IUS ET SCIENTIA

Vol. 9 • Nº 1 ▪ 2023

ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA
© Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

IUS ET SCIENTIA

2023 • Vol. 9 • Nº 1 • ISSN 2444-8478

https://editorial.us.es/es/revistas/ius-et-scientia

https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

CC BY-NC-ND 4.0.

EQUIPO EDITORIAL

DIRECTORES

Dr. Daniel García San José, Universidad de Sevilla

Dr. Fernando Llano Alonso, Universidad de Sevilla / Grupo de Investigación SEJ-504, España

Dr. César Villegas Delgado, Universidad de Sevilla / Grupo de Investigación SEJ-112, España

VOCALES

Dr. Miguel Álvarez Ortega, Universidad de Sevilla, España

Dr. Andrés Bautista Hernáez, Universidad de Málaga, España

Dr. Justo Corti Varela, Universidad CEU San Pablo

Dra. Yolanda García Ruiz, Universidad de Valencia, España

Dra. Laura Gómez Abeja, Universidad de Sevilla, España

Dra. Nicole Kerschen, Université Paris Ouest, Francia

Dra. Itziar de Lecuona Ramírez, Universidad de Barcelona, España

Dr. Luis Lloredo Alix, Universidad Autónoma de Chile, Chile

Dra. Pilar Martín Ríos, Universidad de Sevilla, España

Dr. Enrique César Pérez-Luño Robledo, Universidad de Sevilla, España

Dr. Riccardo Perona, Universidad de Cartagena, Colombia

Dr. Rafael Vale e Reis, Universidad de Coimbra, Portugal

Dr. Michele Beniamino Zezza, Universidad de Pisa

COMITÉ ASESOR

Dra. María Isabel Torres Cazorla, Universidad de Málaga, España

Dra. Ana María Marcos del Cano, UNED

Dr. José Manuel Sánchez Patrón, Universidad de Valencia, España

Dr. Xavier Pons Rafols, Universitat de Barcelona, España

Dra. Anna M. Badia Martí, Universitat de Barcelona, España

Dr. Simone Penasa, Universidad de Trento, Italia

CONSEJO CIENTÍFICO

Dr. Manuel Becerra Ramírez, Universidad Nacional Autónoma de México, México

Dra. María Casado González, Universitat de Barcelona

Dr. Alfonso Castro Sáenz, Universidad de Sevilla, España

Dr. Óscar Duque Sandoval, Universidad Autónoma de Occidente, Santiago de Cali, Colombia

Dra. Nuria González Martín, Universidad Nacional Autónoma de México, México

Dr. Mario Giuseppe Losano, Universidad del Piamone Oriental, Italia

Dr. Francisco Javier Gutierrez Suárez, Universidad Autónoma de Occidente, Santiago de Cali, Colombia

Dra. Cristina Sánchez-Rodas Navarro, Universidad de Sevilla, España

Dr. José Antonio Seoane, Universidad de A Coruña, España

Dr. João Carlos Simões Gonçalves Loureiro, Universidad de Coimbra, Portugal

Dra. Viktorija Žnidaršič Skubic, Universidad de Ljubijana, Eslovenia

Dr. Manuel Gómez Valdéz, Florida International University, Estados Unidos de América

CONSEJO DE REVISIÓN

Dr. José Jesús Albert Márquez, Universidad de Córdoba, España

Dr. Angelo Anzalone, Universidad de Córdoba, España

Dr. Juan José Bonilla Sánchez, Universidad de Sevilla, España

Dr. Ignacio Campoy Cervera, Universidad Carlos III de Madrid, España

Dra. María Isabel Garrido Gómez, Universidad de Alcalá, España

Dr. Luis Ernesto Orozco Torres, Universidad Autónoma de Ciudad Juárez, México

Dr. José Luis Pérez Triviño, Universidad Pompeu Fabra, España

Dr. Ramón Ruiz Ruiz, Universidad de Jaén, España

Dr. Adolfo Jorge Sánchez Hidalgo, Universidad de Córdoba, España

Dr. Javier Zamora Bonilla, Universidad Complutense de Madrid, España

IUS ET SCIENTIA

2023 • Vol. 9 • Nº 1 • ISSN 2444-8478

https://editorial.us.es/es/revistas/ius-et-scientia

https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

CC BY-NC-ND 4.0.

IUS ET SCIENTIA. Vol. 9, Nº 1, junio (2023)

Edita: Editorial de la Universidad de Sevilla.
© Editorial Universidad de Sevilla 2022
https://editorial.us.es/es/revistas/ius-et-scientia
https://institucional.us.es/iusetscientia/index.php/ies/index

Financiación: Revista financiada por la Universidad de Sevilla dentro de las ayudas del VII PPIT-US

Periodicidad Bianual (Junio, diciembre)

ISSN: 2444-8478

DOI: https://dx.doi.org/10.12795/IETSCIENTIA.2023.i01

Maquetación: Referencias Cruzadas - referencias.maquetacion@gmail.com

Licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

IUS ET SCIENTIA
2022 • Vol. 8 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2022
CC BY-NC-ND 4.0.

Índice

COMENTARIOS

RESEÑAS

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. -5
ISSN 2444-8478 •

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

CARTA DE LOS EDITORES

EDITORS´ LETTER

Daniel García San José
Fernando Llano Alonso
César Villegas Delgado

Ciberciudadanía y derecho digital

Hace veinte años, cuando aún no existía el Internet de las cosas donde se intercambian millones de datos e información a través de dispositivos desarrollados con software y sistemas informáticos avanzados, ni se había extendido el recurso a los algoritmos predictivos para la toma de decisiones automatizadas, ni se había explorado el insondable espacio del multiverso en el que, parafraseando al filósofo surcoreano Byung Chul Han, el sr humano va perdiendo su autonomía a medida que profundiza en el mundo de las no-cosas (Undinge), Antonio E. Pérez Luño publicó un libro tan novedoso como provocador que llevaba por título la siguiente pregunta: *¿Ciberciudadanía o ciudadanía.com?* (2003).

El autor de esta monografía, pionero de los estudios sobre iuscibernética e informática jurídica en España, valoraba la contribución de Internet a forjar una ciberciudadanía como forma de ciudadanía internacional y cosmopolita, pero también advertía de los potenciales riesgos que el mal uso de los medios tecnológicos de información y control podrían acarrear no solo contra las libertades, la intimidad y la dignidad de millones de los ciudadanos, sino contra la democracia misma y el Estado de Derecho. La respuesta a la pregunta planteada por Pérez Luño en este libro dependerá, en última instancia, dependerá del nivel de exigencia de los gobiernos democráticos en la defensa de las libertades de los ciudadanos, pero también corresponderá a estos mantener una actitud cívica responsable en el uso de dichos medios.

