos de salud en tiempo real, como la frecuencia cardíaca, la actividad física y la calidad del sueño ¿Cómo leer y procesar datos de dispositivos inteligentes asociados a pacientes? Estos datos pueden ser útiles para el monitoreo de la salud y la prevención de enfermedades.

7. Robótica[25] médica:

Los robots ya se utilizaron en tiempos de pandemia para la desinfección de habitaciones de hospitales. La iniciativa facilitó el trabajo del personal sanitario ofreciéndoles una mayor protección frente a posibles infecciones y reduciendo los tiempos ya que los robots trabajan 24h[26]. El robot elimina las bacterias y virus de las superficies con un 99,9% de eficiencia. También contribuye a la seguridad del personal, ya que para efectuar la desinfección no requiere el uso de productos químicos corrosivos o tóxicos. Las máquinas se mueven por las salas con total autonomía desinfectando todas las superficies con una luz ultravioleta.

Los robots quirúrgicos están siendo utilizados en cirugías para mejorar la precisión y reducir el tiempo de recuperación[27]. Son varias las especialidades quirúrgicas en las que ya están presentes: en cirugía oral y maxilofacial, en neurocirugía, en ginecología, en el cáncer colorrectal, en urología, en cirugía

25 Gavilán, I, "Robots humanoides: desafíos éticos y normativos diferenciales", en Arellano Toledo, V. (Dir.), *Derecho, Ética e Inteligencia Artificial*, Valencia, 2023, p. 521 y ss.

26 *El Mundo,* miércoles, 29 septiembre 2021:" Los robots, nueva arma frente al Covid: cuatro hospitales de Madrid utilizan máquinas autónomas para desinfectar habitaciones".

27 https://www.europapress.es/madrid/noticia-siete-nuevos-equipos-cirugia-robotica-comenzaran-funcionar-hospitales-publicos-20231023143427.html.

torácica, entre otras, y un nuevo modelo de robot quirúrgico modular permite laparoscopia robótica inteligente, prácticamente, en todas las especialidades.

En en la atención de pacientes para tareas de asistencia y transporte, también se manejan los robots humanoides y ya se utilizan para su uso en hospitales como asistentes del personal sanitario para el reparto de bandejas de comida a los pacientes o de otros materiales[28].

8. Realidad virtual (RV) y realidad aumentada (RA):

Estas tecnologías se están utilizando en la educación médica, la terapia y la planificación quirúrgica. La RV puede simular situaciones clínicas y permitir a los profesionales de la salud practicar procedimientos en un entorno virtual.

9. Nanotecnología:

La nanotecnología se utiliza para desarrollar tratamientos y medicamentos a escala molecular, lo que puede mejorar la precisión y la efectividad de los tratamientos.

10. Internet de las cosas (IoT):

Los dispositivos médicos conectados a través de IoT pueden recopilar datos en tiempo real sobre la salud de los pacientes y enviarlos a los profesionales de la salud para su revisión y seguimiento. Tienen el potencial de mejorar significativamente la atención médica, aumentar la precisión de los diagnósticos y los tratamientos y reducir los costos de atención médica. Lo que hace más sostenible al sistema.

11. Otras técnicas como la de los biosensores se están perfeccionando.

La tecnología de los biosensores se descubrió en la década de los años 70 a 80 e hizo posible "cuantificar directamente de forma específica las moléculas, los microorganismos o las células, sin necesidad de utilizar estrategias analíticas complejas». Estos dispositivos permitían obtener los resultados de los análisis de forma fácil, en poco tiempo y con menos gasto. El primer biosensor fue desarrollado para la cuantificación de glucosa en sangre y comenzó

---

28 *EM entremayores,* viernes, 8 de Diciembre de 2023:" Desarrollan dos robots móviles para su uso como asistentes en hospitales repartiendo bandejas de comida o materiales al personal sanitario".

a comercializarse en 1975. Hoy en día es habitual esta práctica. En un futuro inminente, los biosensores de afinidad molecular –con una tecnología simple y similar a la de la glucemia– «harán posible que, en una primera visita al médico, este tome una muestra de sangre del paciente y analice, directamente y en menos de un minuto, la presencia en su sangre de un marcador tumoral o de una hormona específica». «De esta forma se acelera el diagnóstico y se reducen los desplazamientos del paciente»[29].

A pesar de sus posibilidades, las tecnologías emergentes también plantean desafíos relacionados con la privacidad de los datos, la regulación y la ética, que trataremos más adelante y deben abordarse adecuadamente para garantizar su éxito y seguridad.

III. CIENCIAS DE LA SALUD HUMANA Y VETERINARIA.

Las ciencias de la salud humana y veterinaria son campos de estudio relacionados que se centran en la salud y el bienestar de los seres humanos y de los animales, respectivamente. Aunque tratan diferentes especies, comparten similitudes en términos de biología, medicina y cuidado de la salud[30]. Aquí se delinea una visión general de cada campo:

Ciencias de la Salud Humana:

1. **Medicina:** La medicina es la disciplina que se enfoca en el diagnóstico, tratamiento y prevención de enfermedades y trastornos en seres humanos. Los médicos y otros profesionales de la salud trabajan en esta área y en sus diferentes especialidades: la medicina interna, la cirugía, la pe-

29 Así lo explica el investigador y empresario Teófilo Díez-Caballero, gerente de Biosensores S.L., la primera empresa privada dedicada a la I+D+i en este campo tecnológico que se creó en España. Morales, S.: "Biosensores o cómo el médico podrá detectar el tumor en la primera visita" en *El Mundo*, Castellón al día, viernes 13 de octubre de 2023.

30 La Ley 33/2011, de 4 de octubre, General de Salud Pública, estableció la necesidad de disponer de una Estrategia de Salud Pública (Estrategia de Salud Pública 2022, Mejorando la salud y el bienestar de la población, disponible en: https://www.sanidad.gob.es/ciudadanos/pdf/Estrategia_de_Salud_Publica_2022___Pendiente_de_NIPO.pdf) que sirva como herramienta para propiciar que la salud y la equidad en salud se consideren en todas las políticas públicas y se facilite la acción intersectorial en esta materia.

diatría, la ginecología, etc. y muchas otras especialidades para brindar atención médica a las personas.

2. **Enfermería:** Los enfermeros y enfermeras desempeñan un papel crucial en la atención al paciente, brindando cuidados directos, administrando medicamentos y colaborando con médicos y otros profesionales de la salud para garantizar el bienestar de los pacientes.
3. **Investigación Médica:** La investigación médica se dedica a comprender mejor las enfermedades, desarrollar ensayos y tratamientos para avanzar en la medicina. Los científicos médicos realizan investigaciones clínicas y de laboratorio para este propósito.
4. **Salud Pública:** Los profesionales de la salud pública trabajan en la prevención de enfermedades y en la promoción de la salud a nivel de la población. Esto incluye la vigilancia epidemiológica, la educación sobre la salud y la gestión de brotes de enfermedades.
5. **Farmacia:** Los farmacéuticos se especializan en la preparación y distribución de medicamentos, así como en asesorar a los pacientes sobre su uso adecuado y posibles efectos secundarios. En este ámbito la Inteligencia Artificial es utilizada para efectuar simulaciones y pruebas que reduzcan los costes de desarrollo de un potencial fármaco, mejorando así la capacidad predictiva de los distintos escenarios desarrollados junto a las pruebas y ensayos de laboratorio con simulaciones virtuales, analizando algoritmos con la modalidad de *machine working* e incrementando con la modalidad de autoaprendizaje el proceso de desarrollo de nuevos fármacos. Lo que supone acortar los plazos, ahorrar en inversiones y reducir los riesgos.

También se utiliza la IA en la selección de los pacientes para los ensayos clínicos y para la digitalización de la información (Big data). Las plataformas digitales que recopilan toda la información relevante la pasan del formato analógico al digital, permitiendo un tratamiento informatizado archivado *in cloud* de bases de datos interoperables con posibilidad de validación de datos con blockchain. Estos procesos secuencializados, oportunamente orquestados, crean un valor intríseco influyendo positivamente las métricas de valoración[31].

---

31 Moro-Visconti, R. "Le società MedTech e BioTech: piattaforme digitali, inteligenza artificiale e valutazione económica", en *Rivista Diritto di internet*, 2023, Anno V, n.1, pp. 194-195.

Ciencias de la Salud Veterinaria:

1. **Medicina Veterinaria:** La medicina veterinaria se centra en el diagnóstico y tratamiento de enfermedades y lesiones en animales. Los veterinarios pueden trabajar con mascotas, animales de granja, animales salvajes y de zoológico, entre otros.
2. **Investigación Veterinaria:** Los científicos veterinarios llevan a cabo investigaciones para comprender mejor la salud animal, desarrollar vacunas, tratamientos y técnicas de manejo.
3. **Cirugía Veterinaria:** Los cirujanos veterinarios realizan procedimientos quirúrgicos en animales para corregir afecciones médicas o traumatismos.
4. **Salud Pública Veterinaria:** Similar a la salud pública en humanos, la salud pública veterinaria se enfoca en prevenir y controlar enfermedades transmitidas por animales y en garantizar la seguridad alimentaria.
5. **Zoología y Conservación:** Los zoólogos y conservacionistas trabajan para entender y proteger la vida silvestre y los ecosistemas, contribuyendo a la conservación de especies en peligro de extinción.
6. **Medicina de Animales de Laboratorio:** Los veterinarios de animales de laboratorio brindan atención médica a animales utilizados en investigaciones científicas y se aseguran de que se cumplan las regulaciones de bienestar animal.

A pesar de las diferencias, las ciencias de la salud humana y veterinaria comparten conocimientos y técnicas en áreas como la anatomía, la fisiología y la farmacología. Además, ambos campos contribuyen al bienestar general de la sociedad y a la comprensión de las enfermedades y la salud pública[32] en un contexto más amplio y las nuevas tecnologías van a incidir en cada una de ellas generando nuevas expectativas y también cuestiones éticas y jurídicas que solventar. La estrategia mundial sobre salud digital 2020-2025 de la Organización Mundial de la Salud (OMS) persigue mejorar la salud de todos, acelerando el desarrollo y la adopción de soluciones de salud digital adecuadas, que sean accesibles, asequibles, y sostenibles centradas en las personas.

32 Con respecto al concepto de salud pública, vid. Cuadrado Ruiz, Mª Á., "Protección penal de la salud de los consumidores" en Martos Núñez, J. A. (coord.) *Protección penal y tutela jurisdiccional de la salud pública y del medio ambiente*, 1997, pp. 111-134.

IV. RETOS ÉTICOS Y RETOS LEGALES ANTE ESTAS NUEVAS TECNOLOGÍAS.

El avance de la tecnología en los distintos campos de las ciencias de la salud plantea numerosos desafíos éticos y también legales que deben abordarse de una manera efectiva para garantizar los derechos de los ciudadanos y de los pacientes, entre otros, la seguridad, la privacidad y la eficacia de las prácticas principalmente médicas. El peligro de estas tecnologías emergentes está en abusar en su uso "con fines ilícitos". Por ello, sobre todo ética en la investigación, esto es, que la práctica de la ciencia se realice conforme a principios éticos que aseguren el avance del conocimiento, la comprensión y mejora de la condición humana y el progreso de la sociedad.

De igual manera, se hace necesario incorporar la ética para proteger, entre otros, los derechos de propiedad intelectual en el uso de estas herramientas. Por ello, las autoridades han advertido sobre "los sesgos" que estas tecnologías presentan: "Debemos evitar que sustituyan una habilidad que es patrimonio de la Humanidad, que es diferenciar el bien del mal"[33].

Algunas cuestiones clave relacionadas con la salud y las nuevas tecnologías podrían ser:

1. **Regulación de dispositivos médicos:** La fabricación y el uso de dispositivos médicos avanzados, como robots quirúrgicos, implantes biomédicos y dispositivos de monitorización remota están sujetos a regulaciones estrictas en la mayoría de los países. Las agencias reguladoras, como la Administración de Alimentos y Medicamentos (FDA) en los Estados Unidos, establecen estándares para garantizar la seguridad y la eficacia de estos dispositivos.

2. Privacidad y seguridad de datos: La recopilación, el almacenamiento y el intercambio de datos médicos personales están sujetos a regulaciones de la privacidad de datos, como el Reglamento General de Protección de Datos (RGPD), en la Unión Europea, ya que las tecnologías emergentes, como la Inteligencia Artificial y el análisis de datos de salud masivos, plantean preocupaciones sobre la protección de la intimidad de los pacientes y la seguridad de los datos ante las actividades de los hackers para acceder a los mismos. Para

33 Llop, P., en el Seminario "Servicios Públicos de Justicia en tiempos de transformación", Madrid, octubre 2023.

Pilar Nicolás "la utilización y combinación de grandes volúmenes de datos representan, también en el ámbito de la biomedicina, oportunidades para la generación de conocimiento, para la solución de problemas y para mejorar las condiciones de vida de las personas. No obstante, reconocer las ventajas y las oportunidades que las nuevas tecnologías ofrecen ha de implicar, a la vez, una previsión y evaluación de las consecuencias que este nuevo escenario puede acarrear para los derechos de los individuos, si es que no se enmarca en unas garantías adecuadas. El RGPD Reglamento y la normativa española de desarrollo reconocen distintas cuestiones jurídicas, junto con el consentimiento del sujeto, para tratar los datos de carácter personal relativos a la salud y los datos genéticos, en particular cuando se trata de finalidad científica. Es importante subrayar que estas otras bases jurídicas no podrán sustentar el tratamiento si suponen que las garantías para los derechos de los titulares quedan debilitadas. Esta condición exige que los derechos del titular sobre sus datos estén nítidamente definidos y protegidos, lo que puede incluso significar un mecanismo que otorgue un control más reforzado que la expresión de un consentimiento"[34]. Asimismo la utilización de la tecnología Big data[35] en la práctica clínica puede suponer grandes avances para el sistema sanitario, tanto para la asistencia como para la investigación clínica. Para conseguir este objetivo es imprescindible la integración de las diferentes fuentes de información actualmente disponibles. De forma simultánea a estas ventajas potenciales, la aplicación de estas tecnologías puede suponer una fuerte amenaza para la intimidad, por lo que es imprescindible disponer de medidas adecuadas de control de la información, así como de un marco ético y jurídico adecuado, procedimientos transparentes y seguros, que garanticen compaginar la protección de datos con la investigación clínica relevante y la mejora de la asistencia y, a la

34 Nicolás Jiménez, P., "Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada,* nº extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), pp. 129-167.

35 Alcalde Bezhold, G., Alfonso Farnós , I., "Utilización de tecnología Big Data en investigación clínica" en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada,* nº extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), pp. 55-83.

vez, garanticen el máximo nivel de confidencialidad asegurando el respeto a los derechos y libertades de las personas.

3. Telesalud y atención médica *on line*: La expansión de la telesalud y la atención médica *on line* ha generado preguntas sobre la regulación de la práctica médica a distancia, la prescripción de medicamentos y la validez legal de las consultas médicas virtuales. Se deben adaptar las leyes existentes a estas nuevas formas de atención médica para evitar dudas si el acto médico se materializa recurriendo a la Telemedicina. Según Martínez Zaporta[36] deberían retocarse los Protocolos, aprobarse nuevos Códigos de Conductas, o elaborarse guías, una vez que se hayan evaluado las herramientas telemédicas y examinado el resultado de su uso.

4. Responsabilidad legal: La introducción de la Inteligencia Artificial en el diagnóstico y el tratamiento médico también plantea cuestiones de responsabilidad[37] legal en caso de errores o fallos del sistema. Establecer quién es responsable en caso de un diagnóstico erróneo o de un tratamiento inadecuado puede ser un desafío importante. A nivel europeo la armonización del derecho administrativo sancionador en los Estados miembros se ha llevado a cabo sectorialmente. Recientemente esta competencia se ha utilizado en el Reglamento general para la protección de datos[38] y en la Propuesta de la Comisión en materia de IA[39], previendo la posibilidad de imponer sanciones

---

36 Martínez Saporta, E., "Telemedicina y responsabilidad patrimonial de la Administración sanitaria", en *DS* Vol. 16, Número 1, Enero-Junio 2008, pp. 124 y ss, 126 y ss.

37 En este sentido, la Unidad de Excelencia de Investigación "Sociedad Digital: Seguridad y Protección de Derechos" (SD2), junto con el Departamento de Derecho Internacional Privado e Historia del Derecho de la Universidad de Granada, el 30 noviembre 2023, organizaron el curso: *ArtificiaI Intelligence, Law and Online Dispute Resolution,* impartido en inglés por el profesor John Zeleznikow, de la Universidad de La Trobe (Australia).

38 Reglamento 2016/679, del 27 de abril, sobre la Protección de las personas físicas en relación con la elaboración de datos personales, y sobre la circulación de tales datos, art. 83.6.

39 COM (2021)206, art.71. Vid supra p. 4 nota 17. COM(2021) 206 final, art. 72. Propuesta de Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión. Vid., de Miguel Beriain, "El uso de datos de salud para investigación biomédica a la luz de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios", en *Revista Jurídica de Castilla y León*, número 60. mayo 2023, p. 7 y ss.

de hasta 20 y 30 millones de euros, respectivamente[40]. En el Reglamento europeo en materia de mercados digitales[41] la Comisión tiene amplio poderes sancionatorios en relación con las plataformas *on line* de grandes dimensiones[42]. En concreto la Propuesta europea en materia de IA prevé que el Garante europeo para la protección de datos pueda imponer sanciones administrativas a las Instituciones, Agencias y otros organismos de la UE hasta 500.000,00€.

En España, el Real Decreto 729/2023, de 22 de agosto, aprobó el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial (la Agencia) que es una entidad de derecho público con sede en A Coruña. Establece que la efectiva puesta en funcionamiento de la Agencia se producirá con la constitución del Consejo Rector en el plazo máximo de 3 meses desde la entrada en vigor de este real decreto[43].

La Agencia estará encargada de la asunción de todas aquellas materias y competencias que deban ser asumidas por el Reino de España, como Estado miembro integrante de la Unión Europea (UE) en materia de Inteligencia Artificial, sobre todo las relacionadas con la supervisión. En efecto, se pretende dar cumplimiento a todas las obligaciones establecidas en la normativa europea y nacional.

Esta Agencia tiene como objetivos: "la supervisión, el asesoramiento, la concienciación y la formación dirigidas a entidades de derecho público y privado para la adecuada implementación de toda la normativa nacional y europea en torno al adecuado uso y desarrollo de los sistemas de IA, más concretamente, de los algoritmos. Además, tendrá la función de inspección, comprobación, sanción y demás que le atribuya la normativa europea que le resulte de aplicación y, en especial, en materia de inteligencia artificial. Todo ello sin menoscabo de las competencias y funciones que en este ámbito vienen ejerciendo el Ministerio de Sanidad y la Agencia Española de Medicamentos y

---

40 Vervaele, J.A.E., "Verso una rivalutazione europea dell´enforcement nel diritto punitivo?, en Revista *Diritto penale XXI secolo,* anno XXII, 1/23, p. 11.

41 Reglamento 2022/1925, arts. 65-83.

42 Vervaele, J.A.E., *Op. cit*, p. 38. En francés, el mismo, "Ver une réevaluation européenne du droit répressif?, *Revue de science criminelle et de droit pénal comparé*, jul-sep 2023, pp. 509 y ss.

43 Real Decreto 729/2023, de 22 de agosto. Disposición adicional primera. Constitución efectiva.

Productos Sanitarios, en el ámbito de los medicamentos, productos sanitarios y evaluación de nuevas tecnologías para inclusión en la Cartera de Servicios del Sistema Nacional de Salud así como el Ministerio de Trabajo y Economía Social y la Inspección de Trabajo y Seguridad Social, en su función de vigilancia del cumplimiento de las normas del orden social y exigencia de responsabilidades, en el ámbito de las relaciones laborales". Además la Agencia asume la minimización de los riesgos que puede suponer el uso de esta nueva tecnología, concretamente, riesgos para la integridad, la intimidad, la igualdad de trato y la no discriminación, en particular entre mujeres y hombres, y demás derechos fundamentales que pueden verse afectados por el mal uso de los sistemas. Asimismo se encargará del adecuado desarrollo y la potenciación de los sistemas de Inteligencia Artificial. Y, en concreto, la Agencia ejercerá las siguientes competencias[44]:

a) La promoción de entornos de prueba que permitan una correcta adaptación de sistemas innovadores de inteligencia artificial a los marcos jurídicos en vigor.

b) El apoyo al desarrollo y uso de sistemas de IA desde una doble perspectiva ambiental y sostenible: promoviendo un desarrollo y uso energéticamente eficiente e impulsando la adopción de esta tecnología para favorecer la resolución de problemas ambientales. Todo ello con el objetivo de fortalecer las sinergias entre las transiciones digital y ecológica para lograr modelos más sostenibles.

c) El apoyo al desarrollo y uso de sistemas de IA con perspectiva de género, incorporando el principio de igualdad de oportunidades entre mujeres y hombres en su diseño y ejecución y promoviendo la realización de evaluaciones de impacto capaces de identificar posibles sesgos discriminatorios por cualquiera de los motivos prohibidos por el ordenamiento jurídico. Todo ello con el objetivo de eliminar los sesgos discriminatorios de cualquier tipo y, en particular, los sesgos de género y los de índole étnico-racial.

d) La ayuda al fortalecimiento de la confianza en la tecnología y aplicación de la inteligencia artificial, a través de la creación de un marco de

44 Art. 10 del Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial aprobado por el RD 729/2023, de 22 de agosto.

certificación voluntario para entidades privadas, que permita ofrecer garantías sobre el diseño responsable de soluciones digitales y garantizar los estándares técnicos, evitando la sobrerregulación y permitiendo la innovación.

e) La instrumentalización de los mecanismos de identificación de tendencias y evaluación del impacto social en materia de IA.

f) El alineamiento y coordinación con iniciativas de terceros relacionadas con la aplicación de los sistemas de IA.

g) La creación de conocimiento, formación y difusión en relación con la inteligencia artificial ética y humanista, para mostrar tanto su potencial y oportunidades para el desarrollo socioeconómico, la innovación y la transformación del modelo productivo, como los retos, riesgos e incertidumbres que plantea su desarrollo y adopción.

h) La dinamización del mercado para potenciar iniciativas y prácticas innovadoras y transformadoras en el ámbito de la IA.

i) El impulso de la colaboración público-privada para favorecer la creación de marcos de acompañamiento en el sector de la IA con el fin de impulsar su desarrollo humanista y su correcto uso por parte del tejido productivo-empresarial.

j) La ayuda a la ejecución de programas en el ámbito de la IA a través de acuerdos, convenios o cualquier otro instrumento legalmente previsto para apoyar en la ejecución de programas relacionados con la inteligencia artificial.

k) La supervisión de los sistemas de IA para garantizar el cumplimiento de la normativa, tanto nacional como europea, sobre la inteligencia artificial que lleve aparejada el uso de esta tecnología, cuya competencia sea asumida por la Agencia. Más concretamente, le corresponderá la supervisión y, en su caso, sanción de acuerdo con lo estipulado en la normativa europea en lo que respecta a la supervisión de sistemas de IA. El diseño, ejercicio y evaluación de esta función de supervisión se realizará incorporando la perspectiva de género.

l) Cualquier otra función que pudiera ser atribuible a la Agencia por motivo de aplicación de la normativa nacional y europea que entre en vigor en relación al uso seguro y confiable de los sistemas de IA, así como

cualquier otra función derivada de los propios cambios disruptivos de esta tecnología que requiera nuevas actuaciones.

5. Y en general, la **digitalización de la justicia**[45]: las soluciones digitales para iniciar y seguir procedimientos judiciales, y el uso de tecnología de comunicación a distancia para audiencias orales son también aspectos, entre otros, a tener en cuenta en los que hay luces y sombras, avances y obstáculos.

V. MARCO CONSTITUCIONAL, DERECHOS HUMANOS FUNDAMENTALES Y RESPONSABILIDAD PENAL

La Constitución española de 1978 (CE) consagra en su Título I, Capítulo Segundo los Derechos y libertades, precedido por el art. 14, que dispone que los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social. En la Sección 1ª. Se proclaman los derechos fundamentales y las libertades públicas (arts. 15-29), entre los que podemos recordar el derecho a la vida, el derecho a la integridad física y moral (art. 15 CE), el derecho a la libertad y seguridad, (art. 17), el derecho a la producción y creación científica y técnica, la investigación (art. 20.1.b) y dentro de la sección 2ª, Derechos y deberes de los ciudadanos (arts. 30 a 38 CE) el derecho a la propiedad privada (art. 33) en el que incluimos el derecho a la propiedad intelectual e industrial y en el art. 38 se establece derecho a la libertad de empresa.

El artículo 18 incluye derechos fundamentales tan importantes como el derecho a la intimidad, a la privacidad o la inviolabilidad de las comunicaciones. Así dispone el art. 18:

"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

---

45 Vid. El Plan de Justicia 2030. Eficiencia procesal y digital. Los cambios que va a suponer y el impacto en los operadores jurídicos. 2030 Justice Plan (subtitulado EN): https://youtu.be/jEqrh3REly8. Al respecto en Italia, vid. MICHELETTI, D., "Algoritmi nomofilattici a confronto. Ufficio del massimario vs inteligenza artificiale", en *Rivista Studi Senesi*, III Serie LXIX (2023), fasc. 1, pp. 175-188.

2. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo por resolución judicial.
3. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

Ya en el Título IV -Del Gobierno y de la Administración-, la CE establece en el artículo 105 que:

"la Ley regulará: b. -El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

La exigencia de una legislación de protección de la intimidad y la privacidad emana del mismo texto constitucional, y en particular, frente al uso de la informática y las TICs. Aunque el art. 105 no menciona la naturaleza de esos -archivos y registros administrativos-, en la realidad del mundo en que vivimos, lo normal será que estén informatizados, y en ocasiones la transmisión de los datos será electrónica[46], digital, utilizando todo tipo de tecnologías de la comunicación.

Dentro del principios rectores de la política social y económica, -pieza clave del modelo de Estado social previsto en la Constitución de 1978, en el Título I, Capítulo III,- el artículo 43.1 reconoce el derecho a la protección de la salud (no derecho a la salud que vendría explicitado dentro de los derechos y libertades públicas como derecho a la integridad física y moral, art. 15 CE), lo que ha desarrollado en nuestro país uno de los mejores sistemas de salud pública del mundo. Asimismo compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios, estableciendo que la ley establecerá los derechos y deberes de todos al respecto. Además los poderes públicos fomentarán la educación sanitaria, la educación física y el deporte y facilitarán la adecuada utilización del ocio.

Es cierto que como apuntaba Tiedemann[47] "el orden de valores jurídico-constitucional y el orden legal jurídico-penal son espacios relativamente autó-

46 Cuadrado Ruiz, Mª Á., "Interceptaciones telefónicas y nuevas tecnologías", en Revista *Cuadernos Jurídicos,* n.1, 1992, p. 68-69.

47 Tiedemann, K., "Constitución y Derecho penal", en *Revista española de derecho constitucional*, año nº 11, nº 33, 1991, p. 148.

nomos, que tienen sus presupuestos respectivos en diferentes objetivos y finalidades del actuar humano, que muestran regulaciones diferenciadas y, en todo caso, que la Constitución concede al legislador ordinario un amplio margen de libertad para la configuración del ordenamiento penal, todo ello sin perjuicio de la validez teórica de postulados teóricos vinculantes como el de la «unidad del ordenamiento jurídico» o de expresiones como la de que el Derecho penal es la ley a través de la cual se realiza la Constitución".

Todos estos derechos fundamentales y principios rectores garantizados en la CE de alguna forma iluminan al Derecho penal y se "transforman" en bienes jurídicos objeto de esta rama del ordenamiento jurídico[48]. Ciertamente el Derecho penal tiene como misión la protección de bienes jurídicos, ya sean bienes de carácter individual (la vida, la salud individual, la integridad física y moral, el derecho a la intimidad, el patrimonio, la propiedad intelectual e industrial etc.) o bienes de carácter colectivo (la salud pública, el medio ambiente, la administración pública, la fe pública, la administración de justicia, el orden público, etc.)[49] que la Constitución garantiza principalmente en el Título I y en el resto de su articulado.

Pues bien, ¿qué tecnologías de Inteligencia Artificial pueden afectar a las libertades individuales, y a los derechos de los pacientes? ¿Cómo quedarán los usos de la Inteligencia Artificial para la investigación penal o en relación con las empresas u otras personas jurídicas? ¿Cómo nos afecta la ciberseguridad en relación con nuestra salud? ¿Cómo pueden perjudicar los sesgos a la igualdad y a las minorías en el acceso a la atención sanitaria?

Como expusiera Tiedemann, "un cierto ámbito de las cuestiones fundamentales de la dogmática penal están abiertas a la influencia directa del orden constitucional, es decir, en cierto modo se encuentran a la vez dentro de las fronteras de la Constitución y en vinculación con la Política criminal"[50]. Es por ello que el uso de nuevas tecnologías en el ámbito de la salud, y en con-

---

48 Así también Tiedemann, K, *op. cit*, p. 167: bienes jurídicos que coinciden sustancialmente con valores constitucionales fundamentales y bienes jurídicos que lo son en cuanto instrumentos o medios para la salvaguardia de los llamados derechos fundamentales.

49 Muchoz Conde/ García Arán, *Derecho penal. Parte general,* 11ª ed., 2022, p. 56 y ss*;* Ramacci, F., *Corso di diritto penale, Parte generale*, a cargo de Guerrini, R., Torino, 8ª ed., 2023, p. 25 y ss.

50 Tiedemann, K., *op. cit.* p.

creto de la Inteligencia Artificial, plantea no pocos retos penales y, asimismo, vinculados a la política criminal actual relacionados con la protección de datos[51], la seguridad, la privacidad y la eficacia de las prácticas médicas. Estos son algunos de los desafíos penales que pueden surgir:

Violación de la privacidad y de la intimidad: Hoy en día los sujetos, contenido, límite y garantías de estos derechos, ciertamente, no están suficientemente delimitados frente a los usos y abusos de las nuevas tecnologías, de la informática, de las interceptaciones telefónicas, de los accesos a datos almacenados en relación con las actividades técnicas e investigadoras de la empresa, secretos industriales, etc., en los que la privacidad de las personas y de los pacientes en particular pueden verse comprometida. Así, mientras unos estiman que el derecho a la intimidad, a la privacidad tiene como sujeto activo a la persona individual o jurídica y como sujeto pasivo tanto a los poderes públicos como a los ciudadanos, otros consideran que el derecho a la intimidad personal abarca también el conjunto de producciones y creaciones científicas y técnicas, que, con fines industriales y comerciales, se limitan al conocimiento de un número determinado de personas[52].