En el presente número de *Ius et Scientia*, primero de 2023, se publican nueve trabajos originales (cinco artículos y cuatro notas) en los que se analizan cuestiones y dilemas ético-jurídicos característicos de la sociedad de las nuevas tecnologías.

El uso de la Inteligencia Artificial en el análisis de impacto normativo es objeto de estudio por parte de Silvia Matallana Villegas. A fin de explorar el potencial de la Inteligencia Artificial en el ámbito normativo, la autora analiza las oportunidades de involucrar el virtuoso binomio metodología-tecnología para corregir problemas que afectan a la legislación tales como hiperlegislación, la baja calidad de las normas, la hipostenia y la hipertrofia de los sistemas normativos.

Por su parte, Enrique Manuel Puerta Domínguez dedica su artículo al estudio del marco jurídico de la Unión Europea sobre protección de datos y garantías ciudadanas ante la Administración

pública electrónica. La perspectiva del análisis propuesta por este autor integra tanto la legalidad europea como la jurisprudencia del Tribunal de Justicia, las virtualidades aplicativas que tiene la normativa de la UE en materia de protección de datos en lo que afecta a las relaciones entre las Administraciones públicas y los ciudadanos. Tal normativa es exigente a la hora de deparar las obligaciones que competen a los que realizan el tratamiento o depósito de datos personales, y es de recibo que sean los entes públicos los que deban, antes que nada, dar ejemplo de una buena gestión. Materia rica y compleja, aun no ampliamente abordada, conoce una sugerente casuística jurisprudencial.

De explicar el impacto del ChatGPT en el mundo del Derecho, el fenómeno más reciente de la tecnología desarrollada con IA, se ocupa María Dolores García Sánchez, que parte del déficit de regulación y de las múltiples lagunas que actualmente existen en torno a lo que denomina, de forma metafórica, como un "rinoceronte gris". En este artículo se estudia precisamente el estado de la cuestión del fenómeno de ChatGPT en clave de Derecho comparado, concretamente en el ámbito jurídico de Italia, España y la Unión Europea, a fin de poner de manifiesto la necesidad de contar con unas líneas básicas regulatorias para que una IA de este tipo pueda implementarse en el mercado sin atentar contra los derechos fundamentales de los usuarios y minimice los potenciales peligros inherentes a su uso.

De la protección de la biodiversidad desde el punto de vista de los derechos humanos se ocupa Simona Fanni, que se inspira en la jurisprudencia ambiental sobre los derechos de la Naturaleza y en la jurisprudencia climática. Esta jurisprudencia destaca por una serie de rasgos emblemáticos, tales como: el empleo de los derechos humanos y constitucionales para evaluar el cumplimento de las obligaciones estatales que se derivan del derecho internacional de los derechos humanos y del derecho ambiental internacional; el lenguaje de la equidad intrageneracional e intergeneracional; una novedosa concepción de la extraterritorialidad. A este respecto, el presente estudio analiza las decisiones nacionales e internacionales más significativas, y teoriza que los resultados obtenidos por la jurisprudencia considerada podrían ser beneficiosos para la protección de la biodiversidad y su justiciabilidad, incluso mediante el diálogo judicial multinivel.

A la delimitación de los conceptos fundamentales de la lucha contra el cibercrimen por medio del ciberpatrullaje de las Fuerzas y Cuerpos de Seguridad del Estado en el ciberespacio dedica su estudio Manuel Távora Serra. En la labor policial de prevención e investigación de los comportamientos delictivos sin control jurisdiccional previo, es preciso diferenciar entre el *ciberpatrullaje*, cuando dicha actividad tiene lugar con carácter previo a un proceso penal, y la *ciberinvestigación*, cuando tiene lugar en el marco de un proceso penal previamente incoado. A partir de esta distinción el autor explica las claves principales y las implicaciones de ambos términos en la política de seguridad del Estado y en la esfera de protección de los derechos fundamentales y libertades de los ciudadanos.

Dentro del apartado de notas, Iván Hernández Blanco nos presenta un original estudio sobre la gestión de la ciencia, la tecnología y la innovación en los organismos públicos de investigación (OPIs) de España. El autor parte de la constatación de un dato

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 6-8
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.01

revelador: en los últimos años el avance de la inversión en I+D+i ha crecido exponencialmente. Tras la crisis financiera de 2007-2008 y la crisis sanitaria originada por el virus SARS-CoV-2, la inversión en I+D+i en España ha alcanzado los 17.249 millones de euros en 2021, el 1,43% del PIB. Con motivo de este aumento es necesaria una forma eficaz de poder gestionar los recursos en materia de ciencia y tecnología. La financiación concedida por parte de la Unión Europea con los fondos Next Generation EU y concretamente del Mecanismo para la Recuperación y la Resiliencia (MRR) han potenciado aún más esta dotación económica para investigación en los Organismos Públicos de Investigación.

Marta Reguera Cabezas analiza el peculiar caso de la interrupción en Singapur de las técnicas de reemplazo mitocondrial, que pueden reducir significativamente el riesgo de transmisión de enfermedades mitocondriales a la descendencia. Singapur estaba analizando la posibilidad de realizar cambios legislativos históricos que permitirían a las parejas afectadas por enfermedades mitocondriales hereditarias maternas la oportunidad de tener hijos genéticamente no afectados. Sin embargo, tras el informe del Comité Asesor de Bioética (cuyas siglas en inglés son BAC), parece que la República de Singapur, no se convertirá en el tercer país a nivel internacional en autorizar el uso de las técnicas de reemplazo mitocondrial.

Marina Galvín Gordillo nos aproxima al uso de los robots en la medicina y sus aspectos legales. Así como a sus efectos y consecuencias. Por otra parte, en su estudio nos explica los avances en la tecnología y la Inteligencia Artificial y sus aplicaciones en el campo de la medicina y la salud, que ha supuesto el avance en la calidad de vida y está ayudando a curar enfermedades y dando diagnósticos que hasta hace poco eran impensables.

Por último, Manuel Pérez Sarabia, centra su estudio en el ámbito de la deontología profesional, la seguridad del paciente y los principios esenciales de la buena praxis en el ámbito sanitario. En el debate abierto sobre regulación de la telemedicina, la IA y la robótica en el ámbito sanitario, y como estrategia de gobernanza europea prevista en el Libro Blanco sobre inteligencia artificial, así como para garantizar el establecimiento de un marco ético y jurídico apropiado, basado en los valores de la Unión Europea y en consonancia con la carta de Derechos Fundamentales, observa el autor que la situación de disrupción tecnológica no debe ir unida a una disrupción reguladora, puesto que la normativa vigente da respuesta a muchos aspectos esenciales. Por esta razón, propone Pérez Sarabia la deontología profesional, la seguridad del paciente y los principios de trasparencia, veracidad y competencia profesional, como conceptos y principios clave para superar con éxito los retos tecnológicos sanitarios a los que nos enfrentamos, y para que las autoridades públicas puedan garantizar que el desarrollo y uso de tecnologías esté en consonancia con los derechos humanos.

El actual número 1/2023 de Ius et Scientia se cierra con la sección de recensiones, en la que publicamos dos comentarios a libros recientes de Pilar Martín Ríos et al.: *La Tecnología y la Inteligencia Artificial al servicio del proceso*, Colex, Madrid, 2023, 336 páginas (recensión a cargo de Evelyn Téllez Carvajal), y David Vallespín Pérez: *Inteligencia Artificial y Proceso: eficiencia vs garantías*, Juruá, Oporto, 2023, 279 páginas (reseña de Luis Ernesto Orozco Torres).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 6-8
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.01

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

El uso de la Inteligencia Artificial en el análisis de impacto normativo

THE USE OF ARTIFICIAL INTELLIGENCE IN REGULATORY IMPACT ANALYSIS

Silvia Matallana Villegas
Senado de la República, México
matallana.villegas@gmail.com 0009-0003-0962-9462

Recibido: 03 de mayo de 2023 | Aceptado: 09 de junio de 2023

RESUMEN

El Análisis de Impacto Normativo se implementa en la actualidad en varios países como una herramienta de vanguardia para la mejora de la calidad de la ley. Con el objetivo de explorar el potencial de la Inteligencia Artificial en el ámbito normativo, se analizan las oportunidades de involucrar el virtuoso binomio metodología-tecnología para corregir problemas que afectan a la legislación tales como hiperlegislación, la baja calidad de las normas, la hipostenia y la hipertrofia de los sistemas normativos. Se discuten las limitantes y virtudes de esta metodología de evaluación, para detectar áreas de oportunidad de inclusión de la Inteligencia Artificial, con la finalidad de apoyar el contenido y la forma de la intervención legislativa proyectada, anticipando sus posibles impactos. Esto favorecerá la aprobación de normas con menos probabilidades de fallar.

PALABRAS CLAVE

Evaluación de Impacto Normativo
Calidad legislativa
Inteligencia Artificial

ABSTRACT

The Regulatory Impact Analysis is currently implemented in several countries as a cutting-edge tool for improving the quality of the law. The opportunities to involve the virtuous methodology-technology binomial are analyzed to explore the potential of Artificial Intelligence in the regulatory field. The aim is to correct problems that affect legislation such as hyper-legislation, low quality of the law, hyposthenia and the hypertrophy of regulatory systems. The limitations and virtues of this evaluation methodology are discussed, to detect areas of opportunity for the use of Artificial Intelligence. It could support the contents projected by the legislative intervention, anticipating it's possible impacts, so that laws are approved with less chances to fail.

KEYWORDS

Regulatory Impact Assessment
Legislative quality
Artificial Intelligence

I. Introducción

El presente artículo pretende explorar las oportunidades y posibles beneficios en la implementación de tecnologías de la Inteligencia Artificial (IA)[1] en el Análisis de Impacto Normativo (AIN). De manera precisa, el origen de la figura del AIN se encuentra en el movimiento global y europeo cuyo fundamento consiste en el desarrollo de un ordenamiento jurídico de calidad, y conceptos de *better regulation,* y el más reciente de *smart regulation,* bajo los cuales se han logrado sus más notables avances.

En consecuencia, el AIN ha sido reconocido como una expresión de la denominada regulación inteligente, un instrumento que permite introducir metodologías novedosas en el ámbito normativo-legislativo para eficientar la calidad de las leyes y favorecer el desempeño parlamentario. Consiste en un instrumento para examinar de manera sistemática los efectos positivos y negativos de las normas, antes de su adopción (ex ante), y durante su aplicación en la realidad (ex post).

Para referirse al AIN se utiliza, a veces de manera indistinta, el término normativo o regulatorio. El término "normativo" se relaciona con la producción normativa de los poderes públicos, y es adecuado en contextos jurídicos como el nuestro, ya que este instrumento ha centrado su atención mayoritariamente en proyectos de normas y, no como en el ámbito anglosajón, incluyendo planes, programas u otro tipo de intervenciones públicas. Por su parte, las regulaciones se entienden como cualquier acción normativa de los poderes públicos para el desarrollo de una política que suponga obligatoriedad (Carceller, 2019:2).

En última instancia, el término "impacto" es central para comprender y explicar la esencia de este instrumento, dado que la preocupación por los efectos de las normas sobre el entorno es clave para entender su funcionamiento y las finalidades que persigue (Carceller, 2019:4).

En su definición más amplia, consiste en una herramienta para la mejora de la calidad material de las normas *a priori* (ex ante) y *a posteriori* (ex post), mediante la cual se valoran, de forma cualitativa y/o cuantitativa, las consecuencias de las diferentes soluciones que se identifican para resolver la cuestión o el problema detectado. Su función es aportar información empírica que facilite la adopción de las decisiones. Por ello, pretende ser un proceso científico que se apoya en diferentes metodologías vinculadas a los campos en los que se aspira estudiar el impacto producido; su ámbito puede incluir la actividad normativa no legislativa, pero de manera específica se concentra en la de carácter normativo-legislativo.

Los AIN recurren a mecanismos metodológicamente sistematizados y cuantificables para la evaluación individualizada y concreta de la calidad de cada norma jurídica, en términos de su impacto en la actividad de los ciudadanos.

1. La Real Academia de la Lengua la define como "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".

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

De manera reciente, esta metodología ha avanzado en el ámbito legislativo para garantizar la eficiencia y la eficacia de la ley con un énfasis en la calidad material de la ley. Su objetivo consiste en dotar a los legisladores de elementos para la toma de decisiones favoreciendo una debida deliberación parlamentaria. Este instrumento mejora la calidad normativa al anticipar sus efectos, a través del análisis del impacto de las normas, que permite que las leyes puedan concretarse en políticas públicas fundadas en necesidades reales, asegurando su enunciación con una base empírica y objetiva.