*Mientras que en el Título X del Libro II CP en relación con la intimidad, el descubrimiento y la revelación de secretos, el artículo 197. 2 CP castiga con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses al que sin estar autorizado, se apodere, utilice o modifique en perjuicio de un tercero datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. Agravándose la pena en el art. 197. 4 CP y castigándose con prisión de tres a cinco años cuando a) se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archi-

51 Nicolás Jiménez, P., «Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos», *Revista de derecho y genoma humano*: *genética, biotecnología y medicina avanzada,* núm. extra 1, 2019 (ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), pp. 129-167.

52 *Idem, op.cit.*, p. 68.

vos o registros o b) si se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, las penas se impondrán en su mitad superior.

Las personas jurídicas pueden ser tanto sujeto activo de estos delitos del Capítulo I del Título X en virtud del art. 197 quinques CP, cuanto sujeto pasivo, ya que lo dispuesto en ese Capítulo I del Título X será aplicable al que descubriere, revelare, o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos del Código penal (art. 200 CP.)

En cualquiera de estos casos de atentados a la privacidad o intimidad contra una persona física o jurídica, para proceder penalmente sería necesaria la denuncia de la persona agraviada o de su representante legal (art. 201.1 CP). No siendo precisa dicha denuncia cuando el delito afecte a los intereses generales, a una pluralidad de personas, o si la víctima es un menor o una persona con discapacidad o necesitada de especial protección. Tampoco será precisa la denuncia de la persona agraviada o de su representante legal cuando el sujeto activo fuese autoridad o funcionario público[53] cometiendo los delitos del Capítulo I del Título X , fuera de los casos permitidos por la ley, sin mediar causa legal por delito y prevaliéndose de su cargo. (art. 201.2 en relación con el art. 198 CP).

Estos delitos son de los pocos contenidos en el Código penal en los que el perdón del ofendido o de su representante legal extingue la acción penal (art. 201.3 CP), salvo que las personas ofendidas sean menores de edad o personas con discapacidad necesitas de especial protección. En esos casos, el perdón de la persona ofendida no extinguirá la responsabilidad criminal, al tratarse la intimidad y la privacidad como bienes jurídicos eminentemente personales (art. 130.5º CP).

*El derecho a la intimidad y privacidad personal también se referiría al conjunto de producciones y creaciones científicas y técnicas garantizadas en el artículo 20 de la CE. En estos casos patentes, ensayos clínicos, nuevos tratamientos o medicamentos o la utilización de novedosas técnicas quirúrgicas o asistenciales podrían verse afectadas. El Código penal sanciona los atentados contra la propiedad industrial en el Título XIII, Capítulo XI, Sección 2ª,

53 En cuanto al concepto de autoridad y funcionario público vid. Art. 24 Cp.

arts. 273-277 CP y en la Sección 1ª de ese Capítulo XI los delitos contra la propiedad intelectual, art. 270-272 CP. En estos delitos también cabe autoría por parte de personas jurídicas, en virtud de lo que se prevé en el artículo 288 CP[54]. Para proceder penalmente no se exige la denuncia de la persona agraviada o de su representante legal. Tampoco es posible en los delitos contra la propiedad industrial o la propiedad intelectual el perdón del ofendido.

Seguridad de datos, robo de información, acceso no autorizado a registros, extorsión, estafa: La recopilación y el almacenamiento de datos médicos personales en sistemas electrónicos pueden aumentar el riesgo de violaciones de la intimidad[55] y provocar brechas de seguridad, además de atentar contra la propiedad o el patrimonio de las personas, viéndose incluso comprometida la libertad de empresa.

---

54 Art. 288 Cp.: Cuando una persona jurídica sea responsable de los delitos del Capítulo XI, Título XIII Cp. se le impondrán las siguientes penas:

En el caso de los delitos previstos en los artículos 270, 271, 273, 274, 275, 276, 283, 286 del Cp.:

Multa del doble al cuádruple del beneficio obtenido, o que se hubiera podido obtener, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años. Multa del doble al cuádruple del beneficio obtenido, o que se hubiera podido obtener, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años.

Multa del doble al triple del beneficio obtenido, favorecido o que se hubiera podido obtener, en el resto de los casos.

En el caso de los delitos previstos en los artículos 277, 278, 279, 280, 281, 282, 282 bis, 284, 285, 285 bis, 285 quater y 286 bis al 286 quater del Cp.:

Multa de dos a cinco años, o del triple al quíntuple del beneficio obtenido o que se hubiere podido obtener si la cantidad resultante fuese más elevada, cuando el delito cometido por la persona física tiene prevista una pena de más de dos años de privación de libertad.

Multa de seis meses a dos años, o del tanto al duplo del beneficio obtenido o que se hubiere podido obtener si la cantidad resultante fuese más elevada, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis del Cp., en relación a las penas impuestas a las personas jurídicas, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33. Estas penas son la disolución de la persona jurídica (que producirá la pérdida definitiva de su personalidad jurídica), y la intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años.

55 Vid. supra.

La ciberseguridad es un bien jurídico protegible penalmente[56]. La omnipresencia de muchas actividades cibernéticas maliciosas hace necesario llevar a cabo un examen en profundidad de este problema. Pero también es necesario evaluar la cooperación desarrollada dentro de algunas organizaciones internacionales que suponga una mayor cooperación para prevenir y perseguir los ciberataques.

Los delitos cibernéticos[57], como el acceso no autorizado a registros médicos electrónicos o el robo de información de datos relativos a la salud, pueden dar lugar a investigaciones penales y responsabilidad penal. Esto fue precisamente lo que ocurrió el 5 de marzo de 2023 en el Hospital Clínic de Barcelona. Sufrió un ciberataque sustrayéndose muchísimos datos a la institución: datos de carácter personal de pacientes, de profesionales y de colaboradores. El grupo Ransom House reivindicó públicamente el ataque y aseguraron tener en su poder 4,4 terabytes de información sensible. Los datos a los que se accedió ilícitamente se usan para ser publicados en Internet, sin autorización de sus titulares. El director médico del Hospital Clínic, Antoni Castells, explicó que los "piratas" publicaron un enlace un su canal de Telegram para quien quisiera acceder libremente a los mismos, publicados en la 'darkweb'. Y por si alguien se dejaba llevar de la curiosidad, las autoridades advirtieron que compartir ese enlace o publicarlo podía ser asimismo un comportamiento delictivo "ya que puede interpretarse como que de esa forma se está ayudando a la difusión y mal uso de los datos". Y es que el art. 249. 2.a) del CP también considera estafa, el facilitar a terceros, la obtención o simplemente la posesión de datos para la comisión de una estafa[58], porque es entonces cuando otros ciberdelin-

---

56 Cfr. Segura Serrano/ Gordo García, *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio,* Granada, 2013. En relación con los delitos sexuales, vid. Navarro Cardoso, F., Montesdeoca Rodrígez, D., "La cibercriminalidad sexual juvenil como nueva forma de delincuencia", en

Revista penal México, nº. 19, 2021, pp. 37-58. Vid. Ampliamente, Romeo Casabona/ Rueda Martín, *Derecho penal, ciberseguridad, ciberdelitos e Inteligencia Artificial. Volumen I Ciberseguridad y ciberdelitos*, Granada 2023.

57 Tejada de la Fuente,E., Martín de la Escalera, A. M., en Díaz Fernández, A. M. (Dir.), *Conceptos fundamentales de inteligencia* (dir.), 2016, pp. 37-44.

58 Art. 249.2 Cp.: Serán castigados con las penas de prisión de seis meses a tres años: a) " los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos, o programas informáticos,

cuentes pueden usarlos para extorsionar (art. 243 CP)[59] a quien no quiere que se publiquen datos de su historial clínico u otros datos personales, no solo de pacientes, sino también de trabajadores, directivos y proveedores (nombres, direcciones, nóminas, historiales médicos, etc.). La filtración forma parte del mecanismo de extorsión para reclamar un rescate, como ocurrió en este caso en el que los piratas pidieron 4,5 millones de dólares. Es la primera vez que Ransom House[60] reconoce públicamente que es el responsable del ciberataque al Clínico, y contactó con los responsables del hospital para exigirles el pago. Cuando los atentados contra la intimidad y el derecho a la propia imagen se llevan a cabo en el seno de una organización o grupo criminal se agravarán las penas imponiéndose las superiores en grado[61]. Y para que no se hagan públicos estos datos las personas afectadas por la filtración de su historial médico pueden ser además víctimas de estafa[62]. **De estas defraudaciones pueden ser responsables penalmente las personas jurídicas en virtud del art. 251 bis**

o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo". b) Los que para su utilización fraudulenta sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago materia o inmaterial distinto del efectivo".

59 Art. 243 Cp.: "El que con ánimo de lucro obligare a otro, con violencia o intimidación a realizar u omitir un acto o negocio jurídico, en perjuicio de su patrimonio o de un tercero, será castigado con la pena de prisión de uno a cinco años, sin perjuicio de las que pudieran imponerse, por los actos de violencia física realizados".

60 Ransom House es una banda de cibercriminales que trabaja desde fuera de España y está especializada en ataques ransomware. Se trata de un programa dañino que consigue restringir el acceso a determinadas partes o archivos del sistema operativo infectado. Incluso, existen tipos de ransomware que cifran los archivos del sistema operativo y llegan a inutilizar el dispositivo, coaccionando al usuario para que pague el rescate.

61 Art. 197 quarter Cp.

62 Art. 248 Cp.: "Cometen estafa los que con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno". Se impondrá una pena de prisión de seis meses a tres años y si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses.

Art. 249.1 Cp: "También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años a) los que con ánimo de lucro obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información, o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos, o valiéndose de cualquier otra manipulación informática, o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".

CP y del 197 quinquies CP, cuando se trate de delitos contra la intimidad o el derecho a la propia imagen[63]**.**

Desgraciadamente cada vez hay más ataques en el entorno sanitario en general, no solo en España[64], sino también a nivel europeo[65].

Acceso no autorizado y delitos contra la propiedad intelectual y patentes: Ya hemos visto como en el acceso a datos llevado a cabo por Ramson House no se trataba solo de datos personales sino que también esos datos pueden ser ensayos clínicos o patentes contra otras enfermedades, lo que podría vulnerar los derechos de propiedad industrial y patentes. Asimismo la tecnología médica y los dispositivos de salud a menudo también están protegidos por derechos de propiedad intelectual, como patentes y derechos de autor. Los actos de piratería informática o la infracción de estos derechos pueden ser objeto de responsabilidad penal, como ya se ha mencionado, en virtud de los delitos contra la propiedad industrial en el Título XIII, Capítulo XI, Sección 2ª, arts. 273-277 CP y en la Sección 1ª de ese Capítulo XI los delitos contra la propiedad intelectual, art. 270-272 CP. En estos delitos también cabe autoría por parte de personas jurídicas en virtud de lo que se prevé en el artículo 288 CP. No obstante la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios señala en el punto 4 del artículo 33 que:

> «Los datos sanitarios electrónicos que conlleven derechos de propiedad intelectual e industrial protegidos y secretos comerciales de empresas privadas se pondrán a disposición para un uso secundario. Cuando dichos datos se pongan a disposición para un uso secundario, se adoptarán todas las medidas necesarias para preservar la confidencialidad de

63 Título X, Libro II Cp.: *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio.*

64 Con anterioridad, en noviembre de 2022, Ransom House atacó en esta ocasión al Hospital Universitario Son Espases, de Mallorca y exigió 4 millones de euros por liberar sus datos. Otros de sus objetivos han sido instituciones públicas y privadas en diferentes países.

65 En el ámbito sanitario, 2023 fue un año fuertemente marcado por los ciberataques. Un informe de ENISA (la Agencia de Ciberseguridad de la Unión Europea) muestra que los ciberataques se duplicaron en el primer trimestre de 2023: 40 incidentes, frente a una media de 22 en los primeros tres meses de 2021 y 2022, siendo los objetivos no solo los hospitales, sino también los proveedores de servicios.

los derechos de propiedad intelectual e industrial y los secretos comerciales»

Lo que puede suponer una clara merma en los derechos de los titulares de los datos, ya que se verán obligados a ponerlos a disposición de un tercero, en las condiciones que determina la Propuesta, aunque sea en contra de su voluntad[66].

Prácticas médicas fraudulentas: El uso indebido de tecnologías médicas, como la telemedicina pueden utilizarse para cometer otras defraudaciones, como la facturación fraudulenta de servicios médicos, el ofrecimiento de servicios tecnológicamente innovadores en el área biomédica o como el ofrecimiento de análisis genéticos, que puede resultar asimismo delictivos, en virtud del art. 249.2 y 3 CP.[67].

Responsabilidad penal en la toma de decisiones médicas asistidas por Inteligencia Artificial: A medida que la IA se utiliza para el diagnóstico y el tratamiento médico, surgen preguntas sobre la responsabilidad legal en caso de errores o decisiones perjudiciales. Determinar quién es responsable: el médico, el fabricante del software o ambos, puede ser un desafío legal importante[68]. Por ello, Íñigo de Miguel propone frente al uso de mecanismos de decisión automatizada, "dotar tanto a los profesionales sanitarios como a los

66 de Miguel Beriain, I., "El uso de datos de salud para investigación biomédica a la luz de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios", en *Revista Jurídica de Castilla y León*, número 60. mayo 2023, p. 34-35.

67 Vid. supra nota 37. Art. 249. 3 "Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo". Al respecto vid Jorqui Azofra, M., Nicolás Jiménez, P., "¿Estafa en el ofrecimiento de servicios tecnológicamente innovadores en el área biomédica?: especial consideración del ofrecimiento de análisis genéticos", en Romeo Casabona, C., (ed. lit.), Flores Mendoza, F., (ed. lit.), *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica*, 2012, pp. 221-252.

68 Romeo Casabona, C.M., "La atribución de responsabilidad penal por los hechos cometidos por sistemas autónomos inteligentes, robótica y tecnologías conexas", en VVAA, *Estudios político criminales, jurídico penales y criminológicos: libro homenaje al Prof. José Luis Díaz Ripollés,* 2023, pp. 721-733.

pacientes de herramientas que en la práctica sirvan para evitar que se tomen decisiones sobre terceros sin su intervención directa. La implementación de figuras nuevas que sirvan de intermediadores, o la creación de un derecho a la objeción de conciencia relacionado con el uso de estos mecanismos resultan particularmente interesantes en este sentido"[69].

La doctrina ha establecido cuatro grupos de posibles delitos relacionados con la IA: a) delitos cometidos dolosamente por personas físicas o jurídicas, con uso deliberado de la IA; b) delitos imprudentes originados por deficiencias o fallos en la cadena productiva y/o uso de la IA; c) ilícitos provocados por la propia IA, sin intervención humana; d) ilícitos cometidos por seres humanos, instrumentalizados por la IA[70].

En el caso de delitos con intervención de IA, ¿sería penalmente responsable la persona jurídica que la produjo?[71]. Respondiendo a esta cuestión, podemos afirmar que las empresas asumen un papel destacado en los casos en que la intervención de la IA tenga relevancia penal, ya sea por causar el daño, o por la información que contiene y en determinados casos, esas empresas o laboratorios también podrán ser responsables penalmente. Por ejemplo, en el caso de estafas o defraudaciones en virtud del art. 251bis CP, una persona jurídica puede responder penalmente[72].

---

69 Cfr. De Miguel Beriain, I., *Un estudio de impacto ético y social de las nuevas tecnología en la práctica de la biomedicina*, 2021, Tesis doctoral disponible en https://addi.ehu.es/handle/10810/54337.

70 Pagallo, U., Quattrocolo, S.: "The Impact of AI on Criminal Law and its Twofold Procedures", en Barfield, W., Pagallo, U. (eds.), *Research Handbook on the law of artificial intelligence*, Cheltenham, 2018, pág. 404.

71 Januário, T. F. X., "Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales", en Revista *Estudios Penales y Criminológicos.*, 44(ext), 2023.

72 Art. 251 bis Cp.: "Cuando de acuerdo con lo establecido en el art. 31 bis una persona jurídica sea responsable de los delitos comprendidos en esta Sección (*De las defraudaciones)* se le impondrán las siguientes penas: a) Multa del triple al quíntuple de la cantidad defraudada, si el delito cometido por la persona física tiene una pena de prisión de más de cinco años. b) multa del doble al cuádruple de la cantidad defraudada, en el resto de los casos. Asimismo, atendidas las reglas del art. 66 bis, los jueces y tribunales podrán imponer las penas recogidas en los apartados b) a g) del art. 33.7 Cp.

Delitos relativos a la manipulación genética en la investigación y experimentación: La investigación médica con el uso de tecnologías emergentes, como la edición genética, debe cumplir con estrictas pautas éticas y regulaciones legales. Por ejemplo, la edición genética y la clonación, plantean cuestiones éticas y legales sobre la manipulación genética y la creación de seres humanos modificados genéticamente. La clonación reproductiva en seres humanos resulta ser una práctica éticamente inaceptable ya que los individuos clónicos son medios para un determinado fin. La identidad única del ser clónico queda violada. A pesar de que existen declaraciones y convenios internacionales que tratan de responder de forma efectiva en torno a la condena y prohibición de la clonación en seres humanos, sin embargo, dichos textos no llegan a tener una fuerza legal suficiente ante la prohibición de la clonación a nivel mundial.

Los experimentos médicos no éticos pueden dar lugar a delitos y a sus correspondientes sanciones. En concreto, el Título V del Libro II del Código penal se refiere a los *Delitos relativos a la manipulación genética*[73], artículos 159-162 CP entre los que se incluye la utilización de ingeniería genética para producir armas biológicas o exterminadoras de la especie humana, en el art. 160.1 CP.[74], la fecundación de óvulos humanos con fines distintos de la procreación humana, en el art. 160.2 CP. o la creación de seres humanos idénticos por clonación[75], castigada en el art. 160.3 CP.

Homicidio y/o lesiones por imprudencia: La vida y la salud individual también pueden correr riesgos por el uso de la IA u otras técnicas. En casos de negligencia grave o imprudencia en el uso de tecnologías médicas, como pueda ser en la cirugía robótica, u otras, puede surgir la posibilidad de imputaciones por delitos de homicidio imprudente. En los casos en los que se produzca la muerte de una persona por impericia, falta del cuidado debido en el uso de estas tecnologías, en el manejo de los robots en una cirugía con resultado muerte etc., podría imputarse por homicidio por imprudencia grave

---

73 Cuadrado Ruiz, M. Á., "Manipulaciones genéticas, armas biológicas y Bioterrorismo" en Revista Bioética y Ciencias de la Salud, Vol. 7 (2) 2019.Julio-Diciembre.Disponible en https://saib.es/manipulaciones-geneticas-armas-biologicas-y-bioterrorismo/

74 Vid. al respecto Cuadrado Ruiz, *Armas biológicas. Aspectos legales,* Granada, 2011.

75 Huguet Santos, P., *Clonación humana: aspectos bioéticos y legales*, 2005 Tesis doctoral disponible en https://hdl.handle.net/20.500.14352/55804; de Miguel Beriain, I., *La clonación, diez años después*, Cátedra de Derecho y Genoma Humano, 2008

en virtud del art. 142.1 CP o menos grave en el art. 142.2 CP. Si no llega a producirse la muerte, pero sí lesiones personales graves, podría aplicarse el delito de lesiones por imprudencia grave, del art. 152.1CP. o de lesiones por imprudencia menos graves del art. 152.2 CP[76]. En los casos de imprudencia menos grave el delito (ya sea de homicidio, 142.2 *in fine* o de lesiones 152.2 *in fine*) solo será perseguible mediante la denuncia de la persona agraviada o de su representante legal. También el Juez o Tribunal podrá imponer motivadamente la pena superior en un grado, en la extensión que estime conveniente, si el hecho revistiere notoria gravedad, en atención a la singular entidad y al riesgo creado y en atención al deber de cuidado infringido, ocasionando lesiones constitutivas del delito del artículo 152.1.2º o 3º CP. Y si el número de lesionados fuese muy importante, las penas podrían elevarse hasta en dos grados (art. 152 bis CP).

También son condenables penalmente con la pena de prisión de seis meses a tres años, todas las actividades de distribución o de difusión pública a través de internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos (lo que incluiría a la IA) que pudiera promover, fomentar o incitar a la autolesión de personas menores de edad o personas con discapacidad necesitadas de especial protección. Las autoridades judiciales ordenarán en estos supuestos la adopción de medidas necesarias para la retirada de dichos contenidos, la interrupción de los servicios que los ofrezcan o para el bloqueo de unos y otros cuando radiquen en el extranjero (156 ter CP).

---

76 Art. 142 Cp.: 1. "El que por imprudencia grave, causare la muerte de otro será castigado como reo de homicidio imprudente, con la pena de prisión de uno a cuatro años. (…) Si el homicidio imprudente se hubiese cometido por imprudencia profesional, se impondrá además la pena de inhabilitación especial para el ejercicio de la profesión, oficio o cargo, por un período de tres a seis años". 2. "El que por imprudencia menos grave causare la muerte de otro será castigado con la pena de multa de tres meses a dieciocho meses."

Art. 152 Cp.: 1. "El que por imprudencia grave causare alguna de las lesiones previstas en los artículos anteriores, será castigado, en atención al riesgo creado y al resultado producido: 1º con pena de prisión de tres a seis meses o multa de seis a dieciocho meses si se tratare de las lesiones del apartado 1 del artículo 147. 2º con la pena de prisión de uno a tres años, si se tratare de las lesiones del artículo 149. 3º con la pena de prisión de seis meses a dos años, si se tratare de las lesiones del artículo 150. 2. El que por imprudencia menos grave causare alguna de las lesiones a las que se refiere el artículo 147.1, será castigado con la pena de multa de uno a dos meses, y si se causaren las lesiones a las que se refiere el artículo 149 y 150 será castigado con la pena de multa de tres a doce meses".

Falsificación de registros médicos y documentos médicos: La falsificación de registros médicos o documentos médicos, ya sea para obtener beneficios médicos indebidos o para encubrir negligencia médica, puede dar lugar a responsabilidad penal. Las situaciones en las que la alteración o falsificación de registros médicos se considerarían penalmente relevantes podrían enumerarse como:

1. Falsificación de firmas del personal facultativo y/o del paciente dentro de los registros médicos del sistema público de salud. Al considerarse documentos[77] públicos estos hechos podrían dar lugar a un delito de falsedad documental, tipificado en el artículo 390CP, si los autores son autoridad o funcionario público, que conlleva una pena privativa de libertad de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial por tiempo de dos a seis años. Si se llevasen a cabo estas conductas por imprudencia grave, en virtud del art. 391CP la pena sería de multa de seis a doce meses y suspensión de empleo o cargo público por tiempo de seis meses a un año. Si se tratase documentos privados la pena de prisión sería de seis meses a dos años, art. 395 CP.

2. En caso de que se alteren, se simulen en todo o en parte o suponiendo que han intervenido o realizado manifestaciones en un acto o documentos médicos públicos, o se faltare a la verdad en la narración de los hechos se incurrirían en las mismas penas por el delito del art. 390 CP, siempre que los autores sean autoridad o funcionario público. Y con las penas del artículo 395 CP si se tratase de documentos privados. Si es un particular el que lleva a cabo la falsedad del art. 390 CP se le castigará con la pena de prisión de seis meses a tres años y multa de seis a doce meses, en virtud del art. 392 CP.

3. El uso del documento médico sanitario falso, por el que a sabiendas de su falsedad, o para perjudicar a otro será castigado con pena inferior en grado a la de los falsificadores, art. 393 CP. Con igual pena se castigará al que a sabiendas de su falsedad presentare en un juicio documentos o registros clínicos con la finalidad de inducir al engaño al juzgador, estaría incurriendo en dos delitos, el de falsificación y uso de documento falso y el de obstrucción a la justicia del art. 464.2 CP; en este escenario, se aplicará el concurso ideal de delitos Si se

77 A los efectos penales, el Código penal español considera documento "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica", en virtud de los dispuesto en el art. 26 Cp.

tratare de documentos médicos falsos de carácter privado, al que presentare en un juicio, o para perjudicar a otro hiciere uso de ellos, a sabiendas de la falsedad, se le castigará con la pena de prisión de un año y multa de tres a seis meses, según lo dispuesto en el art. 392.2 CP.

4. Si un facultativo consigna datos falsos en certificados médicos será castigado con la pena de multa de tres a doce meses, art. 397 CP. Pero si la certificación falsa tiene escasa trascendencia en el tráfico jurídico será castigado con la pena de suspensión de seis meses a dos años, art. 398 CP.

5. Cuando sea una persona particular quien falsifique una certificación o la utilice con fines comerciales o sin haber intervenido en su falsificación la use con el fin de conseguir sustancias estupefacientes, psicotrópicas o preparados que las contengan, etc., es decir, trafique con ella de cualquier modo, se estaría cometiendo un delito de falsificación de certificados contenido en el art. 399.1 y .2 CP, sancionado con pena de multa de tres a seis meses. Y esta pena será también aplicable cuando el certificado aparezca como perteneciente a otro Estado de la Unión Europea o a un tercer Estado o haya sido falsificado o adquirido en otro Estado de la Unión Europea o en un tercer Estado, si es utilizado en España, art. 399.3 CP.

En definitiva, la alteración o falsificación de documentos médicos y sanitarios o incluso su uso sin haber participado o realizado la falsedad relativa a registros clínicos que contienen información de salud puede dar lugar a graves consecuencias legales y penales para quien las perpetren; es por lo que siempre es recomendable trabajar éticamente, siguiendo los protocolos de seguridad del paciente y de la historia clínica, plasmando notas de evolución claras, completas y precisas, junto a firmas y nombres de responsabilidad legibles, que no den lugar a dudas sobre la veracidad del documento.

Delitos relacionados con los medicamentos[78]: El uso de la telemedicina y las tecnologías de prescripción electrónica también pueden plantear cuestiones de responsabilidad penal en la prescripción de medicamentos, especialmente en el caso de medicamentos incluidos los de uso humano y veterinario, así como aquellos medicamentos en investigación que carezcan aún de la necesaria autorización exigida por la ley o que incumplan las exigencias técnicas

78 Cuadrado Ruiz, Mª Á., "La protección penal de los medicamentos", en Revista *Cuadernos Jurídicos,* n. 7, 1993, pág. 59 y ss.

relativas a su composición, estabilidad y eficacia y con ello se genere un riesgo para la vida o la salud de las personas, pudiendo ser castigados tanto las personas físicas como las jurídicas por estos hechos, en virtud del art. 361 CP con las penas de prisión de tres meses a tres años, multa de seis a doce meses e inhabilitación especial para profesión u oficio por tiempo de tres meses a tres años. Para las empresas, u otras personas jurídicas el art. 366 CP establece de acuerdo con lo dispuesto en el art. 31 bis CP cuando sean responsables de los delitos contra la salud pública (Título XVII, cap. III CP) una pena de multa de uno a tres años o del doble al quíntuplo del valor de las sustancias y productos a que se refieren los artículos 359 y ss. CP o del beneficio que se hubiere obtenido o podido obtener, aplicándose la cantidad que resulte más elevada. Asimismo, los jueces y tribunales podrán imponer las penas recogidas en las letras b) a g) del artículo 33.7 CP.

Asimismo, la producción o comercialización ilícita de productos sanitarios o dispositivos médicos no aprobados así como los accesorios o elementos que sean necesarios para su integridad y se presenten engañosamente, o la elaboración de medicamentos sin autorización, puede conllevar de igual manera a sanciones penales en virtud del art. 361 CP 1 a) b) de seis meses a cuatro años de prisión, multa de seis a dieciocho meses e inhabilitación especial para profesión u oficio de uno a tres años.

Es importante que los profesionales de la salud, quienes desarrollan productos sanitarios, ensayos u otra tecnología médica y las organizaciones de atención médica sean conscientes de estos desafíos penales y trabajen en colaboración con expertos legales para garantizar el cumplimiento de las leyes y regulaciones aplicables, así como de llevar la ética a la práctica médica.

La Inteligencia Artificial puede, asimismo, producir situaciones **discriminatorias por razón de género o raza,** o religión, entre otras. Dependiendo del tipo de datos que se introduzcan para crear los algoritmos que se están utilizando en asistencia sanitaria, por ejemplo, datos procedentes de historias clínicas recabadas en un contexto en que la población era mayoritariamente de una etnia homogénea y luego se utilicen en poblaciones más heterogéneas o incluso minoritarias haría que resultasen mucho menos eficaces, ya que los estudios estarían sesgados por el factor étnico. Es más que probable que las herramientas de IA reproducirán este problema. Pero, de ser así, será muy

complejo garantizar una igualdad real en el acceso a los recursos reales del sistema sanitario[79].

La legislación europea se desarrolla *ad hoc* para diferentes ámbitos, y no existen criterios homogéneos para todos los casos. Además los diferentes factores técnicos y de procesamiento de datos incrementan los factores de discriminación[80]. Hasta el momento, el análisis se ha centrado en el análisis legislativo y técnico para determinar si ha habido discriminación algorítmica. Sin embargo, el factor humano en el desarrollo y el uso que se haga de estas tecnologías también influye. Es por esto que se propone una metodología de análisis que tenga en cuenta todos estos factores para asegurar el respeto al derecho a la igualdad desde el inicio de la creación de la Inteligencia Artificial, teniendo en cuenta la tecnología a aplicar, el contexto en el que se utiliza, la fase operativa de la Inteligencia Artificial y el sujeto que interactúa con ella, con el fin de respetar la regulación europea de esta tecnología y las directrices éticas de la Comisión Europea[81].

Desde el ámbito penal estas circunstancias discriminatorias podrían modificar la responsabilidad penal mediante la aplicación de las circunstancias modificativas de la responsabilidad criminal como la agravante contenida en el apartado 4º del art. 22 CP : cometer el delito por cualquier clase de discriminación relativa a la etnia, raza o nación a la que se pertenezca, sexo, edad, identidad sexual o de género o por razón de género, aporofobia o exclusión social, la enfermedad que padezca o su discapacidad, con independencia de

---

79 Así, de Miguel Beriain, I., "Medicina personalizada, algoritmos predictivos y utilización de sistemas de decisión automatizados en asistencia sanitaria. Problemas éticos", en Revista *Dilemata,* Nº. 30, 2019 (Ejemplar dedicado a: Ética, robótica y tecnologías asistenciales), p. 102.

80 La discriminación, respetando los términos del Convenio 111 de la OIT y de las Directivas 2000/43/CE, 2000/78/CE, 2002/73/CE, 2004/113/CE o 2006/54/CE, consiste en conferir un trato menos favorable a una persona que aquél que se confiere a personas en situación comparable, por razón de alguna condición personal. Desde esta óptica, podría entenderse que un delito de odio es muestra de discriminación en tanto que produce efectos discriminatorios.

81 Legind Larsen, H., y otros, *Flexible Querry Answering Systen*: 15th International Conference, FQAS 2023, Mallorca, Spain, September 5–7, 2023, Proceedings. Vid. Capítulo "Methodology for Analyzing the Risk of Algorithmic Discrimination from a Legal and Technical Point of View".

que tales condiciones o circunstancias concurran efectivamente sobre la persona sobre la que recaiga la conducta. Aunque nuestro Código Penal no regula expresamente en ningún Título o Capítulo los "delitos de odio", y desde luego no los define ni menciona como tal, se considera que lo son todos aquellos a los que sea de aplicación la circunstancia agravante genérica del artículo 22.4ª CP y varios tipos penales de la Parte Especial, como el tipo penal del artículo 510 CP.

También la Inteligencia Artificial y otras herramientas que están surgiendo pueden aplicarse en relación con el artículo 510.1 CP, en el que se establece que el castigo para quienes promuevan la discriminación, el odio, la hostilidad o la violencia contra un grupo, parte del mismo o contra una persona por razón de su pertenencia a aquel, por motivos racistas u otros, o por su origen nacional, su sexo, orientación o identidad sexual, por razones de género, aporofobia, enfermedad o discapacidad sea de pena de prisión de uno a cuatro años y una multa de 6 a 12 meses[82]. El odio, en el sentido en que se emplea en estos delitos (implicando un especial ataque a la dignidad humana como derecho fundamental de la persona, fundamento del orden político y de la paz social -artículo 10 CE-), se emplea en el sentido clásico de "deseo de un mal, originado en un prejuicio o sesgo de intolerancia contra una determinada clase de personas y, en su caso, contra la concreta persona que comparte las características que generan ese deseo[83].

Seguramente en los próximos años –o quizás en menos tiempo- comprobaremos si la automatización aplicada por la IA y otras tecnologías en la práctica de las ciencias de la salud aumentará la eficiencia o la ineficiencia tanto en ámbitos públicos (Administración sanitaria, hospitales públicos, etc.) como en el sector privado (como empresas y laboratorios farmacéuticos, etc.) y si tales hechos lesionan los derechos fundamentales y si son constitutivos de delitos.

---

82 Policías, investigadores y plataformas digitales explicaron los últimos avances en Inteligencia Artificial en la lucha contra los delitos de odio, con el objetivo de articular una Estrategia Europea y colaborar en la posible creación de una Red de Expertos a nivel del Consejo Europeo en el coloquio organizado por el Ministerio del Interior en Madrid los días 4 - 5 octubre 2023, "Uso de la Inteligencia Artificial para hacer frente a los delitos de odio".

83 Díaz López, J. A., *Informe de delimitación conceptual en materia de delitos de odio*. Madrid. Ministerio del Interior pp. 9-10.

VI. CONCLUSIONES

Las regulaciones y las políticas específicas pueden variar, pero en general, se deberían centran en garantizar los Derechos humanos, la seguridad, la privacidad y la eficacia de las prácticas y tecnologías médicas que se están desarrollando y aplicando por la IA y otras tecnologías emergentes en ciencias de la salud. Se trata de un campo en constante evolución que busca equilibrar la innovación tecnológica con la protección de la salud pública, garantizar los derechos individuales y la mejor sostenibilidad de dicho sistema de protección.

A medida que la tecnología avanza, es importante que la atención médica esté disponible y sea asequible para todos. Esto puede requerir políticas y normativas que promuevan el acceso y la equidad en la atención médica.

Los riesgos relacionados con ataques a la ciberseguridad u otros bienes jurídicos deben prevenirse y perseguirse de manera eficaz, también desde el ámbito penal.

La formación de profesionales de la salud en el uso de tecnologías emergentes, de la IA y la actualización de sus habilidades pueden requerir cambios en los planes de estudio de las Facultades de Medicina, Enfermería, Farmacia, Veterinaria y otros grados y Másteres así como en las regulaciones para garantizar la seguridad y la competencia. Por ello, la educación y la realización de prácticas así como la formación ética y legal también son fundamentales para abordar estos desafíos. El manejo de estas herramientas debería iniciarse al comenzar los estudios para así fortalecer un uso adecuado de los mismos y convertirse en una formación continua, ya que la evolución tecnológica supondrá que soluciones válidas a día de hoy queden obsoletas en los próximos años.

En definitiva, "es necesario ser conscientes de las rápidas transformaciones que están ocurriendo y gestionarlas de modo que se puedan salvaguardar los derechos humanos fundamentales, respetando las instituciones y las leyes que promueven el desarrollo humano integral. La Inteligencia Artificial debería estar al servicio de un mejor potencial humano y de nuestras más altas aspiraciones, no en competencia con ellos"[84].

---

84 Francisco, *op. cit*, 2. El futuro de la inteligencia artificial entre promesas y riesgos, *in fine*,

VII. BIBLIOGRAFÍA

ALCALDE BEZHOLD, G., ALFONSO FARNÓS, I., "Utilización de tecnología Big Data en investigación clínica" en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, nº extra 1, 2019 (Ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), pp. 55-83.

BERTOLASO, M., proyecto *Healthcare 5.0: New perspectives in healthcare innovation and assessment* (octubre 2022-marzo 2024), Università Campus Bio-Medico di Roma.

BERMUDEZ, BERMUDEZ, Y., "La responsabilidad penal derivada por las infracciones al DIH cometidas por sistemas de inteligencia artificial en el marco de una operación militar, en Revista *Ratio Juris UNAULA,* 2023.

CUADRADO RUIZ, Mª. Á., "Interceptaciones telefónicas y nuevas tecnologías", en Revista *Cuadernos Jurídicos*, n. 1, 1992, pp. 66 y ss.

CUADRADO RUIZ, Mª. Á., "La protección penal de los medicamentos", en Revista *Cuadernos Jurídicos,* n. 7, 1993, pp. 59 y ss.

CUADRADO RUIZ, Mª Á., "Protección penal de la salud de los consumidores" en Martos Núñez, J. A. (coord.) *Protección penal y tutela jurisdiccional de la salud pública y del medio ambiente*, 1997, pp. 111 y ss.

CUADRADO RUIZ, Mª .A., *Armas biológicas. Aspectos legales*, Granada, 2011.

CUADRADO RUIZ, Mª. Á., CUADRADO RUIZ, M. Á., "Manipulaciones genéticas, armas biológicas y Bioterrorismo" en Revista *Bioética y Ciencias de la Salud*, Vol. 7 (2) 2019, Julio-Diciembre. Disponible en https://saib.es/manipulaciones-geneticas-armas-biologicas-y-bioterrorismo/

DE MIGUEL BERIAIN, I., "Medicina personalizada, algoritmos predictivos y utilización de sistemas de decisión automatizados en asistencia sanitaria. Problemas éticos", en Revista *Dilemata,* Nº. 30, 2019 (Ejemplar dedicado a: Ética, robótica y tecnologías asistenciales), págs. 93-109.

DE MIGUEL BERIAIN, I., LAZCOZ MORATINOS, G., "Inteligencia artificial, personas mayores y biomedicina: la vulnerabilidad en el debate ético-jurídico" en ALKORTA IDIAKEZ, I. (dir.), ATIENZA MACÍAS, E.,

(coord.), *Soluciones tecnológicas para los problemas ligados al envejecimiento: cuestiones éticas y jurídicas*, 2020, pp. 115-137.

DE MIGUEL BERIAIN, I., *Un estudio de impacto ético y social de las nuevas tecnologías en la práctica de la biomedicina*, 2021, Tesis doctoral disponible en https://addi.ehu.es/handle/10810/54337.

DE MIGUEL BERIAIN, I., "El uso de datos de salud para investigación biomédica a la luz de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios", en *Revista Jurídica de Castilla y León*, número 60. mayo 2023, p. 7 y ss.

DÍAZ FERNÁNDEZ, A. M., (dir.), *Diccionario LID Inteligencia y seguridad*: *estructuras de inteligencia, fuentes, análisis, diseminación y operaciones encubiertas*, Ministerio de Defensa, Centro de publicaciones, 2013.

DÍAZ FERNÁNDEZ, A. M., (Dir.), *Conceptos fundamentales de inteligencia*, 2016.

DÍAZ LÓPEZ, J. A., *Informe de delimitación conceptual en materia de delitos de odio.* Madrid. Ministerio del Interior

GAVILÁN, I, "Robots humanoides: desafíos éticos y normativos diferenciales", en Arellano Toledo, V. (Dir.), *Derecho, Ética e Inteligencia Artificial*, Valencia, 2023.

HUGUET SANTOS, P., *Clonación humana: aspectos bioéticos y legales*, 2005. Tesis doctoral disponible en https://hdl.handle.net/20.500.14352/55804.

JANUÁRIO, Túlio Felippe Xavier, "Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales", en Revista *Estudios Penales y Criminológicos*., 44(ext), 2023.

JORQUI AZOFRA, M., NICOLÁS JIMÉNEZ, P., "¿Estafa en el ofrecimiento de servicios tecnológicamente innovadores en el área biomédica?: especial consideración del ofrecimiento de análisis genéticos", en ROMEO CASABONA, C., (ed. lit.), FLORES MENDOZA, F., (ed. lit.), *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica,* 2012, pp. 221 y ss.

FRANCISCO, *Inteligencia artificial y paz*, Vaticano, 8 de diciembre de 2023.

LEGIND LARSEN, H., y otros, *Flexible Querry Answering Systen:* 15th International Conference, FQAS 2023, Mallorca, Spain, September 5–7, 2023.

NAVA GARCÉS, A.E., "La regulación de la Inteligencia Artificial y el Derecho Penal", en ARELLANO TOLEDO, V. (Dir.) *Derecho, Ética e Inteligencia Artificial*, Valencia 2023, pp. 429 y ss.

NICOLÁS JIMÉNEZ, P., «Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos», en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, núm. extra 1, 2019 (ejemplar dedicado a: Uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas), pp. 129-167.

MARTÍNEZ GARCÍA, DALGO FLORES, HERRERA LÓPEZ, JIMÉNEZ, VELASCO ACURIO, "Avances de la inteligencia artificial en salud", en Revista *Dominio de las Ciencias*, Vol. 5, núm. 2, julio 2019, pp.603-613.

MARTÍNEZ SAPORTA, E., "Telemedicina y responsabilidad patrimonial de la Administración sanitaria", en *DS* Vol. 16, Número 1, Enero-Junio 2008, pp. 110 y ss.

MICHELETTI, D., "Algoritmi nomofilattici a confronto. Ufficio del massimario *vs* inteligenza artificiale", en *Rivista Studi Senesi*, III Serie LXIX (2023), fasc. 1, pp. 175-188.

MONTILLA MARTOS, J. A., "Inteligencia Artificial y derechos de participación política", en la Revista *De Lege Ferenda*, nº1, que puede encontrarse en el siguiente enlace: https://revistaseug.ugr.es/index.php/delegeferenda/index. Publicado 6 sep 2023.

MORALES, S.," Biosensores o cómo el médico podrá detectar el tumor en la primera visita" en *El Mundo*, Castellón al día, viernes 13 de octubre de 2023.

MORO-VISCONTI, R. "Le società MedTech e BioTech: piattaforme digitali, inteligenza artificiale e valutazione económica", en *Rivista Diritto di internet*, 2023, Anno V, n.1, pp. 187-195.

MUÑOZ CONDE/ GARCÍA ARÁN, *Derecho penal. Parte general,* 11ª ed., Valencia 2022.

NAVARRO CARDOSO, F., MONTESDEOCA RODRÍGEZ, D., "La cibercriminalidad sexual juvenil como nueva forma de delincuencia", en *Revista penal México*, nº. 19, 2021, pp. 37 y ss.

PAGALLO, U., QUATTROCOLO, S.: "The Impact of AI on Criminal Law and its Twofold Procedures", en BARFIELD, W., PAGALLO, U. (eds.), *Research Handbook on the law of artificial intelligence*, Cheltenham, 2018.

POUYDEBAT, E., *Inteligencia animal: cabeza de chorlitos y memoria de elefantes*, 2018.

RAMACCI, F., *Corso di diritto penale, Parte generale*, a cargo de GUERRINI, R., Torino, 8ª ed., 2023.

ROMEO CASABONA, C.M. (coord.), *Aspectos ético-jurídicos de las patentes biotecnológicas: la dimensión patrimonial de la materia viva*, 2014.

ROMEO CASABONA, C.M., "La atribución de responsabilidad penal por los hechos cometidos por sistemas autónomos inteligentes, robótica y tecnologías conexas", en *Revista de Direito da ULP*, vol. 16 nº. 1 E N. 2 (2022). También publicado en VVAA, *Estudios político criminales, jurídico penales y criminológicos: libro homenaje al Prof. José Luis Díaz Ripollés*, 2023, pp. 721 y ss.

ROMEO CASABONA/ RUEDA MARTÍN, *Derecho penal, ciberseguridad, ciberdelitos e Inteligencia Artificial. Volumen I Ciberseguridad y ciberdelitos*, Granada 2023.

ROZENWURCEL, P., *Seguridad y prevención de la criminalidad: el mapeo de los delitos y de la percepción de seguridad (aplicado a la Ciudad Autónoma de Buenos Aires)*, Universidad de Granada, 2023, disponible en URI: https://hdl.handle.net/10481/85092.

SEGURA SERRANO/ GORDO GARCÍA, *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio*, Granada, 2013.

TIEDEMANN, K., "Constitución y Derecho penal", en *Revista española de derecho constitucional,* año nº 11, nº 33, 1991, pp. 145-174.

TRAVERSI, D., "Genomica in Sanità Pubblica Evidenze scientifiche e prospettive di integrazione nella pratica della prevenzione", en *Journal of Preventive Medicine and Hygiene,* 2023 Mar; 63(3 Suppl 2): E1–E29. Publicado online el 13 enero 2023.

URZÚA INFANTE, C., "Inteligencia Artificial y los problemas éticos", en Arellano Toledo, V. (Dir.) *Derecho, Ética e Inteligencia Artificial*, Valencia 2023.

VERVAELE, J.A.E., "Verso una rivalutazione europea dell´enforcement nel diritto punitivo?, en Revista *Diritto penale XXI secolo*, anno XXII, 1/23, p. 1 y ss.

VERVAELE, J.A.E., "Ver une réevaluation européenne du droit répressif?, *Revue de science criminelle et de droit pénal comparé*, jul-sep 2023, pp. 509 y ss.

INTELIGENCIA ARTIFICIAL Y BIG DATA: LOS RETOS DEL SECTOR PÚBLICO EN LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES

Cristina Más Zamora

Accesit al Premio San Raimundo de Peñafort

Resumen: *El presente trabajo tiene como objetivo analizar la situación actual acerca del uso de los datos de los ciudadanos mediante sistemas de inteligencia artificial por parte de los poderes públicos y los posibles riesgos de desprotección de sus derechos fundamentales.*

En primer lugar, se realiza una aproximación al concepto de inteligencia artificial y se examina la regulación sobre la inteligencia artificial en Europa, así como los desafíos que plantea desde una perspectiva jurídica. Poniendo de manifiesto la necesidad de una mayor intervención regulatoria. Se alerta de los riesgos del tratamiento de los macrodatos de los ciudadanos mediante sistemas de inteligencia artificial en el sector público. Enfatizándose la importancia del principio de transparencia ante la problemática de la opacidad de los algoritmos. Asimismo, se abordan los peligros de la colisión entre los derechos de propiedad intelectual de los algoritmos de la inteligencia artificial frente al principio de transparencia.

Por último, se identifican los principales riesgos generados por los sistemas algorítmicos de la IA en el sector público, con respecto a la protección de los derechos fundamentales de los ciudadanos. En particular, el derecho a la protección de datos de carácter personal, el derecho a la no discriminación y el derecho a la tutela judicial efectiva.

Palabras clave: *Inteligencia artificial, algoritmos, derechos fundamentales, macrodatos, decisiones automatizadas, protección de datos de carácter personal, sesgos discriminatorios*

Abstract: *This paper aims to analyze the current situation regarding the use of citizens' data through artificial intelligence systems by public authorities and the potential risks of undermining*

their fundamental rights.

Firstly, an overview of the concept of artificial intelligence is provided, and the regulation of artificial intelligence in Europe is examined, as well as the challenges it presents from a legal perspective. The need for greater regulatory intervention is highlighted. The risks of processing citizens' big data through artificial intelligence (hereinafter AI) systems in the public sector are discussed, with an emphasis on the importance of the principle of transparency in light of the opacity of algorithms. Furthermore, the dangers of the conflict between intellectual property rights of AI algorithms and the principle of transparency are addressed.

Finally, the main risks generated by AI algorithmic systems in the public sector with respect to the protection of citizens' fundamental rights are identified, particularly the right to personal data protection, the right to non-discrimination, and the right to effective judicial protection.

Key words: *Artificial inteligence, algorithms, fundamental rights, automated decisions-making, big data, protection of personal data, discriminatory biases.*

SUMARIO:

SUMMARY:

I. UNA APROXIMACIÓN AL CONCEPTO DE INTELIGENCIA ARTIFICIAL.

Para muchos, el estudio científico publicado por Alan Turing en 1950 (Test de Turing), en el que se evaluaba la capacidad de una máquina para exihibir un comportamiento inteligente similar al humano[85], constituye el primer acercamiento a la ciencia de la inteligencia artificial (en lo sucesivo, IA). Pero no fue hasta agosto de 1955 cuando se aludió por primera vez al término de IA, por el científico John Mccarthy.[86]

Desde entonces, a medida que ha ido avanzando el desarrollo científico y los usos de la IA, su definición ha tenido que ir actualizándose para adaptarse a esos progresos técnicos. Es por ello que existe una gran dificultad de encontrar una concepción de IA flexible y universal.

En la actualidad, un concepto generalmente aceptado es el propuesto en 2018 por el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial[87]: "*El término inteligencia artificial se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía- , con el fin de alcanzar los objetivos específicos.*"[88]

Posteriormente, ese mismo grupo de expertos, perfeccionó su definición de IA, centrándose en las capacidades de la misma:

"Los sistemas de inteligencia artificial (IA) son sistemas de software (y posiblemente también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesa-

---

85 MATHISON TURING, A "Computing Machinery and Intelligence", Mind, 49, 1950, pp 433-460.

86 MCCARTHY, J., MINSKY, M., ROCHESTER, N., SHANNON, C. "A proposal for the Dartmouth Summer Research Project on Artificial Intelligence" August 31, 1995: AI Magazine Volume 27, Number 4, 2006.

87 Grupo de 52 expertos creado por la Comisión Europea.

88 Comunicación de la Comisión Europea sobre la IA "Inteligencia artificial para Europa" de 25 de abril de 2018 (COM (2018) 237) final).

miento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido."[89]

Tras esta aproximación al concepto general de IA, para poder comprender mejor su funcionamiento debemos entender los elementos que integran la misma, sus diferentes técnicas y enfoques. Así pues, la IA se basa principalmente en el uso de datos y de algoritmos. Debiendo entender por algoritmo, la secuencia finita de reglas formales (operaciones lógicas e instrucciones) que permiten obtener un determinado resultado de la entrada inicial de información que introducimos en dicho algoritmo.[90] De esta manera, los algoritmos permiten transformar automáticamente datos en resultados apropiados para lograr un determinado objetivo. (Commission Nationale de l'Informatique et des Libertés, 2017, 15); (Edwards & Veale, 2017, 24); (Yeung, 2017, 2).

Con respecto a la correlación de la IA con los datos, debemos hacer especial mención al *big data* (macrodatos). El concepto de macrodato (según la definición dada por el Parlamento Europeo)[91] se refiere a la recopilación, análisis y acumulación constante de grandes cantidades de datos (incluidos datos personales), procedentes de diferentes fuentes, y objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones (analítica de macrodatos).

Así, el gran reto del *big data* es la captación, gestión y tratamiento para agregar valor a grandes volúmenes de datos poco utilizados o inaccesibles has-

---

89 Informe, de 8 de abril de 2019, del Grupo de expertos de alto nivel sobre IA titulado «Una definición de la inteligencia artificial: principales capacidades y disciplinas científicas» Página 6. Con posterioridad, estas dos definiciones de IA propuestas por el grupo de expertos, fueron recogidas en el Libro Blanco. Sobre la Inteligencia Artificial – Un enfoque europeo para la excelencia y la confianza, COM(2020) 65 final, Bruselas, 19.2.2020, https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1.

90 European Commission for the efficiency of justice (CEPEJ). *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment.* diciembre 2018. Página 70.

91 Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)), Considerando A.

ta la fecha, todo ello para aportar y descubrir un conocimiento hasta ahora oculto. [92]

Una vez sentado lo anterior, podemos entender como el *big data* y la IA funcionan como tecnologías interdependientes, que se necesitan la una de la otra para a lcanzar su máximo potencial. Así pues, para ser eficiente, la IA precisa disponer de una gran cantidad de datos, con la finalidad de analizarlos y aprender a partir de los mismos. Y en este sentido, es donde se beneficia del *big data*, que le proporciona una amplia muestra de información para alimentar sus sistemas.

En este punto, debemos aclarar que la funcionalidad de la IA no se limita a este análisis de datos para su aprendizaje, siendo éste, en realidad, sólo un subcampo de la IA: el *machine learning*. Así pues, por aprendizaje automático o *machine learning* nos referimos *"al estudio y técnicas que tienen como objetivo el de aprender de un conjunto de datos existentes a través de la extracción de patrones y correlaciones de esos datos. En este proceso de aprendizaje se utilizan algoritmos capaces de procesar grandes cantidades de datos y ofrecer resultados sobre dichos datos, otorgando a los sistemas donde se implantan la capacidad de aprender sin ser programados explícitamente".*[93]

Por último, dentro del *machine learning* (aprendizaje automático) nos encontramos a su vez, otro subcampo denominado *deep learning* (aprendizaje profundo), que usa redes neuronales similares a las conexiones neuronales biológicas del cerebro humano, a partir de ingentes cantidades de datos.

Los algoritmos extraen patrones a partir del análisis de datos y van perfeccionándose sin que el usuario sea capaz de descubrir de manera sencilla porqué o cómo el algoritmo ha adoptado una decisión o ha producido un determinado resultado. Por ello, es ininteligible en la práctica para la mayoría de usuarios, como si de una caja negra (*black box*) se tratase. Aspecto que, como

---

92 COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", **,** *Revista Dilemata nº 24,* 2017, p. 131-150.

93 PALMA ORTIGOSA, A. "El ciclo de vida de vida de los sistemas de inteligencia artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas de algoritmos." En Cotino Hueso, L., *Derechos y garantías ante la Inteligencia Artificial y las decisiones automatizadas,* (2022), Aranzadi, 2024, 33-78

veremos posteriormente, pueda generar numerosos problemas desde el punto de vista jurídico. [94]

El uso de las herramientas basadas en IA ha crecido exponencialmente en los últimos años, convirtiéndose en uno de los elementos clave en el marco actual de la llamada cuarta revolución industrial.[95]

Este desarrollo de los sistemas de la IA ha sido posible gracias a la disponibilidad masiva de datos a los que tienen acceso actualmente las organizaciones (tanto públicas como privadas). Que viene originada por múltiples factores, entre los que destacan la datificación[96] de la sociedad, la interconectividad global, el auge de las tecnologías que facilitan la recogida de datos y, especialmente, el aumento de los recursos que favorecen el almacenamiento estos datos. [97]

Esta disponibilidad masiva de datos es aprovechada a través de herramientas de *big data*, ya que son capaces de procesar de forma rápida y eficiente tal cantidad de información.

II. RETOS EN LA REGULACIÓN EN MATERIA DE INTELIGENCIA ARTIFICIAL.

En los últimos tiempos, a consecuencia de la rápida evolución de las tecnologías de la IA y sus potenciales riesgos, se ha puesto en evidencia la necesidad de crear un marco normativo que garantice unas mejores condiciones de desarrollo y sobre todo, que proporcione a los ciudadanos una completa protección de sus derechos fundamentales.

---

94 CERILLO MARTÍNEZ, A. "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", 50, *Revista General de Derecho Administrativo* (Iustel), 2019.

95 Concepto acuñado por el economista Klaus Schwab, en el Foro Económico Mundial de 2016.

96 Kenneth NEIL CUKIER y Viktor MAYER-SCHÖENBERGER. «The Rise of Big data. How It's Changing the Way We Think About the World». Foreign Affairs Vol. 92, n.º 3 (2013).

97 GIL GONZÁLEZ, E., Ed. BOE, 2016, p. 18. https://www.aepd.es/sites/default/files/2019-10/big-data.pdf (recuperado noviembre 2024).

Con anterioridad a la creación del Reglamento de IA, las iniciativas europeas surgidas respecto a la regulación de la IA han tenido una finalidad esencialmente prospectiva con la que se pretende identificar la magnitud y características de los cambios que pueden producirse como consecuencia del desarrollo de la IA, así como las directrices de las medidas que tenían que adoptarse para garantizar una incorporación segura de estas nuevas tecnologías.[98]

Estas iniciativas se han materializado, mayoritariamente, en la constitución de grupos de trabajo compuestos por expertos de distintas disciplinas que elaboran informes en los que se contienen recomendaciones para el desarrollo de las políticas públicas en este ámbito.[99] Asimismo, se han emitido una serie de textos (*softlaw*), entre los que destacan el Libro Blanco sobre la inteligencia artificial[100] y diversas Resoluciones del Parlamento Europeo,[101] que pese a carecer de valor normativo, permiteron sentar las bases para proyectar el futuro marco legislativo para la IA en Europa.

2.1. Hacia un marco normativo común.

En este contexto, se crea finalmente el primer marco regulador de la UE para la IA: Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE)

---

98 VIDA FERNÁNDEZ, J. "Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea" *Sociedad digital y derecho línea de colaboración entre el BOE, el Ministerio de Economía y Empresa, y su entidad RED.ES*, dirección de Tomás de la Quadra-Salcedo y José Luis Piñar (BOE 2018). P.211, https://www.boe.es/biblioteca_juridica/publicacion.php?id=PUB-NT-2018-97 (recuperado noviembre 2024).

99 Entre los cuales destacan los dos comités *ad hoc* sobre IA, creados por el Comité de Ministros del Consejo de Europa: el CAHAI (cuyo mandato duró desde el año 2019 al 2021), y el CAI (Committee on Artificial Intelligence). Y en España, la Estrategia Nacional de Inteligencia Artificial (ENIA), creada en diciembre de 2020.

100 Bruselas, 19.2.2020 COM(2020) 65 final

101 Debiendo resaltar: Resoluciones de 20 de octubre de 2020, sobre derechos de Propiedad Intelectual para el desarrollo de las tecnologías relativas a la Inteligencia Artificial (2020/2015 (INI)) y de 3 de mayo de 2022, sobre la Inteligencia Artificial en la era digital (2020/2266 (INI)).

2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828. (Reglamento de Inteligencia Artificial).[102]

El cual nace con la finalidad de *"mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial (en lo sucesivo, «sistemas de IA») en la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales".* [103]

Este Reglamento de Inteligencia Artificial (en adelante RIA), se basa en el análisis y clasificación de los sistemas de IA según el riesgo que suponga para los usuarios. De manera que se intensifican las obligaciones y requisitos técnicos de los sistemas o modelos de IA cuanto mayor sea este nivel de riesgo. Concretamente, establece los siguientes niveles de riesgo: riesgo inaceptable, alto riesgo, riesgo limitado y riesgo bajo o mínimo.

En el primer nivel, figuran los sistemas de IA que presentan un **riesgo inaceptable** para los valores de la Unión Europea, entre los que se encuentran la vulneración de derechos fundamentales, tratándose por tanto de prácticas prohibidas por el RIA (Capítulo II RIA).

Si bien el artículo 5 RIA contiene una lista de prácticas que considera prohibidas, no podemos considerar ésta como una enumeración taxativa. Puesto que tendrán tal consideración en función del riesgo que los sistemas de IA puedan representar para los derechos fundamentales, la salud y la seguridad (en base a los resultados que arrojen las evaluaciones del riesgo). Estableciéndose una determinación dinámica, con remisión a otras normativas, y verificaciones recurrentes, en tanto que el art. 112 del RIA prevé que esta lista de prácticas prohibidas recogidas en el art. 5 se revise y amplíe anualmente.

---

102 Que fue publicado en el Diario Oficial de la Unión Europea el 12 de julio de 2024, y entró en vigor a los veinte días de su publicación. Siendo de aplicación, con carácter general, a los 24 meses de su entrada en vigor, aunque para determinados apartados su aplicación seguirá un calendario escalonado.

103 Objetivo recogido en el considerando 1 RIA.

En el segundo nivel, se encuentran aquellos sistemas de IA que acarrean un **alto riesgo** para la salud y la seguridad o los derechos fundamentales de las personas físicas. (Capitulo III RIA). Éstos se encuentran permitidos en el mercado europeo siempre que cumplan determinados requisitos obligatorios, recogidos en los arts. 8 a 15 RIA, tales como la realización de un sistema de gestión de riesgos (que consiste en un proceso repetido y continuo que se desarrolla durante todo el ciclo de vida del sistema de IA de alto riesgo, con revisiones y actualizaciones sistemáticas y periódicas), intensificación de los requisitos de documentación técnica y registro, así como de supervisión humana. Además, se requiere de una evaluación de la conformidad pertinente, antes de su introducción en el mercado o puesta en servicio, así como obligaciones en materia de transparencia.

Existen también determinados sistemas de IA, cuyo **riesgo es limitado** y está asociado con la falta de transparencia en los usos de la IA. A los proveedores y responsables de estos sistemas se les exige que lleven a cabo una serie de requisitos de información y transparencia, que se recogen en el art. 50 RIA.