Las metodologías propias del AIN tienen como propósito, recuperar la legitimidad y la seguridad jurídica de la ley. Adicionalmente, constituyen una herramienta invaluable para promover la legitimidad de una norma, a través de la implementación de consultas públicas como parte de su metodología (Ehrman, 2018).

Teniendo en cuenta que el AIN es una herramienta de política pública que tiene por objeto garantizar la calidad de las regulaciones, de manera indudable la IA sirve para mejorar la formulación, ejecución y evaluación de las políticas públicas que se plasman en la normatividad.[2]

Con el fin de determinar el potencial de su aplicación en la implementación del AIN, primero se comentan las dos limitantes más críticas que la doctrina señala: altera el funcionamiento de la representación política propia del funcionamiento parlamentario cuando antepone lo científico a lo político. En segunda instancia, los tiempos del proceso parlamentario inevitablemente se prolongan con la implementación de las evaluaciones del AIN, al requerir tiempo adicional para su realización.

Cada uno de estos argumentos se explora y discute para determinar si el uso de tecnologías de IA como una competencia tecnológica en el ámbito del Derecho, representa una oportunidad o un obstáculo en la implementación de las metodologías del AIN. Se contrastarán las ventajas que hasta el momento se han generado por la introducción de la IA en el ámbito del Derecho Público, en particular en la formulación de políticas públicas.

Se tendrá en cuenta que la expansión de la IA y su inclusión en el Derecho no necesariamente se ha presentado antagónica, sino más bien simbiótica como lo señala Almonacid (2022:86). Si bien la expansión de las tecnologías propias de la IA ha dado lugar a problemas jurídicos y globales que son claramente discutidos por Parra *et al* (2021), es necesario que la relación norma-tecnología se constituya en un reto y un desafío para el futuro del Derecho.

De acuerdo con Almonacid (2022:87), el adecuado aprovechamiento de la inteligencia artificial requiere un cambio de paradigma para incorporar las ventajas de la unión de la experiencia jurídica tradicional con las innovaciones tecnológicas frente a las ancestrales técnicas legislativas. La historia demuestra que la informática jurídica debe mantener el ritmo en el avance y adaptación en los procesos de transformación social (Almonacid 2020:172). En efecto, en el sector público la IA puede potenciar la capacidad para lograr impactos sociales, económicos y ambientales para el bienestar de los ciudadanos, siempre que se implemente en una forma ética y estratégica (CAF: 2022).

2. En la actualidad, ya se está experimentando con avances tales como el prototipo de chat bot ChatGPT que puede ayudar en el proceso de investigación para la elaboración de política pública.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

En este sentido, un modelo avanzado de impacto normativo, diseñado y comprometido con la calidad antes que con la cantidad de producción normativa, presupone optimizar el proceso legislativo no solo en su costo, efectividad económica, social, ambiental, y eficiencia presupuestal, sino en su eficacia comunicativa que puede contribuir a superar la paradoja de la ilusión normativa y la decepción con el Derecho (Almonacid, 2022).

II. Limitaciones del AIN

2.1. Altera el funcionamiento de la representación política

Una de las principales inquietudes teóricas que genera polémica sobre la delimitación del ámbito del AIN sostiene que antepone lo científico a lo político. Como resultado se altera el funcionamiento de la representación política, considerando que el orden democrático de la ley, por su carácter representativo no puede delegarse. En consecuencia, "el proceso de elaboración y aprobación de la ley no se puede subordinar a un procedimiento técnico que determine sus contenidos, lo que lo colma de falta de legitimidad" (Bronfman, 2006: 39). En efecto, hay quienes han asociado la evaluación legislativa con la política tecnocrática en la que los procesos democráticos son subsumidos por los procesos técnicos de valoración, desatando posibilidades de una influencia tecnocrática indebida.

Frente a este presunto conflicto entre lo político y lo científico, Crick (2001:124) defiende la separación de estos dos ámbitos, cuando considera que la ciencia y la política son procedimientos que avanzan por caminos distintos que no deben mezclarse o fundirse porque son modos diversos de mirar una realidad común con diferentes propósitos. Si éstos se confunden, y son considerados cada uno de ellos como ilimitados, entonces lo político y lo científico entran en conflicto y se contradicen, por lo cual no sería posible su complemento y reconciliación en el ámbito legislativo.

Este cuestionamiento se puede remitir a la discusión sobre la cientificidad de las ciencias sociales y del Derecho, en particular con respecto a las ciencias duras. Es indiscutible que el carácter de científico dota al conocimiento de autoridad, le otorga certeza y validez. La idea de que el saber y la verdad solo existen dentro de la ciencia, llevó a hacer extensivo este modelo de conocimiento como virtud también propia de las ciencias sociales. No obstante, bajo diversos argumentos, hay quienes todavía discuten sobre el auténtico estatus de ciencia que se ha otorgado a las disciplinas científicas sociales y humanísticas.

En este sentido, la crítica que enfrentan las ciencias sociales y, en particular el Derecho, se manifiesta cuando se afirma que a pesar de que hacen uso de técnicas descriptivas propias cuantitativamente exactas, éstas no se acompañan de una teoría sólida que las fundamente, ni de una predicción igualmente precisa. También se señala cómo, cuando desarrollan modelos abstractos muy elaborados, éstos no se arraigan firmemente en el material empírico. Se considera que el concepto de ciencia riguroso no se puede emplear de manera específica en las ciencias sociales, dado que se trata de predecir y analizar comportamientos individuales y sociales.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

Así, las ciencias sociales, tales como la sociología, la antropología y el propio Derecho, han sido señaladas restándoles carácter de cientificidad porque no se basan estrictamente en una rigurosa metodología que siempre involucre mediciones o experimentación. De hecho, en este punto es válido resaltar que las ciencias duras tampoco se basan siempre en experimentación rigurosa, la observación también tiene un papel relevante como método de investigación.

Precisamente ésta es la tarea de la ciencia: conocer a través de describir y explicar, labor que no es ajena a las ciencias sociales y al Derecho. Su propósito, de igual manera, consiste en describir y explicar configuraciones sociales individuales; cuantificar y medir no es un objetivo de la ciencia sino meros instrumentos en la construcción de la verdad. Las ciencias sociales, afirma Weber (1986), al igual que las ciencias naturales, deben producir explicaciones causales que son, a su vez, explicaciones fragmentarias y parciales, esto es, finitas, de una realidad infinita. Esto constituye un elemento básico de la evaluación de las leyes en tanto estudia los efectos de la ley para establecer relaciones de causalidad útiles para el legislador, como cualquier procedimiento técnico-científico (Bronfman, 2006).