Por último, para los sistemas **riesgo bajo o mínimo**, el Reglamento únicamente establece su sometimiento a códigos de conducta (art. 95 RIA), para la aplicación voluntaria de determinados requisitos.

Este enfoque general del RIA, basado en niveles de riesgo, resulta adecuado y consecuente con el principio de precaución, y en consonancia con los estándares internacionales previstos para el uso de la IA.

Para ejercer el control sobre los riesgos que puede plantear el uso de la IA, el RIA, en su artículo 79.2, otorga a las autoridades de vigilancia del mercado de los Estados miembros la facultad de actuar cuando tenga motivos suficientes para considerar que un sistema de IA presenta un riesgo. En ese caso, efectuará una evaluación del sistema de IA de que se trate para verificar el cumplimiento de todos los requisitos y obligaciones establecidos en el Reglamento. Además, si detectara riesgos para los derechos fundamentales, la autoridad de vigilancia del mercado informará también a las autoridades u organismos públicos nacionales previstos en el art. 77, que actúan para los supuestos específicos de vulneración de derechos fundamentales.

Una vez efectuada la evaluación, si la misma constata que el sistema de IA no cumple los requisitos y obligaciones establecidos en el Reglamento, exigirá sin demora indebida al operador pertinente que adopte todas las medidas

correctoras oportunas para adaptar el sistema de IA a los citados requisitos y obligaciones, retirarlo del mercado o recuperarlo, dentro del plazo que estime (y que, en cualquier caso, será como máximo de quince días hábiles), o en el plazo que prevean los actos legislativos de armonización de la Unión pertinentes, según corresponda.

Con respecto al ámbito de aplicación del RIA, el mismo engloba a: 1. Personas afectadas que estén ubicadas en la Unión. 2. Fabricantes que utilicen IA junto con su producto, nombre o marca. 3. Representantes autorizados de los proveedores que no estén establecidos en la Unión 4. Responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión. 5. Proveedores (con independencia de su ubicación) que introduzcan en el mercado o pongan en servicio sistemas de IA o que introduzcan en el mercado modelos de IA de uso general en la Unión. 6. Importadores y distribuidores de sistemas de IA. 7. Proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión.[104]

A pesar de lo anterior, el RIA parece centrarse principalmente en regular cuestiones que afectan a los desarrolladores y responsables del despliegue de la IA (incluyendo como tal tanto a entes públicos como privados, y a personas jurídicas y personas físicas - salvo cuando su uso se enmarque en una actividad personal de carácter no profesional-), sin abordar de manera tan exhaustiva las cuestiones relativas a las personas afectadas por los casos de uso de la IA. Pues, si bien es cierto que se establecen determinadas protecciones para el usuario de la IA, las mismas no quedan definidas con precisión. Tal es el caso del artículo 14 RIA, en el que se regula un elemento clave en la protección de los derechos fundamentales de los ciudadanos en los usos de los sistemas de IA, como es la preceptiva vigilancia humana efectiva durante el periodo que estén en uso los sistemas de IA de alto riesgo. Pero no define que se entiende por "efectiva" a estos efectos (formación o cualificación requerida), ni desarrolla la manera en que debe realizarse la supervisión humana. Únicamente recoge este extremo de manera más específica en los casos de sistemas de identificación biométrica remota, en el que sí se establece que el responsable del despliegue no actúe ni tome ninguna decisión basándose en la identificación generada por el sistema,

104 De acuerdo al ámbito de aplicación previsto en el art. 2 RIA.

salvo si al menos *"dos personas físicas con la competencia, formación y autoridad necesarias"* han verificado y confirmado por separado dicha identificación.

Por otro lado, el RIA también regula los organismos de control y supervisión de los sistemas de IA,[105] estableciendo la creación del Consejo Europeo de IA, que prestará asesoramiento y asistencia a la Comisión y a los Estados miembros para facilitar la aplicación coherente y eficaz del RIA. Asimismo, prevé la creación de la Oficina de IA, mediante la cual la Comisión de IA desarrollará los conocimientos y capacidades de la Unión en el ámbito de la IA. Así como un Foro Consultivo para proporcionar conocimientos técnicos y asesorar al Comité y a la Comisión y un grupo de expertos independientes.

De nuevo, tampoco se regula de manera exhaustiva, desde la perspectiva la persona afectada por los usos de la IA, un mecanismo específico para hacer valer sus derechos ante los citados organismos, ni ante los órganos judiciales. Tampoco se establecen aspectos tan importantes en la práctica como es la imputación individual de las responsabilidades que se deriven de la utilización de la IA o el modo de impugnación de resultados del algoritmo.

De manera que, a pesar de que la Sección 4 del Capitulo IX, se enuncia como *"vías de recurso"*, la regulación en este punto resulta sucinta e insuficiente. Pues reconoce, únicamente, en un sentido amplio, el derecho a presentar una reclamación ante una autoridad de vigilancia del mercado pertinente, sin perjuicio de otras vías administrativas o judiciales de recurso.

Por último, el RIA prevé un régimen sancionador para los incumplimientos de lo establecido en el Reglamento. En primer lugar, fija un régimen sancionador general, por incumplimiento de la normativa por parte de los operadores de los sistemas de IA, cuya concreción atribuye a los Estados miembros. Para estos casos, las multas administrativas por no respetar las prácticas de IA prohibidas (entre las que se encuentran las relativas a la vulneración de derechos fundamentales) podrán ascender a un máximo de hasta 35.000.000 euros (art. 99 RIA).

En segundo lugar, encontramos el régimen sancionador previsto para las instituciones y los órganos y organismos de la UE, cuya competencia se atribuye al Supervisor Europeo de Protección de Datos. En este caso, las multas máximas previstas para los supuestos de incumplimientos en materia de vul-

105 que denomina de "Gobernanza", y se recogen en el Capítulo VII.

neración de derechos fundamentales (por no respetar las prácticas prohibidas por el RIA), ascienden a 1.500.000 euros (art.100 RIA).

Por último, se regula, en su artículo 101, el régimen sancionador para proveedores de modelos de IA de uso general o de propósito general. Teniendo atribuidas las competencias la Comisión Europea, pudiendo imponer multas que no superen el 3 % de su volumen de negocios mundial total anual correspondiente al ejercicio financiero anterior o de 15 000 000 EUR, si esta cifra es superior.

Cabe mencionar en este punto que, con posterioridad a la publicación del RIA, se firma, en fecha 5 de septiembre de 2024 durante la Conferencia de Ministros de Justicia en Vilna, el Convenio Marco del Consejo de Europa sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho (en adelante, el Convenio).[106]

Que se encarga de afianzar los principios de deben regir los usos de la IA y realiza un enfoque más centrado en el ciudadano que pueda verse afectado por dichos usos.

Para su aplicación, se requiere la ratificación posterior de cinco Estados (de los cuales al menos tres deben ser miembros del Consejo de Europa).[107]

2.2. Vicisitudes en la regulación de Inteligencia Artificial y nuevos instrumentos normativos.

La rápida e incierta evolución de la IA exige la dotación de un marco normativo lo suficientemente flexible para adaptarse de manera ágil a estos constantes cambios.[108] Pero que, al mismo tiempo, permita mantener un nivel de

106 https://rm.coe.int/1680afae3c, recuperado noviembre 2024.

107 y entraría así en vigor el primer día del mes siguiente a la expiración de un período de tres meses desde la fecha dicha firma Siendo un tratado internacional, tras su ratificación y publicación, se incorporaría al ordenamiento interno, conforme al art. 96.1 de la Constitución Española.

108 Debemos tener en cuenta en este punto, que las previsiones de los expertos en IA en cuanto su impacto en el futuro sufre constantes variaciones, lo que sugiere que podría ser difícil, incluso para ellos, predecir los resultados de un amplio despliegue de nuevas tecnologías de IA. (punto 85 Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)).

precisión adecuado para ofrecer la seguridad jurídica necesaria. Alcanzar ese complejo equilibrio es el principal objetivo de la regulación en materia de IA.

En este contexto de incertidumbre, el Libro Blanco de Inteligencia Artificial apunta que el marco regulador de la IA debe dejar margen para abordar su desarrollo en el futuro. Considerando que, en aplicación del principio de precaución, toda modificación debe limitarse a aquellos problemas ya detectados con claridad, para los que existan soluciones factibles.[109]

Pero no podemos negar las evidentes limitaciones que tiene el legislador para adaptarse a los constantes cambios de la IA, por lo que deberá recurrir a nuevos instrumentos regulatorios que le permiten enfrentarse adecuadamente a su constante desarrollo tecnológico:

Una de las principales medidas que recoge el RIA en este sentido es la creación de espacios controlados para desarrollar, experimentar y probar sistemas de inteligencia artificial bajo la supervisión de sus autoridades competentes. Son los llamados *sandbox* regulatorios para la IA, entendiendo como tal "*un entorno controlado que fomente la innovación y facilite el desarrollo, el entrenamiento, la prueba y la validación de sistemas innovadores de IA durante un período limitado antes de su introducción en el mercado o su puesta en servicio.*"[110] Estableciéndose en el propio RIA, la obligación de que cada Estado miembro disponga al menos un espacio controlado de pruebas para la IA a nivel nacional, así como otra serie de requerimientos para los mismos, entre los que destaca el deber de presentar informes anuales sobre el progreso y los resultados de los *sandboxes* a la Oficina de la IA y al Comité.

Con esta finalidad (y anticipándose a la imposición recogida posteriormente en el RIA), se aprobó en España el Real Decreto 817/2023 de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de IA.

Igualmente, puede resultar útil en la regulación de la IA la utilización de cláusulas derogatorias (*sunset clauses*) que permitan ir ajustando las regulacio-

---

109 LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza PAG 12, Bruselas, 19.2.2020, COM (2020) 65 final.

110 Artículo 57.5 RIA.

nes a la evolución tecnológica o técnicas de regulación anticipada (*anticipatory rulemaking techniques*). [111]

También pueden utilizarse técnicas de evaluación *ex ante* y *ex post* que persigan obtener y analizar datos sobre cuándo se debe regular un nuevo desarrollo tecnológico o sobre el impacto de las normas ya vigentes. Siendo que en estas evaluaciones *ex ante* debe identificarse con precisión lo que se pretende conseguir y las medidas más apropiadas para ello, por medio de un estudio riguroso. Existiendo a su vez la obligación *ex post* de revisar si efectivamente se han conseguido los objetivos iniciales y si las medidas adoptadas resultan idóneas.

Cabe poner en relieve que las evaluaciones de impacto *ex ante* resultan de carácter preceptivo (por imposición del art. 27 RIA) únicamente cuando se trate de organismos de Derecho público (o entidades privadas que prestan servicios públicos), que vayan a desplegar determinados sistemas de IA calificados de alto riesgo[112]. Debiendo evaluarse el impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales.

Además, en estos casos, las referidas evaluaciones de impacto *ex ante* deben ir acompañadas de un control del cumplimiento *ex post* mediante evaluaciones de conformidad posteriores, así como de su supervisión. Dichos procedimientos se desarrollarán por medio de la cooperación entre las autoridades notificantes de todos los Estados miembros, conforme al procedimiento previsto en la Sección 4 del Capítulo III RIA.

Por último, puede recurrirse a instrumentos de *soft law* ante manifestaciones emergentes de la IA que más adelante se consoliden a través de otros instrumentos de regulación de *hard law* a medida que se vayan desarrollando las tecnologías, como ha venido ocurriendo en Europa con anterioridad a la entrada en vigor del RIA.

---

111 CERILLO MARTÍNEZ, A. "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", *Revista General de Derecho Administrativo* (Iustel), 50, 2019.

112 Sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, conforme a lo dispuesto en el art. 27.1 RIA.

Para velar por el cumplimiento de la normativa en torno al adecuado uso y desarrollo de los sistemas de IA, se ha creado en España la Agencia Española de Supervisión de Inteligencia Artificial (AESIA). Que llevará a cabo tareas de supervisión, asesoramiento, concienciación y formación a entidades públicas y privadas para la implementación de esta normativa en materia de IA. Así como la inspección, comprobación y sanción en este ámbito.[113]

Su creación se adelanta así a la obligación impuesta por la RIA (art. 28) que establece que "*cada Estado miembro nombrará o constituirá al menos una autoridad notificante que será responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión. Dichos procedimientos se desarrollarán por medio de la cooperación entre las autoridades notificantes de todos los Estados miembros.*"

III. IMPLANTACIÓN DE LA INTELIGENCIA ARTIFICIAL POR LOS PODERES PÚBLICOS. OPACIDAD DEL ALGORITMO Y GARANTÍAS FRENTE A LOS DERECHOS FUNDAMENTALES.

3.1. El tratamiento de los macrodatos mediante inteligencia artificial por los poderes públicos.

La reciente digitalización de los organismos públicos[114] , y su facilidad para acceder masivamente a los datos de los ciudadanos, constituyen el escenario idóneo para la introducción y desarrollo de los sistemas de la IA, pues la disponibilidad de esta gran cantidad de datos facilita las predicciones de los

113 Siendo estos los principales fines de la AESIA, recogidos en el art. 4 del Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial.

114 Impulsada con la entrada en vigor en la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015 de Régimen Jurídico del Sector Público (en la que se introdujo el concepto de actuación administrativa automatizada, esto es, actos realizados íntegramente a través de medios electrónicos una Administración Pública y en la que no haya intervenido de forma directa un empleado público).Y desarrollada con el RD 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

algoritmos de la IA y la automatización de las decisiones individualizadas de los órganos estatales con intervención de la IA.

Sin embargo, esta abrupta implantación de la tecnología de la IA en el tratamiento masivo de los datos, desprovista de las herramientas necesarias y de un marco regulador sólido en la materia, puede generar colisiones indeseadas en los derechos fundamentales de los ciudadanos si se usa indebidamente por parte de los poderes públicos. Y en la medida que se tratan conjuntamente ingentes cantidades de datos de la población, existe un elevado riesgo, no sólo de afectar al ciudadano individualmente, si no a varios individuos o colectivos de manera simultanea.

Tal como advierte el Tribunal de Justicia de la Unión Europea (en su sentencia de 8 de abril de 2014)[115]: "*el tratamiento masivo de datos incluso desvinculados de personas concretas, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan*" . Este riesgo indudablemente se ve intensificado con la aplicación de los sistemas o modelos de IA al tratamiento masivo de datos.

Por este motivo, algunos autores, como CONTINO HUESO (2017) [116] destacan la importancia de trabajar la protección de los derechos fundamentales frente a los usos derivados de la IA, desde la dimensión colectiva de los derechos: *"El daño individual producido por el Big Data y la IA puede ser imperceptible para el derecho fundamental desde la perspectiva del individuo titular del derecho, pero bien puede afectar masivamente a los derechos fundamentales de sectores o conjuntos de la sociedad de una manera relevante en esta dimensión colectiva."*

Por lo que, en caso de eventuales lesiones de estos derechos supraindividuales, los ciudadanos podrán acudir, para una mayor garantía, por la vía del

---

115 41 STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12. También, STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB y Secretary of State for the Home Department y otros, ap. 99.

116 COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Revista Dilemata nº 24,* 2017, pp. 131-150.

art. 80 RGPD a ejercer la tutela de sus derechos a través de entidades, organizaciones o asociaciones de representación colectiva.

En este punto, cabe poner en relieve lo dispuesto en el art. 85.1 RIA, que reconoce el derecho a presentar una reclamación ante una autoridad de vigilancia del mercado a aquellas personas (físicas o jurídicas) que "*tengan motivos para considerar que se ha infringido lo dispuesto en el presente Reglamento.*" Ello podría abrir la vía a la legitimación activa de colectivos en el ejercicio de derechos supraindividuales, pues como afirma CASTILLA BAREA (2024) en interpretación del referido artículo: "*el reclamante puede ser tanto un sujeto que se haya sentido directamente perjudicado por la infracción que denuncia, como alguien que actúe movido por cualquier otro interés legítimo como podría ser el caso, por ejemplo de una asociación de consumidores.*"[117]

Del mismo modo, en su caso, podría ser de aplicación la Directiva (UE) 2020/1828, de 25 de noviembre, que regula las acciones colectivas y su transposición en España.

En este punto, hay que tener en cuenta la especial doble vinculación de los poderes públicos con los derechos fundamentales. Pues su obligación no sólo se limita al deber de abstenerse de cualquier actuación que perjudique el contenido y ámbito de aplicación de los derechos fundamentales (vinculación negativa), impuesta por el art. 9.1 CE tanto a los poderes públicos como a los ciudadanos.

Si no que además, el art. 53.1 CE exige expresamente a los poderes públicos su vinculación positiva a los derechos fundamentales. Que se traduce en un deber general de realizar las funciones de acuerdo con la Constitución y un mandato de desplegar la eficacia de los derechos fundamentales en el sentido de establecer su realización plena.

De lo que se deduce que los poderes públicos se encuentran obligados a realizar acciones positivas específicas de cumplimiento, protección y dotación de eficacia a los derechos fundamentales. [118]

---

117 CASTILLA BAREA, M. "Vigilancia, postcomercialización, códigos de conducta y directrices" en Barrio Andrés. M, *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, 2024, p.178.

118 GAVARA DE CARA, J. C., "La vinculación positiva de los poderes públicos a los derechos fundamentales", *Teoría y realidad constitucional,* n.° 20, 2007, pp. 277-278.

De esta manera, la Administración tiene la obligación constitucional de tomar todas las medidas necesarias para proteger activamente los derechos fundamentales de los ciudadadanos frente a los usos de la IA por parte del Estado.

Deber que se impone, de manera expresa y específicamente en el ámbito de la IA, por la reciente Ley 15/2022, de 12 de julio (LA LEY 15917/2022), integral para la igualdad de trato y la no discriminación (BOE de 13 de julio), que requiere a las administraciones públicas la promoción del uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, promoviendo a su vez el sello de calidad de los algoritmos (en sus arts. 23.3 y 23.4).[119]

3.2. Los problemas de explicabilidad del algoritmo.

El principal reto en la protección de los derechos fundamentales de los ciudadanos por el uso de los sistemas de la IA por los poderes públicos, deriva de los problemas de explicabilidad de los algoritmos. Pues a medida que se ha ido desarrollando la tecnología de la IA, los procesos de aprendizaje automatizados de algoritmos basados en el procesamiento de grandes cantidades de datos, la capacidad de reunir datos procedentes de múltiples fuentes diferentes (y de elaborar representaciones complejas de un entorno dado), y la determinación de patrones, han convertido a los sistemas de IA en sistemas más complejos, autónomos y opacos, lo que puede hacer que los resultados sean menos explicables. [120]

Los resultados de los algoritmos más potentes de la IA, los de *deep learning,* en efecto, son difíciles de entender, ya que el proceso que desarrolla es opaco (lo que se conoce como *black box*). Sin embargo, hay muchos algoritmos de aprendizaje automático que son perfectamente inteligibles (cajas blancas) para saber cómo ha llegado a una determinada conclusión (por ejemplo, los llamados "árboles de decisión"). El algoritmo puede demostrar todas las variables que han influido en su decisión y con qué importancia.[121]

---

119 Siendo la primera regulación expresa del uso de la IA por la administración en nuestro país.

120 Resolución del Parlamento Europeo de 3 de mayo de 2022, sobre la Inteligencia Artificial en la era digital (2020/2266 (INI)), p. 14.

121 SALAZAR GARCÍA, I. "Retos actuales de la ética en la inteligencia artificial." En Contino Hueso, L., *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas, Aranzadi*. 2022, pp.79-101.

Es por ello que el deber de transparencia que se exige, con carácter general, a la Administración Pública (arts. 9.3, 24 CE, art. 41.2 Ley 40/2015, arts. 11 y 13 Real Decreto 203/2021), resulta un elemento clave cuando se empleen herramientas de IA, que conlleva una mayor necesidad de que el ciudadano tenga toda la información necesaria en su poder, para su conocimiento.

En este sentido, el Informe publicado por la Comisión Europea (*directrices éticas para una IA fiable)* [122] resalta la importancia explicabilidad y la transparecia del proceso, siendo preciso comunicar abiertamente las capacidades y la finalidad de los sistemas de IA y que las decisiones deben poder explicarse a las partes que se vean afectadas por ellas de manera directa o indirecta. Ya que sin esta información, no es posible impugnar adecuadamente una decisión. [123]

3.3. Obligaciones de transparencia respecto a los sistemas de IA.

Dada la importancia del principio de transparencia en los usos de la IA, el RIA contempla obligaciones relevantes en este sentido, especialmente para los sistemas de alto riesgo, imponiendo a los responsables de su despliegue el deber de transparencia y comunicación de información (art. 13 RIA).

De igual modo reconoce también (en su art. 50) requisitos de transparencia para los proveedores y responsables de determinados sistemas de IA, de riesgo limitado. Así, respecto a los sistemas destinados a interactuar directamente con personas físicas (tales como *chatbot*), se exige que estos sistemas se diseñen y desarrollen de forma que en todo momento las personas estén informadas de que están interactuando con un sistema de IA. Excepto en los casos que resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización.

Asimismo, para los proveedores de sistemas de IA que generen contenido sintético de audio, imagen, vídeo o texto, se establece la obligación de velar por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados de manera artificial.

---

122 Informe del Grupo de expertos de alto nivel sobre la IA de la Unión Europea *directrices éticas para una ia fiable* publicado por la Comisión Europea el 8 de abril de 2019.

123 Como así se recoge posteriormente en el Considerando 27 del RIA.

Respecto a los sistemas de reconocimiento de emociones y sistemas de categorización biométrica estarán también obligados a informar de su funcionamiento a las personas expuestas a él. Exceptuándose de este supuesto los sistemas de IA utilizados para la categorización biométrica y el reconocimiento de emociones que hayan sido autorizados por ley para detectar, prevenir e investigar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros y de conformidad con el Derecho de la Unión.

Por último, el sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación (los llamados d*eepfackes*) harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial. No operando esta obligación cuando la ley autorice su uso para detectar, prevenir, investigar o enjuiciar delitos.

3.4. El deber de transparencia y su colisión con los derechos de propiedad intelectual.

Para entender la importancia de la transparencia del algoritmo en la protección de derechos fundamentales del ciudadano, resulta ilustrativo el caso SyRI (*System Risk Indication).* En el que el Tribunal de la Haya, mediante sentencia de 5 de febrero del 2020 (C/ 09/550982/HA ZA 18-388), consideró que el sistema de algoritmos predictivos utilizado por los organismos públicos holandeses para detectar fraudes en la seguridad social, atentaba contra el derecho a la vida privada de los ciudadanos.

El sistema SyRI, es activado por el Ministerio de Asuntos Sociales y Empleo a petición de otros organismos públicos (municipales, las autoridades fiscales nacionales), y en base a los datos de los archivos en poder de estos organismos, trata de detectar posibles fraudes en las áreas mencionadas, para proceder a su sanción. De manera que se intercambian datos personales de los ciudadanos (entre los que se encontraban datos de trabajo, información sobre sanciones administrativas, datos educativos o datos del seguro de salud), sobre los cuales se elaboraban los perfiles de riesgo de los contribuyentes holandeses.

El tratamiento de estos datos constaba de dos fases: el tratamiento (fase 1) y el análisis (fase 2). En la primera fase, se reúnen los archivos y se pseudonimizan. Entre otras cosas, los nombres personales y de la compañía, los números de seguridad social y las direcciones, se reemplazan por un código (seudónimo).

Cuando ciertas personas se clasifican como de mayor riesgo, se descifran nuevamente utilizando el archivo de clave. Luego, son transferidos al Ministro para la segunda fase del análisis de riesgos.

El Tribunal en su fallo dictaminó que la legislación SyRI no cumplía con los requisitos del Artículo 8, párrafo 2 del CEDH (Derecho al respeto a la vida privada) para justificar el intercambio mutuo de datos personales. Pues consideró que, si bien es lícito acudir a herramientas de este tipo cuando concurra un interés legítimo que lo respalde, y se han adoptado las medidas pertinentes para que su injerencia sea lo menos perjudicial posible en la vida privada del ciudadano, en este caso entendió que la medida resultaba desproporcionada y no ofrecía las suficientes garantías.

Por ello, el Tribunal concluyó que la utilización del sistema SyRI carecía de base legal resaltando que, una de las principales las razones por las que se falló en este sentido, fue la falta de transparencia del algoritmo. Por entender que "*no se conocen los indicadores de riesgo y el modelo de riesgo ni los criterios objetivos que subyacen a la validez de los indicadores de riesgo y el modelo de riesgo*", y consecuentemente, concluye que *"no hay información suficiente para saber cómo operaba."*

En este sentido, hay que prestar atención a las muchas garantías que prestaba el sistema SyRi (como una correcta técnica de anonimización, el cumplimiento del deber de confidencialidad y la intervención de personas físicas para detectar falsos positivos en riesgo de fraude), a pesar de las cuales la sentencia consideró que resultaban exiguas, por no cumplir el requisito de transparencia.

También hay que resaltar que la sentencia reconoce expresamente la legítima finalidad del sistema SyRI pues entiende que la detección del fraude "*es un propósito suficientemente convincente para justificar una interferencia en su vida privada*".

Sin embargo, entiende desproporcionado el sistema SyRI, por la falta de transparencia debido a su falta de independencia y de auditorías, así como la falta de información a los usuarios de los datos que se tratan.

No podemos obviar que en este caso se trataba de un algoritmo empleado por el sector público, al que se le exige un grado de transparencia superior en sus acciones. Lo cual no es del todo extrapolable al supuesto de empresas privadas, para las cuales el deber de transparencia presenta una mayor limitación por los derechos a la propiedad intelectual o los secretos empresariales, que impide que se les obligue a publicar el código fuente o el funcionamiento de sus algoritmos.

En este punto, debemos recordar que en nuestro país el art. 14.1 j) de la Ley 19/2013 de Transparencia, acceso a la información pública y buen gobierno, sí que límita expresamente el acceso de información pública cuando suponga un perjuicio para la protección de la propiedad intelectual (recogiendo a su vez como excepción a este límite, la concurrencia con un interés público o privado, superior que justifique su acceso).

Por su parte, el RIA parece que trata de primar la protección de la propiedad intelectual del algoritmo en este sentido, por lo que se infiere de su parte expositiva y del tenor literal del artículo 78, que contempla que los organismos o personas a los que les resulte de aplicación el Reglamento respetarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades de modo que se protejan, en particular los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente.[124]

Pero a la espera de los primeros pronunciamientos judiciales interpretativos del Reglamento y de un desarrollo normativo mayor en esta materia, la constante colisión del principio de transparencia del algoritmo con los derechos de la propiedad intelectual pueden plantear controversias respecto a la protección de los derechos fundamentales del ciudadano, especialmente al derecho a la tutela judicial efectiva.

Para abordar esta situación, algunos autores plantean incluso que los algoritmos empleados por parte de las Administraciones públicas para la adopción efectiva de decisiones, han de ser considerados reglamentos por cumplir una función material estrictamente equivalente a la de las normas jurídicas, al reglar y predeterminar la actuación de los poderes públicos.

Así, afirma BOIX PALOP (2020) que "*si asumimos que el código fuente que integramos en la adopción de decisiones administrativas tiene materialmente valor normativo, dado que esos algoritmos y programas son empleados como elementos que ayudan a determinar o no concurrencia de ciertas circunstancias de hecho o que establecen la conveniencia o no de asociar ciertas consecuencias jurídicas a los hechos disponibles, es inevitable deducir de ello las consecuencias jurídicas asociadas*". Pues

124 A excepción de los casos mencionados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo (57).

entiende que, en coherencia con ese carácter normativo, seguiría las pautas previstas para la elaboración de reglamentos que se ajustan a la perfección a las necesidades de mayor control que requieren los algoritmos empleados para la Administración para la toma de decisiones. Garantizando así la publicidad de su código fuente, evaluaciones *ex ante* y *ex post,* reconocimiento de posibilidades de defensa y recurso frente a los algoritmos. [125] Postura que no deja de tener posicionamientos en contra de otros autores[126], pues si bien reconocen la necesidad de dotar a los algoritmos de ciertos beneficios que se derivarían de su consideración como reglamentos, no entienden que debieran tener tal condición.

125 BOIX PALOP, A., "Los Algoritmos Son Reglamentos: La Necesidad De Extender Las Garantías Propias De Las Normas Reglamentarias A Los Programas Empleados Por La Administración Para La Adopción De Decisiones." *Revista de Derecho Público: Teoría y Método Marcial Pons Ediciones Jurídicas y Sociales*. (Vol 1), 2020, pp. 223-270. DOI: 10.37417/RPD/vol_1_2020_33. (recuperado noviembre 2024).

126 Postura contraria al reconocimiento de algoritmo como reglamento: HUERGO LORA, A. (2020). Una aproximación a los algoritmos desde el Derecho Administrativo. En A. Huergo Lora (dir.) y G. M. Díaz González (coord.), *La regulación de los algoritmos*, Thomson-Reuters Aranzadi. P.64.

IV. EL DERECHO A LA PROTECCIÓN DE DATOS Y LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL.

4.1. Derecho a la protección de datos en los usos del *big data* mediante inteligencia artificial. Técnicas de anonimización y particularidades del consentimiento.

Entre los derechos fundamentales más afectados por la aplicación de las tecnologías derivadas de IA están los que garantizan la dimensión privada de las personas, especialmente el derecho a la protección de datos personales, recogido, en el art. 18.4 CE, y en el art. 8 Carta de Derechos Fundamentales de la Unión Europea.

En particular, el marco legal de referencia que desarrolla el derecho fundamental a la protección de datos personales lo encontramos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (el Reglamento general de protección de datos, en adelante, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

Dado que el uso de los sistemas de IA en el sector público se basa principalmente en el empleo de macrodatos de los ciudadanos, la cuestionable e insuficiente regulación en materia de IA que encontramos en el RIA en este campo, obliga a acudir a este marco normativo en materia de protección de datos para dar cobertura a las consecuencias jurídicas de los usos derivados de la IA.

Pero en el ámbito del uso de la IA por el sector público, la aplicación de este marco regulador del régimen de datos personales se vuelve muy complejo, debido a las particularidades del tratamiento masivo de datos mediante IA, que dificulta en qué términos pueden predicarse los elementos básicos que rigen el derecho protección de datos, esto es, el consentimiento informado pleno y real del usuario, los derechos ARCO (acceso, rectificación, cancelación u oposición), así como el derecho a no ser sometidos a evaluaciones automatizadas de la persona.