En cuanto al elemento de predictibilidad resulta importante establecer una distinción. En las ciencias duras, la predictibilidad propia de la puesta a prueba de las hipótesis científicas no da cabida a un resultado inesperado, cosa que si ocurre todo el tiempo en las ciencias sociales. En sustitución de la posibilidad de predecir, el conocimiento que se deriva de la investigación social brinda la alternativa de explicar, comprender, valorar y reflexionar sobre hechos sociales. Esto permite que la investigación jurídica sugiera la modificación del corpus jurídico a la luz de la explicación científica y no del voluntarismo.

Gellner (1984:621) sustenta lo anterior cuando considera que la formulación de teorías y predicciones sobre una realidad social que se traduce en el ámbito jurídico, cuenta con el mismo rigor formal, precisión de observación e inventiva intelectual propias de las ciencias duras, lo cual las dota de un carácter de ciencia auténtica y genuina.

Desde la perspectiva tradicional de la ciencia jurídica, la norma es el resultado de la argumentación, y su vigencia la determina su legalidad más no un criterio de verdad. La argumentación jurídica se presenta desde esta perspectiva, como el único instrumento metodológico que hace posible la racionalidad jurídica. Siguiendo este razonamiento aplicado a la metodología jurídica, el objeto de estudio en la ciencia jurídica es una construcción teórica e ideológica producto de la argumentación y por tanto su objeto no existe materialmente. Precisamente, el Derecho se presenta a través de la argumentación jurídica como un instrumento formal que hace posible la aplicación de la norma jurídica desde un espacio de racionalidad (Matallana, 2002).

En el ámbito parlamentario, aunque mediante el procedimiento legislativo se podría garantizar una racionalidad formal, de ello no se deduce automáticamente en una racionalidad material. Incluso, de acuerdo con Segura (1998), en tanto el legislador pretende ser racional, no lo consigue sencillamente porque es imposible. Por este motivo es necesario definir o precisar el estatuto epistemológico de los estudios sobre la legislación. Consciente de esta necesidad, en un intento por plantear una teoría de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

la legislación para prevenir la irracionalidad en la que se encuentra inmerso el proceso legislativo, Atienza (1997) propone la base para una teoría que incluye tanto el proceso formal (validez normativa), de contenido (valores y principios) y de efectividad (practicidad en la sociedad) para la creación de una norma jurídica.

Este contexto le da sentido al AIN al proporcionar un elemento de cientificidad a la dinámica política propia del proceso legislativo, y ceñirse a una metodología apegada al método científico. No obstante, se ha señalado que esto entra en conflicto con la toma de decisiones bajo un criterio político y conlleva a interrogantes en torno a si la evaluación debe ser "apolítica" o, si se debe evaluar de acuerdo al programa político que propuso la norma.

Es precisamente en el ámbito metodológico que se reivindica el concepto de cientificidad para el AIN, en la medida en que dota de neutralidad valórica al método utilizado, siempre y cuando se establezca una clara distinción entre análisis científico y conclusiones políticas. El análisis científico sin duda fortalece la credibilidad de las evaluaciones en tanto vienen a incorporar un enfoque que sustenta el énfasis en la materialidad del Derecho.

En la práctica, la trascendencia de la distinción entre lo político y lo científico ha sido reconocida por el Servicio de Evaluación del Parlamento suizo, en cuando reconocen como una de sus principales fortalezas la clara distinción que se mantiene entre ciencia y política. Su papel se concentra en realizar un análisis científico, dejando a las comisiones de control el hacer recomendaciones políticas. Esta clara distinción refuerza la credibilidad de las evaluaciones. Es tal el compromiso con la evaluación que, Simone Ledermann como funcionaria encargada de esta función del parlamento suizo reconoce la efectividad de las evaluaciones porque en efecto conducen a en muchas ocasiones a un rediseño de las políticas públicas. Además, en la medida que se les da publicidad, mejoran la transparencia y la rendición de cuentas de la acción política (Ledermann 2022:101).

Para refutar a quienes sostienen que el AIN constituye una interferencia política en la regulación administrativa contenida en una determinada intervención, Revuelta asegura que éstos:

> (…) no constituyen una vía de interferencia política en la regulación administrativa elaborada por agencias técnicamente especializadas, sino como una herramienta de ayuda a la toma de toda decisión normativa, que suministra información a quien la adopta (sobre todo, responsables políticos) sobre la situación a regular, medios disponibles para lograr los objetivos perseguidos y posibles efectos. Por eso se aplican también a las normas provenientes del Parlamento (Revuelta, 2014:90).

Los instrumentos técnicos de evaluación pueden sumarse al trámite legislativo, sin detrimento de la evaluación política del impacto social de las normas proyectadas. No obstante, ¿que sucede cuando se presenta una clara contradicción entre la decisión política y la evaluación técnica? ¿Quiere ello decir la decisión basada exclusivamente en consideraciones políticas puede perder su fundamento?

Para responder a este cuestionamiento es de vital relevancia reiterar que la evaluación de impacto solo tiene el carácter de una herramienta de apoyo, y no un sustituto de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

las decisiones políticas dentro del proceso de toma de decisiones democráticas. En ningún caso es de cumplimiento forzoso, sino que tiene un carácter de sugerencia derivada de hallazgos basada en una metodología de análisis de efectos. Los parlamentos tienen la libertad de considerar o no estos hallazgos contenidos en la evaluación de impacto.

2.2. Obstaculiza la productividad legislativa

El AIN implica un retraso en los procesos legislativos al requerir tiempo adicional que, inclusive, se extiende más de lo esperado cuando no hay datos disponibles y estos se tienen que solicitar a otras instancias. El contra argumento asegura que dotan a la intervención legislativa de mayor estabilidad, permanencia e inmutabilidad. Tiene el potencial de corregir un problema de calidad en el poder legislativo. De manera previa (ex ante) a que se presente una iniciativa de ley, evalúa el impacto de la propuesta (ambiental, social, económico, en la equidad de género, financiero etc.), análisis que determinará si de convertirse en ley tendrá como resultado el objetivo que se propuso, y cuáles serán sus efectos en la sociedad.

En el caso del Parlamento Europeo que tiene una mayor experiencia en la materia, se ha reconocido que el tiempo es un factor importante, de manera que la evaluación de impacto no implica necesariamente un retraso en el proceso legislativo. Se procura que esta evaluación se lleve a cabo rápidamente para poder abarcar todo el proceso legislativo. Normalmente reportan que tardan de tres a cuatro meses en promedio, e incluso han alcanzado el record de nueve semanas. Se observa que el reto en términos de los plazos siempre es la dificultad de obtener los datos, ya sea porque no existen o porque no están desagregados, o quizás porque no son comparables entre los veintisiete Estados miembros de la Unión. Por lo tanto, ante este obstáculo se requiere colaborar con la Comisión Europea para hacer esta recolección de datos, siguiendo el espíritu de la colaboración interinstitucional (Maniaki 2022:80).