En primer lugar, es preciso delimitar los supuestos en los que los sistemas derivados de la IA implican un tratamiento de datos personales a los efectos

jurídicos que aquí nos ocupan. Puesto que, si la Administración procede a la correcta anonimización de los datos [127] de los ciudadanos, tras la cual no se trata datos de personas concretas identificadas o identificables, no sería de aplicación la regulación en materia de protección de datos personales.[128]

Ocurre que la anonimización del *big data* presenta especiales problemas técnicos y jurídicos. En este sentido, el propio Libro Blanco de la IA reconoce "*el riesgo potencial de que, incumpliendo las normas de la UE en materia de protección de datos u otras normas, las autoridades estatales y otros organismos recurran a la IA para la vigilancia masiva. Al analizar grandes cantidades de datos y detectar la conexión existente entre ellos, la IA también puede utilizarse para rastrear y desanonimizar datos relativos a personas, y generar así nuevos riesgos en torno a la protección de los datos personales con relación a conjuntos de datos que, en sí mismos, no contienen datos personales.*".[129]

Para abordar esta problemática, los poderes públicos deben proceder a la correcta anonimización de datos de los ciudadanos al tratar sus datos a través de herramientas de IA, mediante la observancia de las recomendaciones fijadas en el Dictamen 5/2014, de 10 de abril de 2014, sobre técnicas de anonimización, creado por el Grupo de trabajo sobre Protección de Datos[130] como así considera el Parlamento Europeo [131] y siendo conveniente la supervisión

---

127 Conforme al RGPD (art.4), se definen los datos personales como: toda información sobre una persona física identificada o identificable («el interesado»). se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

128 Los supuestos de anonimización de los datos, se encuentran expresamente excluidos de la aplicación de la legislación en materia de protección de carácter personal, conforme a lo establecido en la Directiva 95/46/CE (considerando 26).

129 LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza PAG 14, Bruselas, 19.2.2020, COM(2020) 65 final.

130 https://www.aepd.es/documento/wp216-es.pdf, recuperado en noviembre de 2024

131 En su Resolución, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)), p.155: Considera que este dictamen ofrece una visión de conjunto útil, que podría desarrollarse en mayor medida y pide al Comité Europeo de Protección de Datos que adopte directrices basadas en casos de uso específicos y situaciones pertinentes para

y concreción de estas recomendaciones por el Comité Europeo de Protección de Datos.

En segundo lugar, si bien el derecho a la protección de datos de carácter personal se construye sobre la base del consentimiento del individuo, en el ámbito de las tecnologías derivadas de la IA, el concepto del consentimiento se vuelve complejo y difuso, debido a que en muchos casos, la dificultad del funcionamiento del algoritmo hace que el individuo no comprenda el alcance de las consecuencias de su utilización y su incidencia en la protección de sus datos de carácter personal. Por ello, una inobservancia del ya mencionado principio de transparencia por parte de la Administración, podría conllevar la vulneración del derecho a la protección de datos del ciudadano.

De manera que, para que la Administración pueda recabar válidamente este consentimiento para el empleo de sistemas de IA, es preciso que toda la información relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Asimismo, el ciudadano debe tener un conocimiento pleno de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con este tratamiento. Pues además de la obligación del cumplimiento del principio de transparencia que se exige con carácter general a las Administraciones Públicas, en el ámbito de la protección de datos, esta obligación se intensifica por imposición del art. 12 y siguientes del RGPD [132]

En el lado opuesto, nos encontramos los casos en los que concurre la llamada paradoja de la privacidad. Que, en palabas de SORIANO ARRANZ (2021), se define como *"la forma en la que las personas no valoran de manera racional los daños futuros que pueden derivarse de compartir sus datos en el presente. Así, se da prioridad a los beneficios a corto plazo generados por el acceso a los servicios digitales que, como contraprestación, exigen, solicitan o incluso toman sin prácticamente informar de ello, una generosa cantidad de todos aquellos datos*

diferentes tipos de responsables y encargados del tratamiento de datos y diferentes situaciones de tratamiento, incluida una lista de verificación con todos los requisitos que deben cumplirse para anonimizar suficientemente los datos.

132 Ello conforme a lo previsto en los art. 12 y ss RGPD, y en especial, en cumplimiento del principio de transparencia regulado en el art. 12 y desarrollado por el considerando 39 y 58 del mismo texto legal.

de carácter personal relacionados con la interacción o susceptibles de ser recopilados aprovechándola."[133]

Por todo ello, resulta tan complejo para la Administración recabar debidamente el consentimiento del ciudadano para el uso de sus datos en sistemas de tecnología de IA, y éste se encuentra vulnerable frente a las posibles intromisiones en su derecho a la protección de datos de carácter personal. Pues, tal como acertadamente apunta MANTELERO (2018): "*el consentimiento puede ser considerado como tal solo si es libre e informado. Estos requisitos del consentimiento, sobre los que se basa la noción de autodeterminación, están perdiendo fuerza frente a la utilización de técnicas de tratamiento de la información basada en el Big Data*". [134]

Además de todo lo anterior, como ya hemos anticipado, cuando se emplean herramientas de IA para el tratamiento masivo de datos de los ciudadanos, la protección de los derechos fundamentales debería plantear desde una dimensión colectiva. Pero en el caso del derecho a la protección de datos, en los que media el consentimiento otorgado individualmente por cada ciudadano, esta dimensión se torna más complicada de abordar. Pues si el ciudadano tiene una percepción muy limitada de los riesgos que puede implicar el tratamiento de sus datos a nivel individual, aún más le costará comprender las implicaciones potenciales que podría llevar aparejada para la sociedad en su conjunto (o determinados colectivos) y valorar esta dimensión al otorgar su consentimiento.

4.2. Inteligencia artificial y decisiones automatizadas.

Sin perjuicio del deber de información a los ciudadanos que se encuentren interactuando directamente con sistemas de IA (impuesto con carácter general en el citado art. 50.1 RIA), a efectos de amparar el derecho de protección de datos de carácter personal de la población, es indispensable que la Administración además siempre comunique expresamente a los ciudadanos

---

133 SORIANO ARNANZ, A., "Decisiones automatizadas y discriminación: aproximación y propuestas generales" *Revista General de Derecho Administrativo,* n.° 56, 2021, http://laadministracionaldia.inap.es/noticia.asp?id=1511706. Remite a Athey, S., Catalini, C. y Tucker, C., «The digital privacy paradox: small money, small costs, small talk», MIT Sloan Research Paper No. 5196-17, 2017.

134 MANTELERO, A. *El Big Data en el marco del Reglamento General de Protección de Datos,* Barcelona, UOC, 2018, p.9.

en las situaciones en que se encuentren interactuando con un sistema de IA, que recopile sus datos de manera automatizada (por imposición del art 13.2 f) del Reglamento General de Protección de datos). Teniendo la obligación de informar correctamente de la importancia y consecuencias que pueden conllevar este tratamiento para el individuo.

Con ello, se trata de proteger al ciudadano para evitar que sea objeto de una decisión basada exclusivamente en la elaboración de sus datos, incluida la elaboración de perfiles[135].

Si bien es cierto que el derecho del ciudadano a no ser objeto de estas decisiones automatizadas no es aplicable en los casos en que el individuo haya prestado su consentimiento explícito previo, ni en el supuesto de que fuera necesario para la celebración (o ejecución) de un contrato entre el individuo y el responsable del tratamiento. En todo caso, la intervención de la actuación de los sistemas de IA no es ilimitado en estos dos supuestos, pues la ley prevé que el responsable de los datos siempre debe garantizar el derecho del ciudadano a obtener intervención humana.[136]

Por último, los Poderes Públicos podrían tratar de manera automatizada los datos de los ciudadanos sin su consentimiento, en supuestos en que esté autorizado por el Derecho de la Unión Europea o de los Estados Miembros, y siempre que se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado. Como en los casos en que se encuentre en juego la seguridad nacional o exista orden judicial.

En todo caso, los datos en los que se basan estas decisiones automatizadas no pueden pertenecer a las categorías especiales de datos (que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física). Siendo ésta una práctica que, pese a encontrarse expresamente

---

135 Art. 22.1 del Reglamento General de Protección de Datos en relación con el art. 13.2 f) del mismo texto legal y el art. 11 LGPD. Entendiéndose como elaboración de perfiles a estos efectos, cualquier tratamiento automatizado de datos personales, que utiliza dichos datos para evaluar ciertos aspectos de la persona y analizar o predecir sus intereses, comportamiento y otros atributos (Art. 4 del RGPD).

136 Art. 22.3 RGPD.

prohibida[137], a raíz de la implantación de la IA en las decisiones automatizadas con tratamientos masivos de datos, cada vez es mas frecuente.

Tal como ocurrió en el caso del llamado *"escándalo de las ayudas a la infancia"* de los Países Bajos, que, entre otras reacciones, originó un Informe de la Comisión de Venecia de 18 de octubre de 2021.[138]

En este supuesto, la Administración Tributaria, aplicó un sistema algorítmico de IA, mediante el cual realizaba controles a gran escala de las familias que tenían previamente reconocidas las ayudas para comprobar los posibles fraudes. En caso de detectarse una irregularidad, incluso años después de la concesión de la asignación, los beneficiados por las ayudas tendrían que devolver la totalidad del importe (llegando en algunos casos a sumas de hasta 30.000 euros). Uno de los parámetros utilizados para identificar los casos sospechosos de fraude era la ciudadanía, y el algoritmo, sistemáticamente seleccionaba a los solicitantes de origen extranjero para un examen detallado de sus peticiones.

Así, el referido Informe de la Comisión de Venecia (puntos 95 y 96) concluyó que el Gobierno de Países Bajos, al basar el criterio de la nacionalidad como elemento para identificar el fraude, estaría vulnerando el art. 22.4 RGPD, sobre decisiones individuales automatizadas. Y que además *"las prácticas discriminatorias se sistematizaron mediante algoritmos"*.

V. EL DERECHO A LA NO DISCRIMINACIÓN Y LA INTELIGENCIA ARTIFICIAL.

5.1. Sesgos discriminatorios de los algoritmos de la IA.

Otro de los derechos fundamentales que está generando una mayor colisión en el empleo de la IA por parte de los Poderes Públicos, es el derecho a la no discriminación del ciudadano, consagrado en el artículo 21 de la Carta de los Derechos Fundamentales de la Unión Europea (UE), y en el artículo 14 de nuestra Constitución Española.

---

137 22.4 RGPD.

138 CDL-AD(2021)031-e, Netherlands - Opinion on the Legal Protection of Citizens, adopted Venice Commission at its 128th Plenary Session (Venice and online, 15-16 October 2021) https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2021)031-e (recuperado: noviembre 2024).

El mayor reto a la protección de tal derecho lo encontramos en los sesgos de los algoritmos en los que se basan las herramientas de IA. Pues en la medida que estos algoritmos tomen como referencia datos sesgados o que reflejen discriminaciones de género, raza o cualquier otra condición, las decisiones que se fundamenten en los mismos serán potencialmente discriminatorias para tales individuos o colectivos.

Estos sesgos discriminatorios pueden generarse en cualquiera de las fases del proceso de funcionamiento de la IA, incluso en el uso que hacen de estos sistemas los propios usuarios o sus resultados de salida.

Pero en la gran mayoría de los casos la discriminación o sesgos algorítmicos vienen ocasionados por decisiones adoptadas en el desarrollo, implantación y uso del sistema de IA. Siendo que esta discriminación se puede dar por "*inacción*" (art. 4.1º *in fine* Ley 15/2022) o el "*incumplimiento de los deberes",* como puedan ser las obligaciones de responsabilidad proactiva en el diseño, control o evaluación del sistema de IA que exige la normativa de protección de datos el propio reglamento de IA.[139]

Para establecer el grado de afectación del sesgo del algoritmo en un caso determinado, no sólo hay que tener en cuenta la afectación al ciudadano concreto afectado por un modelo de IA, sino que hay que valorar el peligro que supone que ese error o sesgo masivo se replique en miles de decisiones. Pues como se ha dicho, en el tratamiento de macrodatos, debe valorarse la dimensión colectiva de la protección de los derechos fundamentales. En este caso, además, hay que tener en cuenta que si el error no se controla, analiza y en su caso se corrige, las decisiones erróneas pasarán a ser macrodatos que alimentará a los futuros algoritmos, creándose espirales de sesgos, haciendo que ese sesgo se cronifique.

El propio Libro Blanco de Inteligencia Artificial (p.14), aborda esta problemática, y reconoce que: "*Puede suceder que el uso de determinados algoritmos de la IA para predecir la reincidencia delictiva dé lugar a prejuicios raciales o de género, y prevea una probabilidad de reincidencia distinta para hombres y mujeres o para nacionales y extranjeros. (Fuente: Tolan S., Miron M., Gomez E. and Castillo C. "Why Machine Learning May Lead to Unfairness: Evidence from Risk*

139 CONTINO HUESO L. Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público. En *inteligencia artificial y sector público. eduardo gamero casado*. Tirant lo blanch. 2023, pp. 257-338.

Assessment for Juvenile Justice in Catalonia", Best Paper Award, International Conference on AI and Law, 2019.)

Algunos programas de IA de análisis facial muestran prejuicios raciales o de género, y presentan un bajo nivel de error a la hora de determinar el género de hombres de piel más clara, pero un elevado nivel de error al determinar el género de mujeres de piel más oscura. Fuente: Joy Buolamwini, Timnit Gebru; Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018"

Si bien es cierto que los prejuicios y la discriminación son riesgos inherentes a toda actividad social o económica, en el caso de la IA, esta misma subjetividad puede tener efectos mucho más amplios, y afectar y discriminar a numerosas personas sin que existan mecanismos como los de control social que rigen el comportamiento humano.[140]

Estos sesgos disciminatorios vienen originados, principalmente, por la mala calidad de los datos sobre los que se alimenta el algoritmo de la IA. Es decir, se generan debido a la falta de datos de entrenamiento y de prueba diversos y de alta calidad, por ejemplo, cuando se utilizan conjuntos de datos que no representan suficientemente a los grupos vulnerables, o cuando la definición de la tarea o el establecimiento de los propios requisitos están sesgados.

Por otro lado, también pueden producirse estos sesgos por la falta de diversidad en los equipos de desarrolladores de la IA, que refuerza los sesgos intrínsecos, debido al volumen limitado de datos de entrenamiento, o cuando un desarrollador de IA sesgado ha comprometido el algoritmo.[141]

De esta manera, los sesgos estructurales presentes en nuestra sociedad correrían el riesgo de repetirse e incluso incrementarse por los sistemas de la IA de automatización. Pues los algoritmos aprenden a ser tan discriminatorios como los datos con los que trabajan y, como consecuencia de unos datos de entrenamiento de baja calidad o los sesgos y la discriminación observados en la sociedad, podrían sugerir decisiones que son inherentemente discriminatorias. Además, como decimos, podría incluso reforzar los perjuicios existentes en la

---

140 PRESNO LINERA, M.A., *Derechos fundamentales e inteligencia artificial,* Ed.Marcial Pons, 2022.

141 Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)), p.93.

sociedad en tanto que la IA, a diferencia de los humanos, carece de empatía y no puede contrarrestar de manera consciente los prejuicios aprendidos.

Y esto es lo que ha ocurrido con dos de los sistemas de algoritmos de IA utilizados en el ámbito judicial en Estados Unidos y Reino Unido, HART y COMPAS, que permiten determinar el riesgo de reincidencia de un acusado por medio del análisis de distintas variables de predictivos de riesgo.

Pues bien, tras su uso durante años, se ha demostrado que ambos sistemas presentan sesgos discriminatorios. Por ejemplo, en el caso de COMPAS, se demostró la existencia de un sesgo racial indirecto en los modelos que predicen el riesgo de reincidencia mediante el uso de variables sustitutivas que no son neutrales. Aunque la doctrina no es pacífica, diversos estudios afirman que aplicando el citado algoritmo los acusados de raza negra tenían casi el doble de probabilidades en relación con aquellos de raza blanca de ser considerados en situación de alto riesgo de reiteración delictiva[142] Tanto el proyecto COMPAS como HART muestran los problemas de un enfoque discriminatorio o determinista, el cual debería basarse más bien en los sistemas europeos, civilistas, que abrazan la reinserción social. [143]

Otro de los principales riesgos de discriminación en los usos de los sistemas de IA son los derivados de la identificación biométrica. Puesto que las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica remota en tiempo real[144] de las personas físicas pueden dar lugar

---

142 BABUTA, A.; OSWALD, M.; RINIK, C. (2018). «Machine learning algorithms and police decision-making: legal, ethical and regulatory challenges». *Whitehall Report*, núm. 3. Royal United Services Institute for Defense and Security Studies., p.7

143 SIMÓN CASTELLANO P., "*Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?"* IDP. *Revista de Internet, Derecho y Política,* nº 33, 2021, pp.8-9.

144 A estos efectos, cabe recordar la definición que realiza en el art. 3 el Reglamento de estos conceptos:

34) «Datos biométricos»: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

41)«Sistema de identificación biométrica remota»: un sistema de IA destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia;

42) «sistema de identificación biométrica remota en tiempo real»: un sistema de identi-

fácilmente a resultados sesgados y tener consecuencias discriminatorias (debido a la inmediatez con la que operan los sistemas y las dificultades de comprobación o corrección). Esto es especialmente importante en lo que respecta a la edad, la etnia, el sexo o la discapacidad.

En consecuencia, el art. 5.1. h) RIA prohibe expresamente las prácticas de IA que impliquen el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía de acceso del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para la búsqueda selectiva de posibles víctimas de secuestro o personas desaparecidas, trata de seres humanos o explotación sexual; la prevención de una amenaza específica (importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista); y la localización o la identificación o el enjuiciamiento de la persona sospechosa de haber cometido un delito para el que se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de cuatro años.

5.2. Medidas para la corrección de sesgos discriminatorios y garantías frente a los mismos.

Para evitar la existencia de sesgos discriminatorios en una primera fase del proceso de automatización de los datos mediante sistemas de IA, debe garantizarse la utilización de conjuntos de datos que sean suficientemente representativos, especialmente para garantizar que todas las dimensiones de género, etnicidad y otras posibles razones de discriminación ilícita queden correctamente reflejadas en estos conjuntos de datos.

Asimismo, para impedir la existencia de sesgos intrínsecos de los propios desarrolladores de la IA es necesario que se promueva la diversidad en los equipos que desarrollan y aplican las aplicaciones específicas de la IA y evalúan sus riesgos, y en segundo lugar, que se utilicen datos de calidad desglosa-

ficación biométrica remota, en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa; engloba no solo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas;

43)«sistema de identificación biométrica remota en diferido»: cualquier sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota en tiempo real;

dos por género para evaluar los algoritmos de IA y de que el análisis de género forme parte de todas las evaluaciones de riesgo de la IA[145]

Si se detectase la existencia de sesgos discriminatorios en los algoritmos de la IA, en la gran mayoría de casos pueden ser corregidos durante el proceso de automatización de datos. Por tanto, es necesario asegurar en todo caso la intervención humana en el proceso automatizado para este fin, y establecer distintos niveles de control en los sistemas de IA.

En todo caso, la reproducción de estos sesgos discriminatorios debe ser debidamente controlada y castigada, en tanto que el RIA prohíbe expresamente las prácticas discriminatorias, y prevé las sanciones por su incumplimiento:

Concretamente, en su artículo 5 prohíbe la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA con el fin de evaluar o clasificar a personas físicas o colectivos durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la clasificación resultante provoque un trato perjudicial o desfavorable hacia una persona o colectivo que no guarden relación con los contextos en los que se generaron originalmente los datos o que dicho trato sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.

Ese mismo artículo, para evitar la discriminación a personas y grupos en situación de vulnerabilidad, prohíbe también la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona o colectivo, derivadas de su edad o discapacidad o de su situación social o económica para alterar el comportamiento de dicha persona (o de otra persona que pertenezca a dicho grupo), de modo que provoque (o sea probable) perjuicios considerables a esa persona u otra.

En cualquier caso, cabe recordar en este punto que si la Administración Pública emitiese una disposición, acto o cláusula administrativa en base a alguno de los supuestos anteriormente expuestos, se trataría de causa de nulidad de pleno derecho del artículo 47. 1. a) LPAC.

145 Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)), p.229.

El derecho a la tutela judicial efectiva y la inteligencia artificial.

6.1.El derecho a la tutela judicial efectiva en la era del algoritmo.

Cuando los Poderes Públicos generan actos administrativos o decisiones basadas en IA (ya sea como herramienta de apoyo o autónoma), sin dar a conocer al ciudadano cómo el algoritmo ha motivado dichas decisiones, podría incurrir en una vulneración del derecho a la tutela judicial efectiva, reconocida en el art. 24 de la Constitución Española y el art. 47 de la Carta de Derechos Fundamentales de la Unión Europea.

En primer lugar, cabe plantearse en qué grado puede emplearse el algoritmos de IA en el proceso, para poder ser admisible en nuestro ordenamiento jurídico sin conllevar una vulneración del derecho a un proceso con todas las garantías, reconocido en el art. 24 CE.

Para lo que habrá que valorar su posible afección en el principio inherente al titular de la potestad jurisdiccional: el principio de imparcialidad judicial, así como en la igualdad de las partes en el proceso, como principio general del proceso, y en el principio de contradicción materializado en el proceso en el derecho fundamental de audiencia o defensa. Y en un primer plano, si el algoritmo no estuviese configurado de forma adecuada o presenta sesgos el resultado de su análisis afectará a la imparcialidad del juzgador en el momento de dictar la sentencia porque su convicción judicial estará condicionada al determinado sesgo que presente la herramienta de inteligencia artificial (sesgo de género, etnia, edad, clase social, etc. o incluso determinados principios y valores del autor de la herramienta e implícitos en ella). Por el contrario, si se consigue que la herramienta de IA que se use tenga un alto grado de fiabilidad y, por lo tanto, sea admisible en el proceso judicial, igualmente afectará a la convicción judicial; en este caso, en el momento de valoración de la prueba por la alta posibilidad de que el juez esté conforme con los resultados de la prueba y base en éstos su resolución.[146]

Si bien es cierto que, como adelantábamos *ut supra* no siempre resulta posible explicar por qué un modelo de IA ha generado una decisión en particular (algoritmos *caja negra*), y que en tales circunstancias puede ser necesario adop-

146 DE MIGUEL BERIAIN, I., "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados". *Revista de Derecho UNED,* núm. 25, 2019, pp. 531-561.

tar otras medidas relacionadas con la explicabilidad (por ejemplo, la trazabilidad, la auditabilidad y la comunicación transparente sobre las prestaciones del sistema), el grado de necesidad de explicabilidad depende en gran medida del contexto y la gravedad de las consecuencias derivadas de un resultado erróneo.[147]

Y en este último punto, los poderes públicos deben de prestar especial atención a la explicabilidad del algoritmo, atendiendo a las circunstancias del caso. E incidiendo en aquellos supuestos que impliquen sistemas de IA de alto riesgo, para los cuales el RIA ha reconocido expresamente, en su artículo 86 el "*derecho a explicación*" a aquellas personas que se hayan visto afectadas por los resultados de salida de tales sistemas. De manera que, quien considere que tal decisión tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada.

Como propone AMONI REVERÓN (2022), para poder implantar debidamente sistemas de IA en la toma de decisiones sin causar indefensión al ciudadano, cabe la posibilidad de acudir a expertos para interpretar dichos algoritmos. Surgiendo así el derecho a un intérprete, como posible solución a los problemas de opacidad de los algoritmos, que será un conocedor de la materia, que realizará una experticia y explicará el proceso de toma decisiones, así como la información tenida en cuenta. El algoritmo puede entregarse en un formato digital que permita al experto analizarlo y explicar al interesado los motivos de la máquina para decidir y cómo llegó a esa decisión.[148]

Por lo que respecta al ámbito de las investigaciones policiales, se han implantado sistemas de IA con el fin de anticiparse a la comisión de posibles

147 El art. 23.2 de la referida Ley 15/2022 establece en esta materia que las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos.

148 AMONI REVERÓN,G., Libertad, presunción de inocencia y defensa ante la irrupción de la inteligencia artificial en el ámbito policial y judicial penal. En Contino Hueso, L., *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi. 2022., pp 364-452.

delitos y, poder adoptar medidas preventivas necesarias, sistemas tales como *VeriPol*[149], *PredPol*[150] , *CompStat* [151]o a *VioGen*[152].

Cabe mencionar que estas herramientas ya han presentado en la práctica problemas de transparencia y la legalidad del tratamiento que hace de los datos. Concretamente, con respecto al sistema español *Viogen*, se ha determinado mediante auditoría efectuada en enero de 2022, que el sistema no es transparente, pues ni los auditores externos ni las víctimas tienen acceso a la información empleada, ni se ha realizado una evaluación de impacto del sistema conforme al RGPD.

Si bien todas estas herramientas permite reducir tiempos y costes en los procedimientos simplificando los modelos decisorios, no podemos olvidar que estos instrumentos actualmente todavía se encuentran configurados como meros instrumentos de auxilio, para facilitar la actividad del órgano público, pero no tienen permitido sustituir su poder de decisión, tan si quiera en vía administrativa.

En este sentido, se pronunció la sentencia dictada por el Tribunal Administrativo Regional de Lazio de 13 de septiembre de 2019,[153] que resolvió que las decisiones administrativas que puedan incidir en situaciones jurídicas subjetivas no podrán ser tomadas de modo exclusivo por un programa informático, incluso si este ha alcanzado el mayor grado de precisión y perfección, dado que tal actividad solo puede lograrse con un funcionario-persona física. Siendo el papel de los procedimientos informáticos mediante

---

149 Un algoritmo que, basado en el lenguaje de una denuncia presentada, indica la probabilidad de que esta no sea verdad, ayudando por tanto a los policías a enfocar la investigación de forma más eficaz, y así desincentivar las denuncias falsas.

150 Software de IA utilizado en Estados Unidos para dirigir las operaciones policiales. Mediante un sistema predictivo de algoritmos trata detectar el punto geográfico en el que se producirá un delito.

151 Herramienta de IA multifuncional que permite a los departamentos de policía maximizar su estrategia de lucha contra el crimen para reducir y prevenir el delito.

152 Sistema algorítmico que determina en España el nivel de riesgo de una víctima de violencia de género en orden al establecimiento de medidas de protección.

153 Il Tribunale Amministrativo Regionale per il Lazio (Sezione Terza Bis)N. 10964/2019 REG.PROV.COLL.N. 12332/2016 REG.RIC. 13/09/2019 https://canestrinilex.com/risorse/algoritmo-che-decide-giammai-tar-lazio-1096419/.

algoritmos, meramente instrumentales o auxiliares. Por lo que consideró que se había vulnerado el derecho a un proceso equitativo, reconocido en el art. 6 del Convenio Europeo de Derechos Humanos y tutela judicial reconocida en el art. 24 de la Constitución Italiana.

El carácter preceptivo de la intervención humana, que aborda esta sentencia en el ámbito administrativo, se ve intensificado aún más en el ámbito judicial, especialmente en la jurisdicción penal. Pues la aceptación paulatina de mecanismos de análisis de la toma de decisiones probabilísticos de IA funciona a partir de parámetros jurídicos totalmente diferentes a los tradicionales. Por ejemplo, las condenas o absoluciones dependen de un umbral de certeza a partir de los cuales un sistema suficientemente efectivo de cálculo de probabilidades de autoría en el que confiemos sobradamente nos permitirá decidir sobre la condena o absolución de los casos. Este modo de funcionar es completamente diferente al tradicional de presunción de inocencia, ya que cuantificado ese umbral de probabilidad se asume como aceptable e inevitable que se condene a inocentes.[154]

Cabe poner en relieve en este punto que aquellos "*sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, (o a ser utilizados de forma similar en una resolución alternativa de litigios)"* se clasifican *per se* como sistemas de alto riesgo, por el art.6.2. RIA, en relación con el apartado 8 del Anexo III, del mismo.

Por lo que en este punto, (y sin perjuicio de las implicaciones éticas que conllevaría aparejadas) algunos autores se cuestionan si una implantación futura de este modelo de IA, con funcionamiento prácticamente autónomo para determinadas esferas del ámbito judicial, podría vulnerar principios básicos de nuestro ordenamiento jurídico como es el *in dubio pro reo.*

---

154 Con este razonamiento, el autor Boix Palop defiende la ya mencionada postura de reconocimiento del algoritmo como reglamento: Boix Palop, A. *Los Algoritmos Son Reglamentos: La Necesidad De Extender Las Garantías Propias De Las Normas Reglamentarias A Los Programas Empleados Por La Administración Para La Adopción De Decisiones*. Revista de Derecho Público: Teoría y Método Marcial Pons Ediciones Jurídicas y Sociales. Vol 1, 2020, pp. 223-270. DOI: 10.37417/RPD/vol_1_2020_33

De manera que, como afirma FAGIANNI (2022), para proteger al ciudadano de lo que denomina el "*due process of law algorítmico*" en este nuevo concepto de "*justicia compartida*", basado en una suerte de colaboración entre los modelos de IA, autoridades de policía, los fiscales y el juez, es éste último quien tiene que seguir ostentando el monopolio del ejercicio del *ius puniendi*. Por lo que se está hablando de un fenómeno de "*responsabilización de los jueces*", desde la perspectiva del respeto de la independencia e imparcialidad del pronunciamiento por la influencia que puede tener el algoritmo en el proceso decisorio. Por lo que este condicionamiento de la voluntad por la IA impone la obligación de reflexionar sobre la necesidad de una mayor dotación a los jueces de mayores garantías para proteger su autonomía respecto a su decisión en relación con la IA, puesto que atendiendo al requisito de jurisdiccionalidad, no pueden limitarse a ratificar la solución de una máquina.[155]

6.2. El algoritmo como instrumento de graduación de la condena judicial.

En este punto, es preciso poner en relieve el caso "hito" en el que un órgano judicial admitió por primera vez en la historia el uso de un algoritmo de Inteligencia Artificial para graduar la sanción de un reo y que puede resultar ilustrativo con respecto al derecho a la tutela judicial efectiva en este ámbito.[156] Se trata de la sentencia del Tribunal Supremo de Wisconsin dictada en julio de 2016, en el caso *State vs Loomis.*[157]

En este caso concreto, Eric Loomis fue acusado de cinco delitos por su presunta intervención en un tiroteo efectuado desde un vehículo. El acusado, aunque negó ser el autor de los disparos (cargos por posesión de arma de fuego), reconoció la conducción del vehículo (y en consecuencia, los cargos de conducción de vehículo ajeno sin la autorización y peligro de seguridad pública). Por lo que llegó a una conformidad con la fiscalía aceptando estos

---

155 FAGGIANI V., "El derecho a un proceso con todas las garantías ante los cambios de paradigma de la inteligencia artificial", *Teoría y Realidad Constitucional*, núm. 50., 2022, pp.517-546.

156 Siendo objeto de análisis por diversos autores, entre otros: PRESNO LINERA, M.A., Derechos fundamentales e inteligencia artificial, Ed.Marcial Pons, 2022, pp. 33-35, MARTÍNEZ GARAY L., "Peligrosidad, algoritmos y due process: el caso State v Loomis" UNED. *Revista de Derecho Penal y Criminología, 3.a Época, n.o 20 (2018)*

157 State v. Loomis, 881, N.W.2d 749, 7532 (Wis, 2016).

dos últimos cargos, y negando las restantes acusaciones. El juez de instancia en su sentencia, para aceptar la confomidad y graduar la pena, se fundamentó en un informe de evaluación del acusado el informe realizado por el software COMPAS (*Correctional Offender Management Profiling for Alter- native Sanctions*), el cual emite una evaluación de riesgo de reincidencia partiendo de una entrevista realizada al acusado y de sus antecedentes penales, pero como la metodología que utiliza está protegida como secreto comercial solo se reportan al tribunal los resultados del análisis.

Este informe, basado en un algoritmo predictivo de riesgo a través del algoritmo de IA, concluyó que el acusado tenía un elevada probabilidad de reincidencia, concluyendo que representaba "*un alto riesgo para la comunidad*".

Loomis impugnó la sentencia de instancia ante el Tribunal Supremo de Wisconsin, fundamentando su recurso en la vulneración del derecho al debido proceso (*right to due process*) por tres razones: *(1) viola el derecho del acusado a ser sentenciado con base en información precisa, en parte debido a la naturaleza patentada de COMPAS, lo que impide evaluar su exactitud; (2) viola el derecho del acusado a una sentencia individualizada; y (3) utiliza indebidamente evaluaciones de género en las sentencias"*[158]

El Tribunal Supremo Estatal (Supreme Court of Wisconsin), desestimó el recurso al considerar que no vulneraba el derecho a la tutela judicial efectiva, en base a las siguientes fundamentaciones a sus motivos de recurso:

En primer lugar, el acusado no precisaba conocer el funcionamiento concreto del algoritmo, puesto que el sistema COMPAS "*al ser un instrumento patentado que cuenta con secreto comercial, no revela cómo se determinan las puntuaciones de riesgo o cómo se ponderan los factores*". Para ello, fue suficiente que el acusado conociera los factores concretos que había utilizado el sistema COMPAS para valorar el riesgos.

Y en este punto, la sentencia puso sobre la mesa por primera vez el debate (ya detallado *ut supra*) entre la colisión de la protección de la propiedad intelectual de la empresa titular del algoritmo.

El segundo motivo de recurso, se desestimó por entender que la sentencia se ajustaba al caso concreto, puesto que las valoraciones de riesgo aportadas

158 State v. Loomis, 881, N.W.2d 749, 7532, p. 13 (Wis, 2016).

al Tribunal, junto con las restantes circunstancias concurrentes al caso, constituían información suficiente.

Con respecto al último de los motivos del recurso se desestimó por considerar que el sistema COMPAS no suponía una utilización indebida del género. Destacó que tanto la Fiscalía como la defensa habían aceptado en el juicio que toda la evidencia científica disponible indica que los varones tienen unas tasas de reincidencia y de delincuencia violenta superiores a las de las mujeres. Siendo esto así, el Tribunal entendió que prescindir del factor género en la valoración del riesgo disminuiría sensiblemente el acierto de las estimaciones, porque aumentarían las tasas de error tanto para los hombres como para las mujeres. En consecuencia, si incluir el género aumenta la precisión en las estimaciones de riesgo, ello no persigue un objetivo discriminatorio sino que va en beneficio tanto de los acusados como de la administración de justicia en general.

Por último, la sentencia establece los casos específicos en los que pueden utilizarse las valoraciones de riesgo mediante algoritmos:

1. Imponer a delincuentes de bajo riesgo medidas alternativas a la prisión;

2. Valorar si un delincuente puede ser supervisado de manera segura y efectiva en la comunidad,

3. Determinar los plazos y condiciones de la suspensión de la pena y de la libertad condicional y las consecuencias de infringirla. Pero no pueden usarse para decidir una condena privativa de libertad del individuo.

Además establece también que los tribunales deben fundamentar siempre qué otros factores han sido valorados para determinar la condena, además de la valoración de riesgo.

Por lo que esta paradigmática resolución del caso *State vs Loomis*, no ajena a las críticas, ha sentado las bases de la doctrina posterior, fijando los requisitos para la correcta implantación de evaluaciones predictivas de riesgo mediante IA para la graduación de la condena.

Desde el punto de vista de la tutela judicial efectiva, cabe resaltar que el acusado únicamente pudo conocer los datos introducidos en el sistema COMPAS y el resultado del mismo, pero no la relación de causalidad entre éstos, ni la motivación del resultado.

A diferencia de un testigo o un perito, que puede someterse a un interrogatorio por la representación letrada del acusado, el software COMPAS no puede ser cuestionado en juicio, y aun así es tanto o más poderoso que un testigo experto influenciando la sentencia.[159]

Y por este motivo, cabe plantearse las cuestiones expuestas por CASTELLANOS CARAMUNT. J, MONTERO CARO, M.D (2020)[160] de manera que si, no habiendo podido conocer el condenado todos los extremos que motivan la resolución judicial, ni el grado en que la intervención del sistema de IA ha afectado a la graduación de su condena, ello implicaría una violación de su derecho a la tutela judicial efectiva, por vulnerar lo previsto en el art. 120.3 CE, al no haber obtenido en su proceso una resolución debidamente motivada. O por el contrario, más bien debe entenderse el sistema de IA como un elemento que facilita al juzgador su labor mediante cuestiones técnicas (como puede ser la elaboración de perfiles de riesgo en base a criterios estadísticos), equiparable a cualquier otro elemento técnico que influya en la decisión judicial (similar a la de un perito). Entendiendo por tanto que el juez no debe tener un conocimiento profundo en toda materia, más allá de la exigencia del principio *iura novit curia.*

CONCLUSIONES.

Actualmente, los sistemas de IA aún se encuentran en un momento inicial de su desarrollo dentro del contexto tecnológico emergente en el que nos situamos, por lo que no es posible valorar ni su potencial total ni, por consiguiente, el alcance de los posibles riesgos que su indebida aplicación por parte de los poderes públicos, puede implicar en la vulneración de los derechos fundamentales de los ciudadanos.

---

159 AMONI REVERÓN,G., Libertad, presunción de inocencia y defensa ante la irrupción de la inteligencia artificial en el ámbito policial y judicial penal. En Contino Hueso, L., *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, 2022.pp. 364-452.

160 CASTELLANOS CARAMUNT. J, MONTERO CARO, M.D., "Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales," *Ius et scientia,* 2. 2020.

No en vano, se ha puesto en evidencia que el principal reto de los poderes públicos para la protección de tales derechos pasa por mejorar la opacidad de los algoritmos, principalmente en los usos de la IA en la toma de decisiones administrativas automatizadas mediante macrodatos. Por lo que es preciso fortalecer la transparencia del uso de la IA en el sector público en este ámbito, basado en mecanismos de auditoría y rendición de cuentas. Pues sólo así podrá recabar el válidamente el consentimiento del ciudadano para el tratamiento de sus datos de carácter personal en el ámbito del *big data*.

Asimismo, las obligaciones de transparencia de los sistemas de IA, deberían ser objeto de un mayor desarrollo normativo y clarificación, en tanto que se trata de una pieza elemental en esta materia y en constante colisión con los derechos de la propiedad intelectual del algoritmo.

Y en tanto que el sector público realiza un tratamiento masivo de datos de la población, es de vital importancia trabajar la protección de los derechos fundamentales frente a los usos derivados de la IA, desde la dimensión colectiva o supraindividual de los derechos.

En la implantación de los sistemas de IA en el sector público, tanto en el ámbito judicial como administrativo, la principal problemática la encontramos es la colisión del derecho a la propiedad intelectual de los algoritmos de la IA y el principio de transparencia que se exige a los poderes públicos. Lo que no ocurre en el ámbito privado, en tanto que el deber de transparencia que se requiere es menor, por lo que tiende a protegerse el derecho a la propiedad intelectual y el secreto comercial del algoritmo con mayor frecuencia en estos casos.

Ante la falta de una sólida regulación específica y de interpretaciones jurisprudenciales en materia de IA, el marco normativo relativo a la protección de datos de carácter personal ha venido absorbiendo el tratamiento jurídico del uso de la IA por los poderes públicos.

Pero resulta patente la urgente necesidad de crear un marco normativo que, siendo garantista de los derechos fundamentales, sea a su vez lo suficientemente flexible para adaptarse a los cambios de las nuevas tecnologías de la IA, sin coartar su desarrollo.

Pues, en definitiva, si bien los poderes públicos deben tomar las pertinentes medidas en los usos de la IA para evitar la desprotección de los derechos fundamentales de la población, no pueden permanecer indiferentes ante los

múltiples beneficios que lleva aparejada su implantación para la mejora de su eficiencia, ni quedarse relegados en la era de las nuevas tecnologías.

BIBLIOGRAFÍA

AMONI REVERÓN,G., 2022, Libertad, presunción de inocencia y defensa ante la irrupción de la inteligencia artificial en el ámbito policial y judicial penal. En Contino Hueso, L., *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, pp 364-452.

BOIX PALOP, A. 2020, *Los Algoritmos Son Reglamentos: La Necesidad De Extender Las Garantías Propias De Las Normas Reglamentarias A Los Programas Empleados Por La Administración Para La Adopción De Decisiones*. Revista de Derecho Público: Teoría y Método Marcial Pons Ediciones Jurídicas y Sociales. (Vol 1), pp. 223-270. DOI: 10.37417/RPD/vol_1_2020_33. (recuperado noviembre 2024)

CASTELLANOS CARAMUNT. J, MONTERO CARO, M.D., 2020, *Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales*, Ius et scientia, 2.

CASTILLA BAREA, M. "Vigilancia, postcomercialización, códigos de conducta y directrices" en Barrio Andrés. M, *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, 2024, p.178.

CERILLO MARTÍNEZ, A., 2019, *El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?*, 50, Revista General de Derecho Administrativo (Iustel).

COTINO HUESO, L., 2017, *Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales*, Revista Dilemata nº 24, 2017, p. 131-150

2023: Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público. En *inteligencia artificial y sector público. eduardo gamero casado*. Tirant lo blanch. 2023, pp. 257-338.

DE MIGUEL BERIAIN, I., 2019, *La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados.* Revista de Derecho UNED, núm. 25, pp. 531-561.

FAGGIANI V., 2022, *El derecho a un proceso con todas las garantías ante los cambios de paradigma de la inteligencia artificial*, Teoría y Realidad Constitucional, núm. 50., pp.517-546.

GAVARA DE CARA, J. C., 2007, *La vinculación positiva de los poderes públicos a los derechos fundamentales,* Teoría y realidad constitucional, n.° 20, pp. 277-278.

GIL GONZÁLEZ, E., Ed. BOE, 2016, p. 18, https://www.aepd.es/sites/default/files/2019-10/big-data.pdf (recuperado noviembre 2024).

HUERGO LORA, A. 2020. Una aproximación a los algoritmos desde el Derecho Administrativo. En A. Huergo Lora (dir.) y G. M. Díaz González (coord.), *La regulación de los algoritmos*, Thomson-Reuters Aranzadi. P.64.

MANTELERO, A. *El Big Data en el marco del Reglamento General de Protección de Datos,* Barcelona, UOC, 2018, p.9.

MARTÍNEZ GARAY L., "Peligrosidad, algoritmos y due process: el caso State v Loomis" UNED. *Revista de Derecho Penal y Criminología, 3.a Época, n. 20 (2018)*

MATHISON TURING, A 1950, "*Computing Machinery and Intelligence*", Mind, 49, pp 433-460.

MCCARTHY, J., MINSKY, M., ROCHESTER, N., SHANNON, C. 1995, "A proposal for the Dartmouth Summer Research Project on Artificial Intelligence" August 31,: AI Magazine Volume 27, Number 4, 2006.

PALMA ORTIGOSA, A. 2022 El ciclo de vida de vida de los sistemas de inteligencia artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas de algoritmos. En Cotino Hueso, L., Bauzá M. *Derechos y garantías ante la Inteligencia Artificial y las decisiones automatizadas,* 2022, Aranzadi, 33-78.

PRESNO LINERA, M.A., *Derechos fundamentales e inteligencia artificial,* Ed.Marcial Pons, 2022.

SALAZAR GARCÍA, I. 2022, Retos actuales de la ética en la inteligencia artificial. En Contino Hueso, L., *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas, Aranzadi*. pp.79-101.

SIMÓN CASTELLANO P., *Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?* IDP. Revista de Internet, Derecho y Política, nº 33, 2021.

SORIANO ARNANZ, A., "*Decisiones automatizadas y discriminación: aproximación y propuestas generales*" Revista General de Derecho Administrativo, n.˚ 56, 2021, http://laadministracionaldia.inap.es/noticia.asp?id=1511706. Remite a Athey, S., Catalini, C. y Tucker, C., «The digital privacy paradox: small money, small costs, small talk», MIT Sloan Research Paper No. 5196-17, 2017.

LA EXTRATERRITORIALIDAD DEL NUEVO REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

Alfonso Ortega Giménez
Profesor Titular de Derecho internacional privado
de la Universidad Miguel Hernández de Elche (Alicante)
alfonso.ortega@umh.es

Resumen: *El Reglamento europeo de Inteligencia Artificial, supone la primera regulación jurídica de la Inteligencia Artificial de carácter global, directamente aplicable en todos los Estados miembros de la Unión Europea sin necesidad de normas de transposición, y representa un esfuerzo ambicioso para establecer un equilibrio entre la promoción de la innovación tecnológica y la protección de los ciudadanos y sus derechos. El objeto de la Unión Europea con la propuesta del citado Reglamento es el de buscar una posición de liderazgo en el establecimiento de estándares globales para la gobernanza de la Inteligencia Artificial, destacando su compromiso con una Inteligencia Artificial que sea segura, ética y bajo el control humano.*

Palabras clave: *Inteligencia Artificial; Derecho; Unión Europea; Protección de datos; Reglamento Europeo.*

Abstract: *The European Regulation on Artificial Intelligence is the first global legal regulation of Artificial Intelligence, directly applicable in all EU Member States without the need for transposition rules, and represents an ambitious effort to establish a balance between the promotion of technological innovation and the protection of citizens and their rights. The European Union's aim in proposing this Regulation is to seek a leading position in setting global standards for the governance of Artificial Intelligence, underlining its commitment to Artificial Intelligence that is safe, ethical and under human control.*

Keywords: *Artificial Intelligence; Law; European Union; Data Protection; European Regulation.*

SUMARIO:

I. PLANTEAMIENTO.

El Reglamento europeo de Inteligencia Artificial, (en adelante, Reglamento europeo de IA) supone la primera regulación jurídica de la Inteligencia Artificial (en adelante, IA) de carácter global, directamente aplicable en todos los Estados miembros de la Unión Europea (en lo sucesivo, UE) sin necesidad de normas de transposición. Al mismo tiempo, aspira a tener una eficacia universal, como ya ha sucedido con el Reglamento General de Protección de Datos (a partir de ahora, RGPD), es decir, con repercusión más allá de las fronteras de la UE. Se aplicará a sistemas IA que funcionan como componentes de productos o que son productos en sí mismos, que se pretenden comercializar o poner en servicio en el mercado de la UE y fuera de éste.

Esta nueva norma persigue desarrollar un ecosistema de confianza mediante el establecimiento de un marco jurídico destinado a lograr que la IA sea fiable y respete el Derecho. Se basa en los valores y derechos fundamentales

de la UE que tienen por objeto esencial inspirar confianza a los ciudadanos y otros usuarios para que adopten soluciones basadas en la IA, al tiempo que se trata de animar a las empresas a que desarrollen e inviertan en este tipo de soluciones. La IA debe ser un instrumento para las personas y una fuerza positiva en la sociedad, y su fin último debe ser incrementar el bienestar humano.

La técnica utilizada para la regulación de esta materia está inspirada por el RGPD, caracterizado por cuatro elementos[161]: a) La utilización de un Reglamento en lugar de una Directiva como técnica jurídica[162]; b) El establecimiento de rígidos requisitos y obligaciones para distintas categorías de posiciones para el acceso a la actividad y la prestación de cualquier servicio digital; c) El nombramiento por parte de los Estados Miembros de autoridades nacionales competentes para que las empresas encuentren una vía más directa cuando deseen reclamar por el incumplimiento del Reglamento; y d) El establecimiento de órganos colegiados a nivel europeo, aunque con diferentes papeles en función de cada Reglamento[163].

Se configura el Reglamento europeo de IA como un instrumento jurídico que busca armonizar las normas en este campo y establecer un marco regulatorio confiable, no limitado a sectores concretos, con la finalidad de ofrecer respuestas sujetas, entre otros, al principio de proporcionalidad en función

---

161 *Vid.*, en el mismo sentido, GASCÓN MACÉN, Ana, <<El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea>>, CDT, Vol. 13(2), 2021, págs. 209-232, https://doi.org/10.20318/cdt.2021.6256; PAPAKONSTANTINOU, Vagelis; DE HERT, Paul, <<Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI>>, *European Law Blog*, 1 de abril de 2021, https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa- dma-and-the-eu-regulation-of-ai/.

162 A pesar de que en las propuestas legislativas se les denomine "leyes". *Vid.*, sobre el particular, PAPAKONSTANTINOU, Vagelis; DE HERT, Paul, <<EU lawmaking in the Artificial Intelligent Age: Actification, GDPR mimesis, and regulatory brutality>>, *European Law Blog*, 8 julio 2021, https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr- mimesis-and-regulatory-brutality/.

163 Comité Europeo de Inteligencia Artificial (art. 56 Reglamento europeo de IA), si bien el Parlamento propone cambiar su nombre al de European Artificial Intelligence Office (AI Office) e incrementar considerablemente sus funciones. Otros organismos colegiados previstos en las leyes digitales son: Comité Europeo de Innovación en materia de Datos (art. 29 RGPD), Junta Europea de Servicios Digitales (art. 61 RSD), Grupo de Alto Nivel (art. 40 RMD), que se unen al ya existente Comité Europeo de protección de datos (art. 68 RGPD).

de los riesgos que ocasione la IA. La IA está diseñada para ser utilizada en cualquier sector de la actividad, dando lugar a que las normas reguladoras de los distintos sectores se apliquen en relación con el diseño y desarrollo de IA, por ejemplo, siendo de aplicación la normativa de protección de datos, la normativa sobre secretos empresariales, legislación sobre protección de los consumidores y prácticas comerciales desleales, entre otros[164].

El Reglamento europeo de IA no sólo está diseñado para fomentar la adopción de sistemas de IA en el mercado interior, sino que también tiene la ambición de posicionar a la UE como un líder mundial en el desarrollo de una IA confiable y ética. Este marco legislativo responde a la necesidad de ofrecer, a nivel global, un alto nivel de protección de los intereses públicos, como la salud y la seguridad, mientras se asegura el respeto de los derechos fundamentales.

El artículo 2.1 del Reglamento europeo de IA[165] se convierte en uno de los artículos fundamentales, ya que delinea el ámbito de aplicación de la ley, especificando quiénes estarán sujetos a las nuevas regulaciones; y, por tanto, quiénes deben acatar las obligaciones contenidas en el Reglamento. Los proveedores y usuarios de sistemas de IA, ya sea dentro de la UE o en terceros países, se verán afectados por este Reglamento cuando la información de salida del sistema de IA se utilice en la UE. Esta disposición garantiza que la regulación tenga un alcance transfronterizo, abarcando no solo a los actores dentro de la UE sino también aquellos cuyos sistemas de IA puedan afectar a los ciudadanos de la UE. El carácter de extraterritorialidad de la norma debe ser regulado y analizado con detenimiento debido a las múltiples implicaciones que trae consigo, siendo una de las mayores novedades de esta propuesta.

Uno de los aspectos más destacados del Reglamento europeo de IA es su enfoque tecnológicamente neutral y su intento de ser resistente al tiempo, teniendo en cuenta la rápida evolución de la tecnología y el mercado de la IA. Esto es

---

164 *Vid.* MIGUEL ASENSIO, Pedro Alberto, *Manual de Derecho de las Nuevas Tecnologías*. *Derecho Digital*, Aranzadi, Cizur Menor, Navarra 2023, págs. 121.

165 El artículo 2.1 Reglamento europeo de IA señala: "El presente Reglamento es aplicable a: a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la Unión, con independencia de si dichos proveedores están establecidos en la Unión o en un tercer país; b) los usuarios de sistemas de IA que se encuentren en la Unión; c) los proveedores y usuarios de sistemas de IA que se encuentren en un tercer país, cuando la información de salida generada por el sistema se utilice en la Unión".

fundamental para una regulación duradera y adaptable que pueda mantenerse al día con los avances tecnológicos sin necesidad de cambios frecuentes.

El Reglamento europeo de IA también proporciona una definición clara de los principales actores en la cadena de valor de la IA, tales como proveedores[166], usuarios[167], representantes autorizados[168], importadores[169] y distribuidores[170], así como los fabricantes de productos. Este enfoque detallado es esencial para clarificar las responsabilidades y garantizar una igualdad de condiciones en toda la industria. Por otro lado, los sistemas de IA se encuentran clasificados en función de su capacidad para dañar y poner en peligro la seguridad y los derechos fundamentales de las personas. Por ejemplo, los sistemas de IA calificados como de alto riesgo tienen una mención especial en el Reglamento europeo de IA. Esto indica la importancia de un enfoque específico para los sistemas que pueden tener implicaciones significativas en la seguridad y los derechos de las personas es el caso de aquellos sistemas de IA usados para la gestión del tráfico en la carretera tendrá la calificación de alto riesgo.

El Reglamento europeo de IA representa un esfuerzo ambicioso para establecer un equilibrio entre la promoción de la innovación tecnológica y la protección de los ciudadanos y sus derechos. A medida que la propuesta con-

---

166 Art. 3.2: "toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que desarrolle un sistema de IA o para el que se haya desarrollado un sistema de IA con vistas a introducirlo en el mercado o ponerlo en servicio con su propio nombre o marca comercial, ya sea de manera remunerada o gratuita".

167 Art. 3.4: "toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional". El Parlamento Europeo propone cambiar este término por el de "implementadores" ("deployers" en inglés).

168 Art. 3.5: "toda persona física o jurídica establecida en la Unión que haya recibido el mandato por escrito de un proveedor de un sistema de IA para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor".

169 Art. 3.6: "toda persona física o jurídica establecida en la Unión que introduzca en el mercado o ponga en servicio un sistema de IA que lleve el nombre o la marca comercial de una persona física o jurídica establecida fuera de la Unión".

170 Art. 3.7: "toda persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercializa un sistema de IA en el mercado de la Unión sin influir sobre sus propiedades".

tinúa su camino a través del proceso legislativo, se anticipa que será objeto de debates significativos y, posiblemente, de ajustes. Lo que permanece claro es que la UE busca una posición de liderazgo en el establecimiento de estándares globales para la gobernanza de la IA, destacando su compromiso con una IA que sea segura, ética y bajo el control humano.

II. EL ARTÍCULO

2.1 DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL.

El artículo 2.1 del Reglamento europeo de IA puede ser considerada desde el punto de vista del Derecho Internacional Privado como una norma de derecho aplicable, y concretamente, una norma de conflicto unilateral cuyo objetivo es determinar a qué situaciones de la UE es aplicable el Reglamento europeo de IA. Estas situaciones serán diferentes en función de si se analizan desde la posición de los operadores económicos, de las autoridades nacionales competentes o de los tribunales de justicia[171].

La primera perspectiva de análisis es la de los operadores económicos, es decir, la de los "proveedores", "usuarios", "representantes autorizados", "importadores" y "distribuidores" de "sistemas de inteligencia artificial" (sistemas IA), denominados demanera global en el Reglamento de IA como "operadores". Para estos operadores resulta fundamental, antes de llevar a cabo su actividad económica,saber si el Reglamento les resultará aplicable. En principio, la respuesta podría parecer sencilla: la futura normativa será de aplicación a sistemas IA que funcionan como componentes de productos o que son productos en sí mismos que se pretenden comercializar o poner en servicio en el mercado UE. Esta afirmación puede ser correctaen relación con importadores y distribuidores. No así para proveedores, usuarios y representantes autorizados.Por consiguiente, cualquier sistema IA desarrollados por proveedores o utilizados por usuarios establecidos en terceros Estados resultan accesibles por potenciales clientes ubicados en Europa. ¿Resulta esto suficiente para que el

171 *Vid.* LOPEZ-TARRUELLA MARTÍNEZ, Aurelio, <<El futuro reglamento de Inteligencia Artificial y las relaciones con terceros estados>>, *Revista Electrónica de Estudios Internacionales (REEI)*, núm. 45, 2023, págs. 5-11.

Reglamento europeo de IA resulte aplicable? Atenor de su artículo 2.1, la respuesta debe ser negativa. Esta disposición establece unos criterios de conexión que, en principio, implican que el futuro Reglamento únicamente seva a aplicar a proveedores y usuarios que llevan a cabo actividades que presentan una vinculación estrecha con la UE. Tales criterios están basados en las doctrinas de los "efectos en el mercado" y de las "actividades dirigidas" existentes en otras ramasjurídicas. No obstante, la manera en la que están redactados es defectuosa y pueden conllevar dos consecuencias: inseguridad jurídica de los operadores a los que, en ocasiones, les puede resultar difícil determinar si están obligados a cumplir con los requisitos y obligaciones establecidas en el Reglamento; y aplicación injustificada de la futura normativa a actividades que no presentan suficiente vinculación con la UE[172].

El artículo 2.1 del Reglamento europeo de IA desempeña un papel crucial en determinar los operadores económicos que estarán sujetos a las obligaciones del Reglamento y cómo deben interpretar su aplicación prospectiva. La discusión sobre la aplicación prospectiva es esencial para los operadores económicos, ya que les proporciona la claridad necesaria para planificar y adaptar sus estrategias de negocio en concordancia con los requisitos regulatorios.

En el contexto del Reglamento europeo de IA, los operadores económicos incluyen a los proveedores, usuarios de sistemas de IA representantes autorizados, importadores y distribuidores que operan en el mercado único. El artículo 2.1 especifica que el Reglamento se aplicará a los operadores económicos que pongan en el mercado de la UE o pongan en servicio sistemas de IA. Este enfoque prospectivo significa que los operadores económicos deben, en primer lugar, conocer si el Reglamento les será aplicable y, en caso afirmativo, anticipar cómo las disposiciones reglamentarias impactarán en sus productos de IA aún no comercializados, así como en los servicios que planean ofrecer en el futuro.

Para conocer si incide en su ámbito de aplicación, la disposición establece unos criterios de conexión que van a implicar que el Reglamento se aplique a sistemas de IA desarrollados por proveedores o utilizados por usuarios establecidos en terceros estados. El criterio de conexión será el de la vinculación estrecha con la UE. Los criterios a seguir serán los ya definidos por la doctrina

---

172 *Vid.*, en sentido amplio, LOPEZ-TARRUELLA MARTÍNEZ, Aurelio, "El futuro …", <<cit.>>.

como "efectos en el mercado"[173], y de las "actividades dirigidas" existentes en otras ramas jurídicas.

Estos criterios de conexión plantean consecuencias: la primera de ellas, inseguridad jurídica para los operadores que encontrarán dificultes para determinar si están sujetos a ciertas obligaciones y la segunda, que el reglamento y sus disposiciones se les aplique injustificadamente por no presentar suficientes vínculos con la UE[174], por ejemplo, la aplicación de la legislación europea a empresas establecidas en terceros estados en aquellos supuestos que presentan una mínima vinculación con la UE.

La aplicación del artículo 2.1 del Reglamento europeo de IA por las autoridades nacionales competentes es curiosa; pues contrariamente a lo establecido en el RGDP, el Reglamento europeo de IA no establece un derecho para las personas físicas o jurídicas depresentar una reclamación ante las autoridades nacionales de supervisión por el incumplimiento de las disposiciones del Reglamento por parte de proveedores, usuarios o cualquier otro operador de sistemas IA. Además, esta aplicación lleva consigo la necesidad de establecer un marco de competencia internacional entre dichas autoridades. Este artículo 2.1. del Reglamento europeo de IA establece el ámbito de aplicación material de la normativa, definiendo lo que se entiende por sistemas de IA y estableciendo las bases para su regulación, supervisión y control.

El Reglamento europeo de IA también plantea cuestiones de jurisdicción y aplicación extraterritorial. La UE debe trabajar para garantizar que sus regulaciones sean respetadas más allá de sus fronteras, lo cual es un reto significativo en el espacio digital globalizado. Esto puede requerir acuerdos bilaterales o multilaterales, así como un diálogo constante con otras jurisdicciones para asegurar la cooperación en la supervisión y cumplimiento de estas regulaciones.

El Consejo de Europa y otras organizaciones internacionales de derechos humanos son foros críticos para el diálogo sobre cómo las aplicaciones de IA pueden afectar los derechos humanos. Las regulaciones de la UE pueden in-

---

173 En materia de Derecho de la competencia. Sobre el particular, *Vid.* MONTI, Giorgio, <<The global Reach of EU Competition Law>>, *EU Law Beyond EU Borders: The extraterritorial Reach of EU Law*, Oxford Academic, 2019, págs.174-196.

174 *Vid.* LOPEZ-TARRUELLA MARTÍNEZ, Aurelio, "El futuro …", <<cit.>>, págs. 6.

fluir en la creación de directrices globales para garantizar que la IA se desarrolle de manera que respete la dignidad humana y los derechos fundamentales.

Es fundamental que las regulaciones de la UE consideren el impacto en los países en desarrollo, que pueden carecer de la infraestructura para cumplir con estándares estrictos. La cooperación internacional para el desarrollo y la asistencia técnica serán cruciales para asegurar que la IA sea una herramienta de avance y no una fuente de división.