Para solventar esta limitante,Valle-Cruz *et al.* (2020) anticipan que el mayor impacto de la IA en la etapa de evaluación en el corto plazo será la disminución de los tiempos necesarios, proporcionando acceso a información valiosa en tiempo real. Esto además permitirá que la evaluación pueda convertirse en un proceso que puede desarrollarse de manera continua y sistemática.

Existen otras limitantes propias de su implementación del AIN, como lo es la demanda de recursos humanos y financieros adicionales en la contratación de expertos. En particular, el Servicio de Evaluación del Parlamento Suizo, dispone de un presupuesto propio para contratar expertos para el caso de asesoramiento en temas específicos como políticas ambientales, por ejemplo, o mandatos sobre cuestiones legales, pero también se puede vincular a un método, por ejemplo, un análisis estadístico específico.

Los costos elevados, especialmente en aquellos casos en los que las materias reguladas son de carácter técnico, se pueden reducir con la IA. Así mismo, el tiempo de investigación que se detina a encontrar información exacta puede favorecerse con estas tecnologías, aumentado la eficiencia y la eficacia en el procedimiento de evaluación.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

Por otra parte, la IA puede asistir el trabajo parlamentario acortando el proceso de la evaluación legislativa y apuntalando la técnica legislativa a través de las bases de datos de las leyes vigentes mediante algoritmos que pueden identificar múltiples problemas que afectan la legislación tales como la proliferación o inflación normativa, antinomias, redundancias, estratificaciones, abrogaciones innominadas e hipostenia legislativa, entre otros. Todos se relacionan con la parte formal de la legislación y pueden ser más fácilmente identificadas mediante el uso de tecnología, que en este caso puede ser incluso superar la capacidad humana.

III. Virtudes de incorporar la IA al AIN

3.1. Favorece la neutralidad y objetividad del AIN

Se ha criticado la técnica evaluativa en cuanto puede llegar a asumir la defensa y promoción de intereses particulares. No se puede ignorar la influencia a partir de los intereses sociales en conflicto durante la toma de decisiones. En efecto, su prestigio como herramienta técnica peligra en la medida en que se asocie con un determinado grupo social, partido político o grupo social o de presión, que pueden llegar a desviar el resultado de la evaluación.

Los instrumentos de evaluación administrativa deben procurar tener un distanciamiento de estos intereses en lo posible para garantizar su neutralidad, como una medida de "sana neutralidad disciplinaria". De acuerdo con Bronfman (2006:41), "debe dotarse de resguardos orgánicos y procedimentales que aseguren su rigor e independencia frente a los intereses afectados".

Esta distancia puede atenderse en las diferentes modalidades y factores que implican momento, costo y personas que lo realizan, teniendo en cuenta que estas decisiones influyen en la posibilidad de que afecte su neutralidad en la medida en que los evaluadores pueden llegar a tener su propia posición personal. Por tanto, un factor relevante es la manera de involucrar los recursos humanos y financieros necesarios para la AIN.

Para alcanzar neutralidad, se requiere garantizar el uso racional de los recursos humanos con el fin de evitar solapamientos innecesarios en el caso de encargar la investigación a un órgano independiente o a un grupo de expertos. En todo caso siempre se corre el riesgo de la interferencia de los especialistas sobre la decisión política en tanto existan compromisos adquiridos con la propuesta legislativa (De Vrieze, 2017).

Existe un debate sobre si las nuevas tecnologías pueden ser neutrales o necesariamente responden a intereses económicos e incluso políticos, ya que la IA al ser un producto social puede, desde su diseño, orientarse hacia priorizar intereses de un determinado grupo social sobre otros. Sin duda, resulta pertinente y prudente explorar, con la cautela del caso, la posibilidad de involucrar IA con la finalidad de neutralizar estos factores humanos que se han comentado.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

3.2. Respalda las capacidades predictivas sobre los efectos normativos

Bien sea que se realice antes, durante o posterior al proceso legislativo, el análisis de los efectos potenciales de la intervención legislativa la dota de capacidades de predicción en tanto se evalúan los resultados, pero también se pronostican sus efectos. Es así como una de las funciones primordiales de la AIN es detectar con anticipación los problemas que generará la entrada en vigor de la norma, lo que Bronfman visualiza como sus capacidades predictivas y potencialidades técnicas; convirtiéndola en una profecía con pocas posibilidades de fallar (Bronfman, 2006:37). Este objetivo se alcanza en la medida que logre detectar con anticipación los problemas que generará la entrada en vigor de la norma.

Indudablemente, la labor de los especialistas que se vinculan en la evaluación, apoyados por la IA, agrega al trámite legislativo los conocimientos científícos y técnicos, y en diversas disciplinas, que redundan en incrementar la capacidad de predecir los efectos de la ley. Esta capadidad predictiva se despliega, como de manera acertada lo identifica Rivera, cuando el evaluador esboza una hipótesis de los probables resultados, del encaje institucional de la norma en el sistema normativo, o recurre al derecho comparado para demostrar el porqué lo efectos se producirán o no dadas las peculiaridades del orden interno repecto al objeto de comparación. (Rivera, 2015:172) Esta función de pronosticar puede ser apoyada por la IA como área de oportunidad, como ya se ha venido anticipando en las consideraciones anteriores.

3.3 Apoya la legitimidad de la consulta

La importancia de la participación de los destinatarios de la norma en el proceso legislativo se entiende en tanto el proceso de formación de la ley convoca distintas preocupaciones sociales legítimas. El desafío consiste en lograr la manera de reconocer y tutelar la mayor parte de los intereses involucrados, o por lo menos alcanzar la armonización de los intereses sociales afectados a lo largo del proceso resolutivo (Reveles, 2017).

La trascendencia de contar con alternativas de participación directa para la sociedad para hacer más genuina la representación de intereses sociales, justifica la implementación de la herramienta del AIN. Así se rescata el papel de la participación directa de los ciudadanos como un recurso para fortalecer la democracia actual, cuando recupera la figura de la consulta como parte del proceso de la intervención legislativa. Consiste en un proceso de consulta con los actores, privados y públicos, afectados en sentido positivo o negativo, directa o indirectamente, sobre el cumplimiento del nuevo dispositivo normativo. A través de la figura de la consulta pública se proporciona al público en general la información relativa a los beneficios reales esperados por la intervención legislativa, promoviendo el ejercicio concreto de la participación democrática.