El Reglamento europeo de IA tiene el potencial de configurar no solo el panorama regulatorio europeo sino también la gobernanza global de la IA. Sin embargo, para que sea efectivo y justo, debe articularse dentro del marco del derecho internacional, respetando los tratados existentes y contribuyendo al desarrollo de nuevos estándares y principios. Esto requiere un esfuerzo concertado para la cooperación internacional, la diplomacia tecnológica y la promoción de un enfoque inclusivo y holístico que abarque todas las regiones y sectores de la sociedad.

La regulación de la Reglamento europeo de IA por parte de la UE introduce desafíos significativos en términos de jurisdicción y alcance territorial. La naturaleza inherentemente global de la IA y su industria asociada exige un escrutinio detallado de cómo la normativa de un territorio puede influir en, o ser implementada por, entidades que operan internacionalmente. La aplicación del artículo 2.1 del Reglamento europeo de IA hace evidente la necesidad de un enfoque holístico y globalizado para la regulación, con un énfasis en la cooperación internacional y la armonización regulatoria.

La preocupación primordial en cuanto a la jurisdicción es el alcance extraterritorial del reglamento. Es decir, la UE debe definir cómo sus normas afectarán a las empresas y entidades fuera de su territorio que producen o proveen sistemas de IA utilizados dentro de la UE. Esto plantea preguntas sobre la soberanía y la aceptación de estas normas por terceros países, y cómo se gestionarán los conflictos de leyes.

La aplicación del art. 2.1 del Reglamento europeo de IA por las autoridades nacionales competentes no solo plantea cuestiones sobre la competencia judicial internacional de autoridades, sino que también enfatiza la necesidad de un diálogo global y la colaboración para desarrollar un enfoque armonizado y equitativo hacia la regulación de la IA. En última instancia, el éxito de la UE en la regulación de la IA no se medirá solo por la eficacia de su legislación

interna, sino también por su capacidad para influir y formar parte de un marco normativo global cohesivo.

Las autoridades nacionales competentes no son meros ejecutores de la legislación de la UE en materia de IA; son participantes activos en el escenario regulatorio global. Al aplicar el art. 2.1 del Reglamento europeo de IA, estas entidades contribuyen a la formación de un paisaje internacional que es más cohesivo, justo y equilibrado. Su papel va más allá de la implementación de políticas, extendiéndose a la influencia de la gobernanza de la IA a nivel mundial, lo cual es crucial para abordar los retos que la tecnología presenta en una sociedad interconectada.

El propio artículo 2.1 del Reglamento europeo de IA señala además que, en ocasiones puede ocurrir que la aplicación del futuro Reglamento se plantee en el marco de una acción civil presentada ante un órgano judicial relativa, por ejemplo, a una responsabilidad extracontractual derivada del funcionamiento defectuoso de un sistema IA, o al incumplimiento de un contrato celebrado entre un proveedor de sistemas IA y un usuario, o a una disputa entre cualquiera de estos y un particular que es parte de un contrato de prestación de servicios en los que se utilizan estos sistemas. En dichos litigios,el incumplimiento de los requisitos u obligaciones establecidos en el Reglamento para las distintas categorías de sistemas IA puede ser invocado como fundamento de la demanda.

Tratándose de litigios en materia civil o mercantil, la competencia judicial internacional del tribunal del Estado miembro ante el que se presente la demanda vendrá determinada por el Reglamento "Bruselas I bis" –siendo competentes los Tribunales del estado donde el presunto perjudicado tenga su residencia habitual, los del lugar de trabajo o donde se produjo la infracción del Reglamento europeo de IA–; y la ley aplicable por el Reglamento "Roma II" – si setrata de un litigio por responsabilidad extracontractual – o el Reglamento "Roma I" – si el litigio es sobre el incumplimiento de un contrato internacional–. Eso sí, el derecho material aplicable será el propio Reglamento europeo de IA, y no podrán aplicar derecho extranjero de un tercer Estado.

III. LA APLICACIÓN EXTRATERRITORIAL DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL.

El objetivo de este amplio ámbito territorial es que la protección que ofrece el Reglamento General de Protección de Datos (en adelante, RGPD)[175] "viaje" con los datos personales allá donde vayan en una sociedad globalizada donde los datos cruzan fronteras con un simple clic. La UE se guía por el razonamiento de que ofrecer protección solo para el procesamiento de datos que tiene lugar dentro de las fronteras europeas no sería suficiente. Esta medida también busca ofrecer igualdad de condiciones para las empresas europeas sin crear una regulación más estricta que supusiera cargas solo para ellas. La aplicación extraterritorial del RGPD significa que cualquier empresa que desee acceder al mercado europeo para ofrecer sus servicios y bienes y tratar datos personales "europeos" en el proceso debe cumplir con estas reglas, aunque tenga su sede en un tercer país[176].

La aplicación extraterritorial de la legislación no es algo nuevo[177], pero sí que se puede ver que está cobrando mucha fuerza en los aspectos relativos a la regulación de Internet[178].

---

175 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE *núm*. 119, de 4 de mayo de 2016).

176 *Vid.* GASCÓN MACÉN, Ana, <<The extraterritorial application of European Union Data Protection Law>>, *Spanish Yearbook of International Law*, Nº 23, 2019, págs. 413-425.

177 *Vid.* DOVER, Robert; Frosini, Justin, *The Extraterritorial Effects of Legislation and Policies in the EU and US* (European Union, Brussels, 2012) [doi: 10.2861/75161]. Según GASCÓN MACÉN a pesar de que la UE nunca ha sido una completa defensora de la extraterritorialidad, comienza a redoblar su ejercicio a través de la extensión territorial, la cual permite controlar aquellas conductas que, aunque se lleven a cabo en el extranjero, repercutan en los intereses generales de la UE. Véase GALLEGO HERNÁNDEZ, Ana Cristina, <<La aplicación de la extensión territorial del Derecho de la Unión Europea>>, *Cuadernos Europeos de Deusto,* n.º 63 (septiembre), 2020, págs. 297-313. https://doi.org/10.18543/ced-63-2020pp297-313.

178 *Vid.* Internet Society, *The Internet and extra-territorial effects of laws,* Internet Society, 2018, pág. 1. Esta organización advierte que muchos Estados están imponiendo reglas

El RGPD ha sido duramente criticado porque, con la cantidad de empresas que se encuadran en estos criterios en todo el mundo, es más fácil para las multinacionales adaptarse a él mientras que es muy costoso para las *pymes*[179]. Además, las autoridades de protección de datos en los Estados miembros tienen recursos limitados, por lo que Svantesson argumenta que, como habrá más empresas extranjeras que no cumplan con el RGPD que recursos para investigarlas, la aplicación real del mismo necesariamente será arbitraria, lo que socavaría la legitimidad de cualquier acción de ejecución que se adopte[180]. Sin embargo, AZZI considera legítima esta aplicación extraterritorial y argumenta que la UE está equipada con las herramientas relevantes para hacer cumplir el RGPD en el exterior, aunque haya que desarrollarlas más[181]. DE HERT y M. CZERNIAWSKI añaden que este enfoque, aunque no sin inconvenientes y desafíos para los intereses estatales y los derechos individuales, resuelve uno de los mayores problemas a los que se enfrentaba hasta entonces la normativa europea de protección de datos, que era la falta de jurisdicción sobre los responsables del procesamiento de datos en terceros países que afectaban a un número considerable de datos de europeos[182].

Los legisladores europeos eran bastante conscientes de que la aplicación extraterritorial de las leyes podía tener impactos indeseables. El propio RGPD en su considerando 115 establece que la aplicación extraterritorial de algunas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho

que se extienden a Internet en otros lugares, obstaculizan la innovación, disuaden la inversión en sus propios países y corren el riesgo de crear nuevas brechas digitales que perjudiquen a sus propios ciudadanos.

179 *Vid.* SCOTT, Mark; CERULUS, Laurens; KAYALI, Laura, <<Six months in, Europe's privacy revolution favors Google, Facebook>>, *Politico.eu*, 23 de noviembre de 2018.

180 *Vid.* SVANTESSON, Dan Jerker B, <<European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments>>, *Journal of Intellectual Property, Information Technology and E-Commerce Law,* vol. 9, nº 2, 2018, págs. 113-125.

181 *Vid.* AZZI, Adèle, <<The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation>>, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 9, nº 2, 2018, págs. 126-137.

182 *Vid.* DE HERT, Paul; CZERNIAWSKI, Michal, <<Expanding the European data protection scope beyond territory: Article 3 of the General Data. Protection Regulation in its wider context>>, *International Data Privacy Law*, vol. 6, nº 3, 2016, págs. 230-243, doi:10.1093/idpl/ipw008.

internacional e impedir la protección de las personas físicas garantizada en la UE en virtud del RGPD; y, por tanto, las transferencias de datos sólo deben hacerse respetando las condiciones del mismo. Así vemos que el RGPD establece su propia aplicación extraterritorial, pero excluye la de las leyes extranjeras en muchos casos. Un conflicto de esta naturaleza puede darse, por ejemplo, cuando las autoridades estadounidenses requieran datos en el marco de una investigación penal a una compañía situada en su territorio pero que sean referentes a un residente de la UE en contra de lo establecido en el RGPD, por lo que la empresa puede encontrarse con obligaciones legales contradictorias.

Los problemas son múltiples y los críticos tienen buenas razones para estar preocupados, pero la dificultad para garantizar la aplicación del RGPD o la falta de recursos para ello no pueden hacer que apuntemos a estándares más bajos de protección de los derechos fundamentales; sobre todo teniendo en cuenta cómo el RGPD ha servido para elevar este nivel de protección no sólo en Europa. Al final la Comisión ha buscado solucionar y regular un problema, definido por la actuación transfronteriza de los intermediarios, que está situado normalmente fuera de las fronteras europeas, pero con un fuerte impacto sobre sus ciudadanos.

Para comprender la naturaleza de la extraterritorialidad en el Reglamento europeo de IA, es esencial analizar los elementos clave que subyacen a su aplicación. El primer elemento es el criterio de "oferta" y "uso". Según el reglamento propuesto, las regulaciones se aplicarán no solo a las entidades que ofrecen servicios de IA en la UE, sino también a aquellas cuyos sistemas de IA se utilizan en la UE, independientemente de si esa entidad está establecida o no en la UE.

El segundo elemento es el principio de "efecto". El principio de efecto implica que, si un sistema de IA tiene un impacto significativo en los individuos o entidades en la UE, entonces la ley se aplicará. Esto se extiende incluso a sistemas desarrollados y operados completamente fuera de la UE, lo que destaca la intención del Reglamento de proteger a sus ciudadanos de riesgos potenciales independientemente de la ubicación de la empresa de IA.

La extraterritorialidad en el Reglamento europeo de IA también se refleja en las obligaciones de las entidades no europeas. Estas empresas deben designar a un representante legal en la UE para asegurarse de que cumplen con la ley y actuar como un punto de contacto con las autoridades regulatorias. Esto es similar a los requisitos establecidos por el RGPD y es fundamental

para asegurar que las entidades no europeas puedan ser sujetas a supervisión y sanciones si no cumplen con los estándares establecidos.

Este enfoque tiene implicaciones significativas para la gobernanza global de la IA. Por un lado, establece un alto estándar que podría inspirar a otras jurisdicciones a seguir su ejemplo, promoviendo una forma de "diplomacia regulatoria". Por otro lado, también plantea preguntas sobre la soberanía y el equilibrio de poder en la regulación de las tecnologías emergentes.

La extraterritorialidad, sin embargo, no está exenta de críticas y preocupaciones. Algunos argumentan que esta podría conducir a conflictos de leyes, donde las empresas se encuentran atrapadas entre regulaciones incompatibles de diferentes jurisdicciones. Además, la carga administrativa y financiera de cumplir con múltiples sistemas regulatorios puede ser onerosa, especialmente para las *startups* y las *pymes*.

Para abordar estas preocupaciones, la UE puede necesitar colaborar con socios internacionales para desarrollar estándares comunes o mecanismos de reconocimiento mutuo que faciliten el cumplimiento transfronterizo. Además, la UE debe considerar los impactos económicos de sus regulaciones extraterritoriales y equilibrar la protección de los consumidores con un entorno propicio para la innovación y el comercio.

La aplicación extraterritorial de la Reglamento europeo de IA sugiere, además, un esfuerzo por parte de la UE para evitar lo que se ha denominado "carrera hacia el fondo" en términos de estándares de regulación de IA. Al promover normativas estrictas de IA, la UE intenta prevenir que las empresas busquen jurisdicciones con regulaciones más laxas para el desarrollo y despliegue de sus sistemas de IA, lo que a largo plazo podría debilitar los derechos de los ciudadanos y la innovación responsable.

La expansión extraterritorial de las normativas de IA representa una ambición por parte de la UE, apoyada por los esfuerzos de España de establecer estándares globales que prioricen los derechos humanos y la ética en el desarrollo tecnológico. El liderazgo europeo en esta área pretende fomentar un diálogo global que culmine en la adopción de prácticas coherentes y éticas en la IA, asegurando así su beneficio y sustentabilidad a largo plazo para la sociedad internacional.

La aplicación extraterritorial de cualquier reglamento representa un desafío jurídico complejo, especialmente en el ámbito del derecho digital y de la IA.

El RGPD establece criterios para su aplicación territorial, los cuales, en ocasiones, pueden conducir a interpretaciones que extienden injustificadamente la jurisdicción de la UE. Estos criterios incluyen la oferta de bienes o servicios a ciudadanos de la UE, independientemente de la realización de un pago, y el monitoreo del comportamiento de los sujetos que se encuentren en la UE.

Un primer supuesto de aplicación extraterritorial injustificada puede surgir cuando una empresa fuera de la UE realiza un tratamiento incidental de datos de ciudadanos europeos. Por ejemplo, un sitio web con base en Asia, cuyo objetivo principal son los consumidores locales, podría quedar inadvertidamente sujeta al RGPD si un ciudadano de la UE visita su página web.

Otro escenario es el de las empresas que utilizan cookies para monitorear el comportamiento de los visitantes de sus sitios web. Si bien este monitoreo es a menudo parte de estrategias de marketing digital, bajo el RGPD, la simple utilización de cookies podría implicar la regulación de dichas prácticas empresariales bajo las leyes europeas.

Además, los criterios relacionados con la oferta de bienes o servicios no distinguen adecuadamente entre actividades dirigidas de manera específica al mercado de la UE y aquellas que no lo están. Esto genera incertidumbre entre los operadores económicos internacionales, que pueden verse sujetos al RGPD por actividades de alcance global no enfocadas directamente en consumidores europeos.

De acuerdo con el art. 2.1 a), el Reglamento europeo de IA resulta aplicable "a los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la Unión, con independencia de si dichos proveedores están establecidos en la Unión o en un tercer país". Se trata de un criterio de conexión informado por la doctrina jurisprudencial de las"actividades dirigidas", utilizado por ejemplo en materia de contratos celebrados por losconsumidores en Internet, o de infracción en línea de títulos unitarios de propiedad industrial. Este criterio garantiza que el Reglamento resulta aplicable en situaciones quepresentan una estrecha vinculación con la Unión.

Alternativamente, el art. 2.1 b) establece la aplicación del Reglamento a "los usuarios de sistemas de IA que se encuentren en la Unión". Este segundo criterio es criticable por dos razones.

Para empezar, la utilización de los términos "se encuentre en la Unión" otorga al Reglamento un ámbito de aplicación extremadamente amplio. La

aplicación resulta injustificada pues la situación presentauna vinculación muy escasa con la Unión. Este problema se solucionaría con una modificación de la disposición que limite su aplicación a usuarios establecidos o con residencia habitual en la UE.

Efectivamente, el Reglamento europeo de IA no resulta aplicable a proveedores establecidos en la Unión Europea que comercializan sus sistemas IA exclusivamente en terceros Estados; en cambio, si resulta aplicable a usuarios establecidos en la Unión que prestan sus serviciosen terceros Estados. La diferencia de trato resulta injustificada. En ambos casos la vinculación con la Unión Europea es la misma. Si la intención es que los usuarios europeos de sistemas IA respeten los estándares previstos en el Reglamento con independencia del país en el que ofrezcan sus servicios, los proveedores establecidos en la Unión Europea que comercialicen sistemas IA en terceros Estados también deberían cumplir con esos estándares.

Alternativamente, se podría defender una modificación del art. 2.1 b) para que elReglamento únicamente fuera aplicable a usuarios de sistemas IA cuando la informaciónde salida generada por el sistema se utilice en la Unión, independientemente de si tienensu residencia habitual o establecimiento en territorio europeo o no.

Y, finalmente, en atención al art. 2.1 c), el Reglamento también resulta aplicable "a los proveedores y usuarios de sistemas de IA que se encuentren en un tercer país, cuando la información de salida generada por el sistema se utilice en la Unión". Se trata de un criterio que puede conllevar una aplicación extraterritorial injustificada del Reglamento;y que éste resulte aplicable en situaciones difícilmente previsibles para proveedores de sistemas IA establecidos en terceros Estados[183].

183 *Vid.* LOPEZ-TARRUELLA MARTÍNEZ, Aurelio, "El futuro …", <<cit.>>, págs.14-17.

IV. LA APLICACIÓN EXTRATERRITORIAL DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y SU INFLUENCIA EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL.

La aplicación extraterritorial de RGPD y su influencia en el Reglamento europeo de IA marca un precedente significativo en cómo la legislación europea puede impactar globalmente la regulación de tecnologías emergentes. Este enfoque extraterritorial refleja la ambición de la UE de establecer estándares internacionales en la protección de datos y la ética de la IA, influenciando así la conducta de empresas y gobiernos más allá de sus fronteras.

La naturaleza pionera del RGPD de la UE en términos de su alcance extraterritorial no puede ser subestimada. Desde su implementación en mayo de 2018, el RGPD ha servido como un faro global, iluminando el camino hacia una mayor protección de datos personales más allá de las fronteras nacionales. En su artículo 3, el RGPD establece claramente que su jurisdicción no se limita geográficamente a la UE, sino que se extiende a cualquier entidad que procese los datos de sujetos de la UE, independientemente de dónde se encuentre esta entidad. Este enfoque progresista es el primero de su tipo en privacidad de datos y regulaciones de protección a nivel global.

El impacto de la disposición extraterritorial del RGPD ha sido profundo y multifacético. Ha obligado a empresas de todo el mundo, grandes y pequeñas, a examinar y, en muchos casos, a reestructurar sus políticas y prácticas de manejo de datos para garantizar el cumplimiento. Las multas por incumplimiento son considerables, alcanzando hasta el 4% del volumen de negocios global anual o 20 millones de euros, lo que es más alto, creando así un poderoso incentivo para que las empresas fuera de la UE respeten las regulaciones europeas.

Los principios fundamentales del RGPD, como la transparencia, el consentimiento del sujeto de los datos y el derecho al olvido, han establecido un nuevo estándar global. La necesidad de que las empresas obtengan un consentimiento claro y afirmativo antes de procesar los datos personales ha cambiado la naturaleza del marketing digital y la gestión de la privacidad en línea. Además, el derecho al olvido permite a los individuos solicitar la eliminación

de sus datos personales, lo que ha llevado a una reevaluación global de cómo se almacenan y se mantienen los datos personales[184].

Este liderazgo europeo en la protección de datos ha impulsado a otros países a seguir su ejemplo. Por ejemplo, naciones como Brasil con su *Lei Geral de Proteção de Dados*, o Japón y Corea del Sur han implementado o están en el proceso de fortalecer sus propias leyes de protección de datos alineándose con los estándares establecidos por el RGPD. Esta ola de cambio global subraya la influencia significativa que el RGPD tiene en la configuración de las leyes de protección de datos en todo el mundo, promoviendo un enfoque más coherente y armonizado en la protección de la privacidad.

La influencia extraterritorial del RGPD también ha tenido implicaciones significativas para el comercio internacional y las operaciones empresariales transfronterizas. Las empresas fuera de la UE deben ahora considerar las implicaciones del RGPD en sus estrategias de expansión y entrada en mercados europeos. Las implicaciones van desde la designación de representantes en la UE hasta la realización de evaluaciones de impacto de protección de datos y la adopción de medidas técnicas y organizativas para asegurar el cumplimiento.

La aplicación extraterritorial ha claramente inspirado la propuesta de IA, porque ésta según su artículo 2.1 se aplicará a los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la UE, con independencia de si dichos proveedores están establecidos en la UE o en un tercer país; los usuarios de sistemas de IA que se encuentren en la UE; y los proveedores y usuarios de sistemas de IA que se encuentren en un tercer país, cuando la información de salida generada por el sistema se utilice en la UE. Es decir, que la aplicación a los proveedores se desgaja totalmente de la cuestión de dónde estén situados, lo importante es que introduzcan sus sistemas en la UE, o incluso que sin hacerlo los resultados de esos sistemas se usen en la UE.

La justificación de su aplicación extraterritorial parece clara, proteger los derechos fundamentales de los ciudadanos europeos en el mercado de la UE, independientemente del país de origen del proveedor o usuario. El resultado sería distinto y perjudicial si el Reglamento europeo de IA solamente fuera aplicable cuando se encontrasen establecidos en la UE. Como segundo moti-

184 *Vid*., en sentido amplio, GONZÁLEZ FUSTER, Gloria, *The emergence of personal data protection as a fundamental right of the EU*. Springer Science & Business Media, 2014.

vo, se garantiza la igualdad de condiciones a todos los competidores del libre mercado. Los requisitos y obligaciones para comercializar los sistemas IA son bastante rígidos, por ello, si solo fueran exigibles a empresas de estados miembros, aquellas empresas situadas en terceros estados se encontrarían en situaciones de ventaja competitiva. Así, también se evita el riesgo de que empresas de servicios tecnológicas situadas en Europa, se desplacen a terceros estados por sus legislaciones más laxas en esta materia[185]. Sin embargo, es necesario reforzar los criterios de conexión para que sean suficientemente claros y no generen inseguridad jurídica.

La influencia del RGPD en la regulación de la IA es un fenómeno que no se limita a los aspectos técnicos de la protección de datos, sino que también abarca la ética, la transparencia y la responsabilidad en el uso de algoritmos de IA. A medida que la IA se integra en más aspectos de la vida cotidiana, el enfoque del RGPD en la protección de la privacidad y en el manejo de datos personales se convierte en una base fundamental para el desarrollo de regulaciones específicas de IA.

La influencia del RGPD en la regulación de la IA se manifiesta principalmente en la exigencia de transparencia y aplicabilidad. Los sistemas de IA, especialmente aquellos que se basan en aprendizaje automático y redes neuronales, pueden ser opacos, haciendo difícil entender cómo toman decisiones o llegan a conclusiones. Esto entra en conflicto con los principios del RGPD, que establecen que los individuos tienen derecho a entender cómo se procesan sus datos. En respuesta, los reguladores y los diseñadores de sistemas de IA están trabajando en el desarrollo de técnicas de "IA explicable" que permitan desglosar y presentar de manera comprensible los procesos de toma de decisiones automatizados.

Además, el principio de minimización de datos del RGPD, que estipula que solo se deben recoger los datos estrictamente necesarios para el propósito específico para el que se procesan, también impulsa a los desarrolladores de IA a considerar cuidadosamente qué datos son realmente necesarios para

---

185 *Vid.* BOMHARD, D.; MERKLE, M., <<Regulation of Artificial Intelligence>>, *Journal of European Consumer and Market Law*, vol. 10, Issue 6, 2021, págs. 257-261, https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/10.6/Eu

Ebers, M. et al., pág. 583.

entrenar sus algoritmos. Esto puede conducir a un diseño más consciente y limitado de sistemas de IA que respeten la privacidad por diseño, un concepto que está en el corazón del RGPD.

La necesidad de responsabilidad en el uso de la IA también es un legado del RGPD. La regulación exige que las entidades sean capaces de demostrar cumplimiento con sus principios, lo que incluye mantener registros detallados de procesamiento de datos, realizar evaluaciones de impacto en la protección de datos y tener en cuenta la protección de datos desde la fase de diseño de cualquier producto o servicio. Esto se traduce en una cultura de responsabilidad que es esencial en el ámbito de la IA, donde las decisiones algorítmicas pueden tener grandes impactos en la vida de las personas.

La protección contra decisiones automatizadas es otro punto donde el RGPD ha influido en la regulación de IA. Los individuos tienen el derecho a no estar sujetos a decisiones basadas únicamente en el procesamiento automático, incluyendo la elaboración de perfiles, que produzcan efectos legales sobre ellos o les afecten significativamente. Este derecho impacta directamente en cómo se diseñan y despliegan los sistemas de IA, asegurando que haya siempre una opción para la intervención humana.

En conclusión, la influencia del RGPD en la regulación de la IA es profunda y multifacética. El RGPD ha establecido estándares altos para la protección de datos y la privacidad, que ahora están siendo incorporados en el desarrollo y la regulación de sistemas de IA. A medida que la tecnología avanza, es probable que los principios del RGPD continúen guiando cómo la sociedad y los legisladores abordan los desafíos planteados por la IA.

El impacto extraterritorial del Reglamento europeo de IA representa un notable cambio en la forma en que la legislación puede influir en la conducta corporativa y las políticas gubernamentales a nivel global. Al igual que el RGPD, el cual ha sentado un precedente global en cuanto a la protección de datos, el Reglamento europeo de IA busca imponer un marco ético y seguro para el desarrollo y la utilización de la IA, independientemente de la localización geográfica de las empresas o los datos.

Esta extensión de la jurisdicción más allá de sus propias fronteras es una clara indicación de que la UE está tratando de establecer un estándar de oro en la regulación de la IA, promoviendo así una especie de "efecto Bruselas" – entendido como la tendencia de las leyes de la UE a ser adoptadas o a influir

en la legislación de otros países debido a su rigor y su extenso alcance– que puede influir en la normativa a nivel mundial.

Este alcance global es significativo para la gobernanza de la IA, ya que requiere que las empresas no solo estén atentas a las regulaciones locales, sino que también consideren los requisitos regulatorios internacionales. Esto puede llevar a la adopción de prácticas de IA más éticas y transparentes a nivel mundial, ya que las empresas buscan garantizar la compatibilidad con el Reglamento europeo de IA para mantener su competitividad en un mercado importante. Además, el Reglamento europeo de IA tiene el potencial de influir en la formación de normas internacionales al ser un referente en discusiones globales sobre el tema. Organizaciones internacionales y foros de políticas públicas pueden mirar hacia el Reglamento europeo de IA al desarrollar estándares o al recomendar prácticas para la gobernanza de la IA.

En un mundo cada vez más interconectado, donde los sistemas de IA pueden ser desarrollados en un país, entrenados con datos de múltiples jurisdicciones y desplegados en todo el mundo, la claridad y la coherencia en la regulación son esenciales. En este sentido, la UE está liderando el camino al abordar estos desafíos a través de un enfoque regulatorio que tiene en cuenta no solo el impacto local sino también las implicaciones globales.

Con estos pasos, la UE está modelando no solo su propio ecosistema digital sino también estableciendo un marco que podría estandarizar las expectativas y los requerimientos para la IA en todo el mundo, demostrando así el poder de la regulación extraterritorial en la era digital.

La aplicación extraterritorial de legislaciones como el RGPD plantea una serie de desafíos significativos que van desde aspectos jurídicos hasta operativos. La complejidad aumenta cuando se consideran los diferentes enfoques a la privacidad y protección de datos que existen a nivel mundial.

En primer lugar, el desafío jurídico es uno de los más evidentes. La noción de que una ley europea tenga efectos más allá de sus fronteras puede ser vista como una extralimitación de la jurisdicción por parte de otros países o regiones. Esto podría generar conflictos de leyes cuando las empresas internacionales se ven obligadas a navegar entre regulaciones potencialmente contradictorias. Por ejemplo, una empresa estadounidense puede enfrentarse a requerimientos incompatibles entre el RGPD y las leyes locales de privacidad o vigilancia de Estados Unidos.

Otro aspecto desafiante es el cumplimiento operativo. Las empresas fuera de la UE, especialmente las *pymes*, que no tienen los mismos recursos que las grandes corporaciones, pueden tener dificultades para entender y adaptarse a los requisitos del RGPD. Obligaciones como, por ejemplo, realizar evaluaciones de impacto sobre la protección de datos, designar un representante en la UE o gestionar solicitudes de derecho al olvido, requieren no solo una comprensión profunda de la ley, sino también la implementación de procesos internos que puedan ser onerosos.

La vigilancia y la aplicación también presentan obstáculos. Aunque el RGPD permite imponer multas elevadas, la capacidad real para hacer cumplir estas sanciones en jurisdicciones fuera de la UE es limitada. Las autoridades de protección de datos de la UE deben confiar en la cooperación de sus contrapartes extranjeras o en mecanismos internacionales de resolución de disputas, lo cual no siempre es rápido ni eficiente.

La necesidad de equilibrar la protección de datos con otros derechos y libertades también es un desafío. Por ejemplo, el derecho a la libertad de expresión y la regulación de datos pueden entrar en conflicto, como se ha visto en casos que involucran el derecho al olvido en el contexto de resultados de búsqueda en internet. Encontrar un equilibrio entre los distintos derechos requiere un delicado acto de malabarismo jurídico que puede variar considerablemente entre jurisdicciones.

Por último, está el desafío de la constante evolución tecnológica. Las leyes deben adaptarse a las nuevas tecnologías y prácticas de procesamiento de datos, lo que puede ser un proceso lento. Esto significa que incluso cuando las empresas logran cumplir con el RGPD, deben mantenerse al día con los cambios tanto en la tecnología como en la interpretación legal del reglamento para mantener ese cumplimiento.

En resumen, mientras que el RGPD ha sido pionero en establecer la norma de la extraterritorialidad en la protección de datos, su aplicación efectiva más allá de las fronteras de la UE enfrenta múltiples desafíos. Abordar estos desafíos requiere un enfoque colaborativo internacional y una consideración constante de cómo se pueden alinear las leyes de protección de datos con otras jurisdicciones y con la evolución tecnológica.

La cooperación internacional en la era de la IA es esencial para crear un ambiente de entendimiento mutuo y estándares compartidos que puedan be-

neficiar a todas las partes involucradas. Con el avance de la tecnología, las fronteras se vuelven cada vez más permeables, lo que hace que la colaboración transfronteriza sea más significativa que nunca.