Este proceso de consulta que involucra a los futuros destinatarios directos de la norma: "permite construir un consenso sobre la estructuración del cuerpo normativo, sin que implique la subordinación de bienes públicos a intereses privados, ya sea de grupos de interés del sector privado, como de intereses de grupos parlamentarios o entre ellos y el Poder Ejecutivo" (Ehrman, 2018:55).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

En efecto, el AIN cumple varios objetivos a través de la consulta pública: resuelve las inconveniencias de la intermediación propia de la figura de la representación, pero además como lo advierte Reveles (2017), fomenta en conjunto la deliberación, la transparencia, la responsabilidad política y la rendición de cuentas.

Ahora bien, la consulta pública también tiene sus limitantes cuando es utilizada como parte del AIN, en tanto puede deslegitimar el proceso de negociación política parlamentaria cuando se entrega un resultado adverso al interés de la mayoría parlamentaria.

Es por esto que cuando el AIN forma parte del proeso de formación de la ley, es importante "enmarcarse en la relación representativa y dotarse de los resguardos orgánicos y procedimentales que aseguren su rigor e independencia frente a los intereses afectados" (Bronfman, 2006: 41).

La implementación de una consulta participativa eficaz reclama valerse de las ventajas de la interacción del binomio virtuoso entre metodología y tecnología, específicamente del análisis del impacto normativo y la IA, teniendo en cuenta que los medios de recolección de la información se centran especialmente en mecanismos digitales, ya sea por las páginas o los correos institucionales, los grupos de trabajo, foros o entrevistas que implican la interacción directa entre servidores públicos y los grupos de interés.

El uso de herramientas de IA tales como la internet y las redes sociales pueden proporcionar un espacio de participación, debate, deliberación, argumentación, movilización y protesta virtual fundamental. No obstante, Almonacid (2022) cuestiona que se cuente con la evidencia de confirme que la IA ha llegado o llegará a concurrir para que la participación en lo público sea realmente efectiva.

3.4. Mejora de la calidad material de las leyes

La calidad de las normas jurídicas compromete dos dimensiones: por una parte, la calidad técnica y formal, que exige rigor, claridad y coherencia con el resto del ordenamiento. En segunda instancia, la calidad material, en cuanto a su contenido, demanda que la norma sea eficiente, efectiva y eficaz para alcanzar los objetivos normativos propuestos.

Este contenido material de las leyes implica enfatizar su condición de instrumentos de políticas públicas. Por ende, para evaluar su efectividad se precisa de una visión integral, cuya evaluación de impacto requiere la participación de un equipo de trabajo multidisciplinario que domine las distintas herramientas metodológicas, y cuente con habilidad y destreza en todos los espacios de conocimiento involucrados. A lo largo de las etapas que integran la formulación y elaboración de las políticas públicas se encuentran áreas de oportunidad para las IA que fueron identificadas por el CAF (Figura 1).

En cuanto a la formulación del problema que se busca atender, una adaptación de IA puede identificar tendencias para anticipar situaciones y pronosticar posibles resultados e impactos. Precisamente, la IA soluciona problemas complejos a partir de la identificación de un problema y su delimitación, identifica datos o características de un problema y plantea los resultados potenciales de una solución (Almonacid *et al*, 2020).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

Figura 1.

Fuente: CAF, 2022, p. 35.

Así mismo, se puede utilizar la IA para captar y analizar los intereses y preocupaciones de los ciudadanos o grupos de opinión, recogiendo resultados a partir de las redes sociales, encuestas o sondeos de opinión. La herramienta adaptable puede ser, por ejemplo, el procesamiento del lenguaje natural (CAF, 2022 p. 35).

Por lo tanto, dentro de los procedimientos de elaboración y formulación de las normas se deben desplegar herramientas de diverso tipo destinadas al entrenamiento en técnicas de definición de problemas, el establecimiento de objetivos de política, la identificación de soluciones alternativas, la evaluación de impacto y participación de las partes interesadas en el diseño e implementación del análisis de impacto normativo. Estos aspectos se deben centrar en prácticas de la vida real, por lo que pueden ser identificadas mediante el uso de tecnologías de IA.

De manera incuestionable se require explorarlas para que puedan incidir en la mejora de la formulación, ejecución y evaluación de las políticas públicas que se formalizan en la ley. Las ventajas que representa su uso en las diferentes etapas de la AIN irán dependiendo de su adaptación de las capacidades que ofrece esta tecnología a las necesidades de cada ejercicio de escrutinio. De acuerdo con las etapas del AIN al ciclo legislativo, puede incluirse IA en el ejercicio de todas las fases de evaluación de la ley.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

Figura 2.

Fuente: Elaboración propia

IV. Conclusiones

A través de la discusión de las limitantes de la AIN, y sus ventajas se han detectado diversas oportunidades de mejora de la calidad de la normatividad que puedan favorecerse y potencializarse a través del uso de tecnologías cognitivas provenientes de la IA.

El Análisis de Impacto Legislativo (AIN) se inserta como una nueva función en la dinámica parlamentaria en la forma de un sistema de vanguardia. La doctrina contemporánea la visualiza no solo como una herramienta de mejora en la calidad de la legislación, sino inclusive como una obligación basada en la responsabilidad del poder legislativo con relación a la efectividad, medida por los resultados e impactos, de las leyes que él mismo propone y aprueba.

Esta herramienta es conveniente para afinar y depurar los contenidos de una ley, proceso que por las premuras propias de la actividad legislativa pocas veces se realiza, incidiendo de manera determinante en la calidad legislativa, su efectividad, y en el fortalecimiento de la ley como instrumento de regulación social. Esto se logra en la medida en que suministra la retroalimentación necesaria para mejorar o enmendar la legislación que no logra cumplir su función.

La IA presenta una infinidad de oportunidades a explorar en los procedimientos de elaboración de las normas donde se pueden desplegar herramientas desde la formulación de los problemas a resolver con una intervención legislativa, o mediante un diagnóstico preciso que pruebe que hay otras alternativas de solución, con lo cuál ayuda a controlar la hiperinflación legislativa. Igualmente, puede apoyar de manera sistemática la función de monitoreo y seguimiento de la eficacia de las normas, con lo que se

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

pueden corregir los problemas de hipertrofia e hipostenia de los sistemas normativos en la actualidad.