El Reglamento europeo de IA establece un marco que no sólo afecta a las entidades dentro de sus fronteras, sino que también invita a un diálogo global para establecer principios comunes de ética y seguridad en la IA. Esto tiene implicaciones importantes para la forma en que los países pueden colaborar en el desarrollo y la gobernanza de la IA. La UE, a través de este reglamento, fomenta la creación de alianzas internacionales para garantizar que las tecnologías de IA sean seguras, transparentes y responsables, independientemente de su origen.

El intercambio de conocimientos y prácticas entre reguladores de todo el mundo es un aspecto crucial de esta cooperación[186]. Esto podría incluir el intercambio de información sobre las mejores prácticas regulatorias, así como colaboraciones en investigaciones que aborden los desafíos únicos que presenta la IA. Los foros internacionales, como las Naciones Unidas o el G7/G20, ya están comenzando a prestar atención a estas cuestiones, y la UE se posiciona como un líder en estas conversaciones, proponiendo modelos y prácticas que pueden adaptarse y adoptarse globalmente.

Una colaboración efectiva también puede facilitar la armonización de los estándares de IA, lo que es fundamental para las empresas que operan en múltiples jurisdicciones. Con una mayor armonización, las barreras al comercio y a la innovación pueden reducirse, permitiendo que los avances en IA se compartan y se apliquen más ampliamente.

La cooperación internacional en materia de IA también puede ayudar a abordar desafíos conjuntos, como la lucha contra la discriminación y la salvaguarda de los derechos humanos. La IA tiene el potencial de exacerbar las desigualdades y perpetuar los prejuicios si no se gestiona adecuadamente. A través de la cooperación internacional, las naciones pueden trabajar juntas para establecer normativas que prioricen la equidad y la inclusión en los sistemas de IA.

---

186 *Vid*. RENDA, Andrea, <<Artificial Intelligence: Ethics, governance and policy challenges>>, *Report of a CEPS Task Force*, Centre for European Policy Studies, 2019.

Además, los países pueden colaborar en el desarrollo de capacidades y la educación para asegurar que las futuras generaciones estén equipadas para participar en la economía de la IA. Esto incluye no sólo el desarrollo de habilidades técnicas, sino también la comprensión ética y social necesaria para implementar la IA de manera responsable.

Finalmente, la cooperación internacional en materia de IA puede mejorar la preparación ante emergencias y la capacidad de respuesta a desastres. La IA puede ser crucial en la predicción de desastres naturales o en la coordinación de respuestas a emergencias globales. Una colaboración estrecha puede asegurar que los beneficios de la IA se utilicen para proteger a las poblaciones y para mitigar los riesgos de manera efectiva y oportuna.

V. BIBLIOGRAFÍA CONSULTADA.

AZZI, Adèle, <<The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation>>, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018.

DE HERT, Paul; CZERNIAWSKI, Michal, <<Expanding the European data protection scope beyond territory: Article 3 of the General Data. Protection Regulation in its wider context>>, *International Data Privacy Law*, 2016.

DOVER, Robert; Frosini, Justin, *The Extraterritorial Effects of Legislation and Policies in the EU and US,* European Union, Brussels, 2012.

GALLEGO HERNÁNDEZ, Ana Cristina, <<La aplicación de la extensión territorial del Derecho de la Unión Europea>>, *Cuadernos Europeos de Deusto,* n.º 63 (septiembre), 2020.

GASCÓN MACÉN, Ana, <<El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea>>, CDT, 2021

LOPEZ-TARRUELLA MARTÍNEZ, Aurelio, <<El futuro reglamento de Inteligencia Artificial y las relaciones con terceros estados>>, *Revista Electrónica de Estudios Internacionales (REEI)*, 2023.

MIGUEL ASENSIO, Pedro Alberto, *Manual de Derecho de las Nuevas Tecnologías. Derecho Digital*, Aranzadi, Cizur Menor, Navarra, 2023.

MONTI, Giorgio, <<The global Reach of EU Competition Law>>, *EU Law Beyond EU Borders: The extraterritorial Reach of EU Law*, Oxford Academic, 2019.

PAPAKONSTANTINOU, Vagelis; DE HERT, Paul, <<EU lawmaking in the Artificial Intelligent Age: Actification, GDPR mimesis, and regulatory brutality>>, *European Law Blog*, 2021.

PAPAKONSTANTINOU, Vagelis; DE HERT, Paul, <<Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI>>, *European Law Blog*, 2021.

SVANTESSON, Dan Jerker B, <<European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments>>, *Journal of Intellectual Property, Information Technology and E-Commerce Law,* 2018.

SCOTT, Mark; CERULUS, Laurens; KAYALI, Laura, <<Six months in, Europe's privacy revolution favors Google, Facebook>>, *Politico.eu*, 2018.

IV. SECCIÓN DE ESTUDIOS DIVULGATIVOS

INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD PENAL

Dr. José Neftalí Nicolás García
Profesor Derecho Penal Universidad de Murcia

Resumen: *En este artículo se analizará la inteligencia artificial, su posible relación con el derecho penal y se abordará el tema de si los robots o máquinas pueden llegar a considerarse sujetos del derecho penal y, en su caso, si las personas (físicas o jurídicas) podrían ser responsable penalmente por los actos realizados por robots o máquinas que utilicen inteligencia artificial.*

Palabras clave: *Inteligencia Artificial, Derecho Penal, Responsabilidad Penal.*

I. INTRODUCCIÓN

Hoy en día es indiscutible que la inteligencia artificial es una realidad, está presente en nuestra vida cotidiana y que ha llegado para quedarse. También es incuestionable que la inteligencia artificial está produciendo innumerables ventajas en el conjunto de la sociedad, aunque su uso indiscriminado conlleva riesgos que pueden afectar directamente bienes jurídicos protegidos por el derecho penal e incluso a los derechos fundamentales de las personas.[187]

En el sector legal, la implementación de la inteligencia artificial generativa ha supuesto grandes ventajas, permitiendo la automatización de la creación y revisión de documentos legales, la predicción de resultados judiciales basada en la jurisprudencia previa, y ha proporcionado herramientas para la toma de decisiones estratégicas en los diferentes asuntos legales. Además, ha facilitado la personalización de los servicios profesionales, permitiendo a los profesionales del derecho ofrecer soluciones más afinadas y basadas en datos a sus clientes.

Sin embargo, nos encontramos en un punto en el que el propio destino y el progreso de la sociedad humana puede verse comprometido por sus propias decisiones, en lo que a inteligencia artificial se refiere. Decisiones que hasta ahora eran tomadas por humanos están siendo tomadas por sistemas inteligentes y eso puede afectar a una o a muchas personas, empresas, administraciones públicas, etc... Y ni las decisiones humanas son perfectas ni, de manera consecuente, las artificiales o algorítmicas lo son. Por ello, debe asegurarse la máxima legitimidad, licitud, objetividad, ética, seguridad, respeto, justicia y transparencia de estas, del mismo modo en el que pretendemos que lo sean las humanas.

Las decisiones y conductas mediante sistemas inteligentes pueden causar daños a los sujetos afectados por las mismas y afectar a bienes jurídicos protegidos por el derecho penal, lo que genera inevitablemente la necesaria reflexión sobre el régimen de responsabilidad aplicable en tales supuestos y si los marcos vigentes, hasta que dispongamos de otros, son suficientes para dar una respuesta adecuada a los daños causados por estos sistemas en los diferentes

187 Esther Sánchez A.T. (2023). *El desafío de la Inteligencia Artificial a la vigencia de los derechos fundamentales*. Cuadernos Electrónicos De Filosofía Del Derecho. Valencia.

contextos que se pueden plantear, así como para garantizar el derecho a un resarcimiento efectivo a las personas afectadas.[188]

La necesidad de adecuación de la legislación actual para dar respuestas a los distintos supuestos que se pueden plantear en materia de responsabilidad requiere urgente revisión, lo cual nos lleva a nombrar que el hecho de que la Unión Europea está liderando los esfuerzos para consensuar determinados principios y normas éticas de la inteligencia artificial, siendo pionera en la regulación, elaborando propuestas en diferentes ámbitos y sirviendo así de referente al resto de países.

2. INTELIGENCIA ARTIFICIAL Y SUJETOS RESPONSABLES

Uno de los grandes retos que nos propone la inteligencia artificial es en relación con la responsabilidad sobre los daños causados por su funcionamiento y perjuicio a los derechos de las personas. La responsabilidad derivada de la vinculación con la IA es una exigencia jurídica y eso es algo indudable.

Partiendo del Informe del Comité de Asuntos Legales del Parlamento Europeo, de 27 de enero de 2017, sobre las cuestiones jurídicas vinculadas a la robótica y la inteligencia artificial en la Unión Europea, se puede afirmar que en cualquier ámbito de la vida diaria, incluido el ámbito judicial, cada vez más se utiliza la tecnología, lo que supone un riesgo para la sociedad. Por ello, es importante hacer referencia a los bienes jurídicos que hay que proteger frente a esos riesgos y amenazas por el avance de la inteligencia artificial. La vida, la salud, la integridad física y moral, así como los derechos, personalísimos o no, de las personas se pueden ver vulnerados.

En este sentido, debemos tener en cuenta lo que declara la Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales:

188 Muñoz Vela, J. M. (2021). *La inteligencia artificial: Un enfoque global de responsabilidad desde la ética, la seguridad y las nuevas propuestas reguladoras europeas.* Tesis doctoral. Universidad de Valencia.

"…la IA ha experimentado un gran avance en los últimos años, convirtiéndola en una de las tecnologías estratégicas del siglo XXI, que puede generar considerables beneficios en términos de eficiencia, precisión y adecuación y que, por consiguiente, aporta una transformación positiva a la economía y la sociedad europeas, pero también enormes riesgos para los derechos fundamentales y las democracias basadas en el Estado de Derecho.."

Por ello, lo que primero vamos a plantear es si realmente es posible que exista alguna relación entre dicha inteligencia y el derecho penal, de tal forma que pueda ser posible que aquella cometa un hecho que la ley señala como delito. Si bien es verdad que la inteligencia artificial, al ser la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano, supone que hasta cierto punto tenga una forma de pensar autónoma, distinta e independiente de la del ser humano, para poder plantearnos si, por acción u omisión, realmente pueden tener relación directa con el derecho penal (de modo que sí se pueda cometer un hecho que la ley señala como delito), debe descubrirse si es posible que una máquina que utilice inteligencia artificial pueda actuar de forma dolosa o culposa, cumpliendo así con el elemento de tipicidad subjetiva, así como que pueda desarrollar, hasta cierto punto, una capacidad de culpabilidad, pues entonces se deberá establecer de qué forma debe aplicarse la teoría del delito en supuestos donde las máquinas o robots que utilicen inteligencia artificial se involucren en un hecho delictivo.[189]

Con base en lo anterior y suponiendo que una máquina que utilice inteligencia artificial cometa un hecho que la ley señala como delito, ¿la máquina debe ser considerada responsable directa, o solo se le tendrá como instrumento del delito? En este último caso, ¿será conveniente que se incluya en el artículo 22 del Código Penal una agravante aplicable a aquellos que utilicen máquinas que usen la inteligencia artificial para la comisión de un hecho delictivo?

En mi opinión, depende de la intención con la que se crea la máquina que utiliza inteligencia artificial y la capacidad de la persona para limitar la misma. Es decir, si la máquina se crea y se programa con la finalidad de cometer un delito, podría considerarse un instrumento para ello, acogiéndose así la teoría de la autoría mediata; sin embargo, si la comisión del delito se realiza a partir

189 Martínez Hernández, D.F. (2001) *Inteligencia Artificial, Derecho y Compliance.* Revista Mexicana de Ciencias Penales. P 68.

del pensamiento previo de la máquina y al final decide, de forma autónoma, realizar una determinada conducta y, como resultado, comete un delito, se podría considerar que sí sería responsable penalmente, aunque fuera por dolo eventual excluyendo el dolo directo, liberando de cualquier tipo de responsabilidad penal al programador o a la persona física o jurídica que se ocupe de ella, a menos que dicha persona pudiera limitar los actos que pueda realizar de la máquina. No obstante, la persona física o jurídica que creó la máquina que utiliza inteligencia artificial, en este caso podría ser responsable civil subsidiaria, en cuyo caso la legislación se deberá basar en las Normas de Derecho Civil sobre Robótica de la Unión Europea. [190]

Quizá, una posible solución sería considerar a aquellos que utilicen la inteligencia artificial como una persona jurídica, conforme al artículo 31 bis del Código Penal, y aplicarles la doctrina del Tribunal Supremo sobre la responsabilidad penal de las personas jurídicas, a saber:[191]

a) es exigible un juicio de culpabilidad específico sobre la actuación de la persona jurídica, basado en el principio de autorresponsabilidad

b) el fundamento de la responsabilidad penal no es objetiva, sino que ha de tener su soporte en la propia conducta de la persona jurídica.

c) el principio de presunción de inocencia se aplica a la persona jurídica y es autónomo respecto del de la persona física.

d) la persona jurídica actúa sin disponer un sistema de control de sus administradores y empleados dirigidos a controlar la observancia de la norma, del ordenamiento jurídico o no controla las fuentes de peligro de la actividad a la que se dedica.

Actualmente, puesto que la inteligencia artificial no puede ser considerada como un sujeto de derecho, ni tiene reconocida personalidad jurídica, la responsabilidad penal por los delitos cometidos mediante el uso de esta tecnología, recae en los sujetos que utilizan la inteligencia artificial o la programan para delinquir.

Por último, se hará referencia a un catálogo de delitos que pueden ser cometidos con la inteligencia: delitos de estafa cometidos a través de medios in-

190 Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica.

191 STS 234/2019, de 8 de mayo.

formáticos, delitos relativos al mercado y consumidores, delitos de pornografía infantil, delitos de descubrimiento y revelación de secretos, delitos de daños informáticos, delitos de odio y discriminación llevados a cabo por medio de internet o de las tecnologías de la información, delitos de falsedades, acoso, usurpación de identidad, etc…

3. CONCLUSIONES

La inteligencia artificial avanza a un ritmo acelerado y exponencial generando grandes transformaciones en nuestro entorno y riesgos para los derechos de las personas, los cuales se pueden ver vulnerados.

El derecho vigente no regula la inteligencia artificial ni permite proporcionar respuestas adecuadas a los distintos retos que plantea. Los marcos reguladores de la responsabilidad en España y la UE no pueden proporcionar soluciones a la totalidad de contextos y situaciones que se pueden plantear en relación con daños ocasionados por el funcionamiento o uso de sistemas inteligentes.

La relación que pudiera existir entre el derecho penal y la inteligencia artificial es un tema complejo. Actualmente, puesto que la inteligencia artificial no puede ser considerada como un sujeto de derecho, ni tiene reconocida personalidad jurídica, la responsabilidad penal por los delitos cometidos mediante el uso de esta tecnología, recae en los sujetos que utilizan la inteligencia artificial o la programan para delinquir.

Quizá, una posible solución sería considerar a aquellos que utilicen la inteligencia artificial como una persona jurídica y aplicarles la doctrina del Tribunal Supremo sobre la responsabilidad penal de las personas jurídicas.

Por todo ello es necesario legislar sobre materia. En particular, unas normas éticas deben presidir la programación de la inteligencia artificial y situar al ser humano en el centro de su programación. Y también establecer unas causas tasadas que permitan solicitar judicialmente el apagado de la inteligencia artificial para aquellos casos que no funcione correctamente y puedan vulnerar los derechos de las personas, especialmente cuando pueda atentar contra bienes jurídicos tutelados por el derecho penal.

BIBLIOGRAFÍA Y JURISPRUDENCIA.

Esther Sánchez A.T. (2023). *El desafío de la Inteligencia Artificial a la vigencia de los derechos fundamentales*. Cuadernos Electrónicos De Filosofía Del Derecho. Valencia.

Martínez Hernández, D.F. (2001) Inteligencia Artificial, Derecho y Compliance. Revista Mexicana de Ciencias Penales. P 68.

Muñoz Vela, J. M. (2021). *La inteligencia artificial: Un enfoque global de responsabilidad desde la ética, la seguridad y las nuevas propuestas reguladoras europeas*. Tesis doctoral. Universidad de Valencia.

Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica.

STS 234/2019, de 8 de mayo.

Zamorano Ballesteros. R (2023) *Culpable la IA*. Disponible en https://www.abogacia.es/actualidad/opinion-y-analisis/culpable-la-ia/#:~:text=La%20Inteligencia%20Artificial%20no%20es,que%20la%20programaran%20para%20delinquir. Fecha de consulta: 21 de junio de 2024

LA INTELIGENCIA ARTIFICIAL NECESITA DATOS DE CALIDAD Y SEGUROS.

Julián Lozano Carrillo

Asociado principal penalista del departamento de Resolución de conflictos de Garrigues

Mientras caminaba este verano por los valles de Sapa, en Vietnam, contemplando la flora tan diversa de la zona, utilicé una conocida aplicación móvil que, al fotografiar un objeto, ofrece diferente información sobre el mismo.

En un primer escaneado de una flor -un tipo de rosa relativamente común-, dicha aplicación me ofreció el nombre exacto de la fotografiada, la especie concreta a la que pertenecía, el tipo de flor que era y multitud de información adicional de otros tipos de variedades de flores similares e, incluso, algunas sugerencias de compra. Sin embargo, al fotografiar otra flor mucho menos habitual, la aplicación me mostró información de especies que en nada se parecían a la fotografiada y cuyo único elemento en común era el color.

¿Por qué la aplicación ofrecía este resultado tan distinto en uno y otro caso? La respuesta está en los famosos "datos". En el primer supuesto, el de la rosa, el sistema contaba con una importante fuente de datos previamente conocidos por la aplicación, que habían servido para ayudar a la identificación de la flor, mientras que, en el supuesto de la especie menos conocida, el sistema no tenía suficientes datos y no era capaz de ofrecer una respuesta óptima.

Este es un sencillo ejemplo de cómo lo que conocemos como "inteligencia artificial" (IA) necesita datos para alimentar sus sistemas y ofrecernos un resultado a la altura de las elevadas expectativas que tenemos de dicha tecnología: poco menos que ayudarnos a convertirnos en "super humanos" gracias a su uso.

Y es que, como breve recordatorio para los lectores tras las diferentes actividades formativas de la Fundación Ruiz-Funes del año 2024 en materia de **inteligencia artificial**, esta se basa en una **combinación de técnicas** como el aprendizaje automático (machine learning), las redes neuronales, la lógica difusa, la optimización y la inteligencia computacional, mediante las cuales, y con el uso de algoritmos, es capaz de realizar tareas que normalmente requieren inteligencia humana, como puede ser el reconocimiento de voz e imágenes, comprensión del lenguaje natural, aprendizaje, razonamiento, planificación, adaptación, toma de decisiones, resolución de problemas, manipulación de objetos, traducción prácticamente simultánea, etc.

LA INTELIGENCIA ARTIFICIAL GENERATIVA NECESITA DATOS DE CALIDAD Y SEGUROS.

Dentro de la inteligencia artificial, la rama que más interés despierta en nuestro sector jurídico es la conocida como **"inteligencia artificial generativa",** que permite la creación de modelos para generar contenido original y creativo (por ejemplo, texto, siendo especialmente conocido ChatGPT; imágenes, como pueden ser Dall-E o Midjourney; o video, como es el caso de Gen-1 o Sora). Estos modelos utilizan un conjunto de datos (dataset) para generar la información de salida (outputs: contenidos, predicciones, recomendaciones, etc.). Durante este proceso de creación o de entrenamiento de estos sistemas con la información o datos previamente facilitados, el modelo va aprendiendo y generando nuevas salidas u outputs.

De esta forma, no es nada extraordinario que el modelo nos ofrezca una respuesta no acertada o directamente errónea, lo que se conoce como **alucinaciones**, y ello suele deberse, entre otros motivos, a que estos sistemas no tienen datos suficientes con los que poder entrenar, y, por tanto, mejorar los modelos y los resultados de información. Dicho de otro modo: **la IA no ofrecerá un resultado óptimo sin datos**.

Pero no solo necesitamos urgentemente poner a disposición del desarrollo de la IA nuestro conocimiento, nuestros datos, sino también **que estos datos sean de calidad y seguros** para que el sistema sea fiable, y las tareas de procesamiento de esos datos, efectivas. Este es el principal objetivo y preocupación de la Estrategia Europea de Datos[192] que ha evolucionado la ya tradicional concepción de los "portales de datos", pasando por el concepto de "datos abiertos" hasta la actual concepción de **"espacios de datos".**

Se estima que el 90% del conocimiento de la humanidad se encuentra en formatos que aún no han sido convertidos en datos manejables por los sistemas de inteligencia artificial (muchos de ellos, libros tradicionales). La Estrategia Europea de Datos parte, así, de la idea de **poner en común los datos y la sabiduría en una especie de mercado** único de los datos donde puedan ser compartidos y utilizados por todos con un marco jurídico de confianza, aunque procedan de diversas fuentes, ya que dichos datos son esenciales para el aprendizaje y la mejora continua de los sistemas.

Por otro lado, la Estrategia Europea de Datos persigue **convertir estos espacios comunes en una garantía para la innovación de las aplicaciones y sistemas de la IA,** pues, con acceso a estos datos, los desarrolladores podrán crear aplicaciones más innovadoras y adaptadas a las necesidades de cada sector. En el caso del legal, me referiré en breve al supuesto del CENDOJ, donde la falta de acceso a sus datos está limitando el desarrollo de nuevas tecnologías y aplicaciones.

PORTALES DE DATOS VS DATOS ABIERTOS Y ESPACIOS DE DATOS

Por dar unas breves pinceladas de estos conceptos, los **portales de datos** venían a ser las tradicionales páginas webs públicas, generalmente creadas por ayuntamientos, comunidades autónomas u otras administraciones y organismos públicos, donde se dan a conocer un conjunto de datos abiertos al público sobre cuestiones generalmente relacionadas con la cultura, meteorología, turismo o cuestiones estadísticas. Posteriormente, se evolucionó hacia el con-

192 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

cepto de **datos abiertos**"[193], introducido por la Directiva relativa a los datos abiertos y la reutilización de la información del sector público del año 2019, bajo el principio general de que estos datos puedan ser reutilizables tanto con una finalidad comercial como no comercial (artículo 3). Finalmente, se ha llegado al actual concepto de **espacios de datos** al que nos hemos referido anteriormente.

En el artículo "Cuando los datos abiertos se encuentran con los espacios de datos" publicado en el portal adminitracionelectronica.gob.es[194], se trata de explicar la diferencia entre el concepto de portal de datos y espacios de datos como si se tratara de un picnic. Textualmente la explica del siguiente modo:

"Imagínate un picnic entre amigos. Un amigo organiza el picnic como organizador y trae la mesa y los cubiertos (este amigo representa la infraestructura de intercambio de datos en forma de portal) (Figura 1). Algunos amigos (proveedores de datos) contribuyen a este picnic trayendo comida y bebida. Los proveedores de datos ponen la comida y bebida en la mesa que está disponible para el resto de amigos (reutilizadores de datos), quienes pueden consultar lo que hay disponible, y beber, comer y consumir lo que quieran. Este es un **picnic abierto**; cualquier amigo puede venir y participar del picnic como proveedor o consumidor. El anfitrión proporciona la mesa y los cubiertos necesarios para consumir la comida y bebida. Este tipo de picnic tiene sus ventajas. Sin el anfitrión, es posible que los amigos no se hubieran reunido para hacer un picnic. Sin embargo, este modelo también tiene desventajas. Los amigos dependen del anfitrión. Si el anfitrión llega tarde, proporciona una mesa de mala calidad o necesita volver a casa, los amigos no tienen otras opciones para su picnic.

Sin embargo, es difícil tener un picnic único que satisfaga las necesidades de todos en cada situación. Por lo tanto, no todos los ecosistemas de intercambio de datos funcionan como un portal de datos, lo que explicaremos imaginando los ***espacios de datos*** como un tipo diferente de picnic. En este picnic, no hay

193 Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público, https://www.boe.es/doue/2019/172/L00056-00079.pdf

194 Fuente: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/2024/Marzo/noticia-2024-03-11-Cuando-datos-abiertos-encuentran-espacios-de-datos.html?paginaHemeroteca=1

anfitrión (Figura 2). Cada amigo tiene su propia mesa donde puede ofrecer comida y bebida. Los amigos dan o reciben lo que necesitan en interacción directa con los otros amigos que necesitan u ofrecen algo. Alguien trae comida y bebida, otro trae cubiertos y platos, y otro trae una mesa. Cada amigo es titular de los derechos de lo que ofrece. Puede tomar más tiempo reunir toda la comida, bebidas, cubiertos y mesas necesarias, pero es probable que el picnic se lleve a cabo si hay suficientes amigos y son diversos en sus opciones. El picnic también es más resistente, ya que varios amigos pueden ofrecer el mismo tipo de comida o suministros, y dura mientras haya alguien cerca.

Este caso se asemeja a un espacio de datos ideal con una estructura descentralizada, donde cada participante tiene soberanía sobre sus datos y puede decidir con quién compartirlos. Esta estructura permite varios niveles de apertura en los datos: algunos datos están restringidos y solo pueden ser utilizados por determinadas partes interesadas. Los espacios de datos admiten esta funcionalidad adicional para casos de uso que la necesitan".

LA UE ESTÁ PREPARANDO EL MARCO LEGAL PARA FACILITAR LA COMPARTICIÓN DE DATOS

A fin de tratar de dotar de ese marco jurídico de confianza, la Unión Europea está desarrollando e implementando una importante **batería legislativa** con la que pretende y alienta a que tanto los estados como las organizaciones, empresas y ciudadanos compartan esos datos, haciéndolos no solo abiertos, sino también comunes en el ámbito europeo. Si bien esto pudiera parecer en sí mismo algo beneficioso para la sociedad, los desafíos técnicos, éticos, jurídicos y para los derechos fundamentales que este sistema entraña son tremendos.

Por ponerles un ejemplo: el Reglamento (UE) 2023/2854, del Parlamento Europeo y del Consejo de 13 de diciembre de 2023, sobre normas armonizadoras para un acceso justo a los datos y su utilización[195], consciente de la recogida de datos de usuarios de productos y servicios conectados a internet, establece, en su artículo 3, como una obligación que todos los productores y

195 Reglamento (UE) 2023/2854, del Parlamento Europeo y del Consejo de 13 de diciembre de 2023, sobre normas armonizadoras para un acceso justo a los datos y su utilización, por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos).

diseñadores de estos productos los fabriquen de modo que los usuarios tengan siempre un conocimiento de qué tipo de información se está recogiendo con su uso. En concreto, la norma establece que dichos datos, por defecto, deben ser accesibles con facilidad, seguridad, gratuitamente, en un formato completo, estructurado, de utilización habitual y de lectura mecánica, de modo que se garantice que los usuarios puedan acceder a esos datos, conocerlos y, en su caso, puedan suprimirlos, creando un catálogo de derechos para los usuarios sobre esta materia.

Y decimos que los **desafíos jurídicos** son tremendos, entre otros motivos, porque **no todos los datos pueden estar disponibles al público**: podrían estar protegidos bien por los derechos de propiedad intelectual, bien por la normativa de protección de consumidores, o por el derecho de la competencia y otra normativa europea. También podría tratarse de datos de carácter personal o ser datos especialmente comprometidos en determinados ámbitos estratégicos a nivel europeo, para cuyos supuestos la norma también prevé una serie de exclusiones o limitaciones en su uso.

Pero claro, si limitamos todos los ámbitos de uso de estos datos abiertos, de nuevo nos podríamos encontrar ante el principio de un círculo vicioso, y mi smartphone no me facilitaría información fiable sobre la flor que he fotografiado. Por ello, la Unión Europea pretende **aprovechar el valor de estos datos en beneficio de la economía y la sociedad**, marcando el camino hacia la creación de espacios comunes en sectores u ámbitos estratégicos, como son la salud, la agricultura, energía, movilidad, finanzas o la administración pública, y dotándoles de una infraestructura segura que preserve la privación de la información, y que tenga unas normas de acceso justas, transparentes, proporcionales y no discriminatorias.

ESPACIOS COMUNES DE DATOS EN EL SECTOR LEGAL O JURÍDICO

Actualmente ya existen diversos proyectos activos de espacios comunes de datos en el ámbito de la salud -cuya necesidad se hizo patente a raíz de la pandemia por la Covid-19- y en el de la cultura europea, pero echamos de menos una mayor posibilidad de reutilización gratuita y libre de los datos en el **sector legal o jurídico**.

Existe actualmente una gigantesca base de datos llamada CENDOJ donde se conservan miles de sentencias, autos y otros precedentes jurisprudenciales, cuyo uso y tratamiento de forma masiva no se encuentran abiertos. Son diferentes los autores que claman por la posibilidad de su apertura, como fue el caso de Dª. Elen Izarabal en su ponencia en el Congreso IAbogatec 2.0, celebrado por el Ilustre Colegio de la Abogacía de Murcia de noviembre de 2023. Además, el uso de los datos judiciales abiertos se convierte en una premisa esencial para la transformación digital de la justicia, como explica el interesante documento para Datos.gob sobre "La regulación de los datos abiertos y la reutilización de la información en el sector público en el ámbito judicial. Retos, dificultades y oportunidades", elaborado por D. Julián Valero, catedrático de la Universidad de Murcia para la Secretaría de Estado de digitalización e inteligencia artificial del Ministerio de Asuntos Económicos, quien apela a la "gran oportunidad" de contar con datos abiertos en el ámbito judicial para la generación de servicios avanzados basados en la innovación tecnológica en el ámbito judicial y, en general, para lograr una mayor eficiencia en el sector legal (Legaltech).

En definitiva: poder acceder, clasificar, procesar y compartir estos datos creados por todas las administraciones públicas, organizaciones, instituciones y empresas, y por los propios ciudadanos, todo ello en un marco jurídico transparente, confiable y seguro es crucial para el desarrollo de las nuevas tecnologías de la inteligencia artificial. La garantía de protección de los derechos fundamentales de los ciudadanos, los derechos de propiedad intelectual de los creadores de los datos, y la protección de la sensibilidad de otros datos es la barrera que jurídicamente ha de crearse para que no solo los datos y los sistemas sean confiables, sino para que también los ciudadanos confiemos en los sistemas de inteligencia artificial que poco a poco van introduciéndose en nuestro día a día.