Indudablemente, uno de los mayores impactos de la IA en la etapa de evaluación será la reducción significativa del tiempo de investigación al proporcionar acceso a información valiosa en tiempo real, requisito para prestar un servicio eficaz y eficente.

De manera similar, la consulta participativa como parte del AIN demanda un aprovechamiento de las ventajas de la interacción del binomio metodología-tecnología. La IA se perfila como un instrumento eficaz para captar la participación ciudadana y detectar los intereses y preocupaciones de los ciudadanos o grupos de opinión, exaltando su calidad de elemento fundamental del AIN para anclar la ley en la realidad.

La evaluación de la ley debe tener el objeto de convertirla en una profecía con pocas posibilidades de fallar. Sin lugar a dudas, los beneficios de la implementación de la IA como un principio de buena práctica de gobernanza y acceso a la participación en los procesos de análisis de impacto normativo, están aún por ser explorados y éticamente aprovechados.

Bibliografía

Almonacid, Juan Jorge (2022). Consulta participativa: Gran reto del Análisis de Impacto Normativo y la Inteligencia Artificial. *Revista Pluralidad y Consenso*, Instituto Belisario Domínguez, Senado de la República, México.

Almonacid, Juan Jorge y coronel, Y. (2020). Aplicabilidad de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado, *Revista de Derecho Privado,* Universidad Externado de Colombia, n.° 38, enero-junio 2020, 119-142, doi: 10.18601/01234366.n38.05.

Atienza, Manuel (1997). *Contribución a una teoría de la legislación*, Madrid, Tecnos. Consultado en https://www.researchgate.net/publication/304543443_Contribucion_para_una_teoria_de_la_legislacion

Caf (2022) *Conceptos fundamentales y uso responsable de la Inteligencia Artificial en el sector público*. Informe 2, Banco de Desarrollo de América Latina.

Bronfman, Alan (2006). *El sentido de la evaluación legislativa en los sistemas políticos democráticos*. En: La evaluación de las leyes. XII Jornadas de la Asociación Española de Letrados de Parlamentos.

Caballero, Rafael (2020). Apuntes metodológicos para evaluar la efectividad de una ley. *Boletín mexicano de derecho comparado*, 52(154), 411-423. Epub 12 de mayo de 2020. https://doi.org/10.22201/iij.24484873e.2019.154.14148

Carceller, Julia (2019), Análisis de impacto normativo sobre derechos y libertades fundamentales. *Papeles el tiempo de los derechos*, número 5, p. 4. ISSN: 1989-8797 https://redtiempodelosderechos.files.wordpress.com/2019/01/derechos-libertadesfundamentales-5-19.pdf

Crick, Bernard (1968). *En defensa de la política*, Madrid.

De vrieze, Franklin (2017). *Guía para el control post-legislativo de los parlamentos,* WFD, Londres.

Ehrman, Roberto (2018). *La evaluación de impacto legislativo: un programa para la mejora de los resultados de la legislación*. Cuadernos de Ciudad de México.

Gellner, Ernest (1984) El rasgo científico de las ciencias sociales. *Epistemology of Social Science*, ISSJ Unesco Vol. XXXVI, No. 4, 1984

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

Maniaki, Alexia (2022). *Experiencia desde el Parlamento Europeo en Evaluación de Impacto Normativo.* En: Senado de la República (2022) Memoria del Primer Congreso Internacional en Análisis de Impacto Legislativo, Instituto Belisario Domínguez.

Matallana, Silvia. (2020). *La construcción discursiva de la racionalidad jurídica.* En Cáceres, Nieto, Enrique. Pasos hacia una revolución en la enseñanza del derecho en el sistema romano-germánico, tomo 5. https://biblio.juridicas.unam.mx/bjv/detalle-libro/6227-pasos-hacia-una-revolucion-en-la-ensenanza-del-derecho-en-el-sistema-romano-germanico-tomo-5-version-electronica

Parra, Dario, Concha, Ricardo (2021). Inteligencia artificial y derecho. Problemas, desafíos y oportunidades, *Universitas,* vol. 70, Pontificia Universidad Javeriana.

Reveles Vázquez, Francisco (2017). Problemas de la representación política y de la participación directa en la democracia. *Estudios políticos (México)*, (42), 11-35. Recuperado en 24 de octubre de 2022, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-16162017000300011&lng=es&tlng=es.

Segura, Manuel (1998). *La racionalidad jurídica,* Madrid, Tecnos, 1998.

Valle-Cruz, D., Criado, I., Sandoval-Almazán, R. y Ruvalcaba-Gómez, E. A. (2020). Assessing the public policy-cycle framework in the age of artificial intelligence. From agenda-setting to policy evaluation. *Government Information Quarterly*, 37(4). https://doi.org/10.1016/j.giq.2020.101509.

Van ooijen, C. Ubaldi, B. y Welby, B. (2019). *A data-driven public sector: enabling the strategic use of data for productive, inclusive and trustworthy governance*. OECD Working Papers on Public Governance n.o 33. https://doi.org/10.1787/09ab162c-en

Weber, Max (1986). *Sobre la teoría de las ciencias sociales,* Barcelona, Ediciones Planeta-Agostini.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 9-22
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.02

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

El marco jurídico de la Unión Europea sobre protección de datos y garantías ciudadanas ante la Administración pública electrónica

EUROPEAN UNION LEGAL FRAMEWORK ON DATA PROTECTION AND CITIZENS' GUARANTEES TOWARDS ELECTRONIC PUBLIC ADMINISTRATION

Enrique Manuel Puerta Domínguez
CEU Cardenal Spínola
empuerta@ceuandalucia.es 0000-0003-1816-5703

Recibido: 24 de diciembre de 2022 | Aceptado: 11 de junio de 2023

RESUMEN

El presente estudio aborda, en clave analítica tanto de la legalidad europea como de la jurisprudencia del Tribunal de Justicia, las virtualidades aplicativas que tiene la normativa de la UE en materia de protección de datos en lo que afecta a las relaciones entre las Administraciones públicas y los ciudadanos. Tal normativa es exigente a la hora de deparar las obligaciones que competen a los que realizan el tratamiento o depósito de datos personales, y es de recibo que sean los entes públicos los que deban, antes que nada, dar ejemplo de una buena gestión. Materia rica y compleja, aun no ampliamente abordada, conoce una sugerente casuística jurisprudencial.

PALABRAS CLAVE

Protección de Datos
Administración pública
Unión Europea

ABSTRACT

This study addresses, in an analytical key both European legality and the jurisprudence of the Court of Justice, the application potentialities that the EU legal provisions have on data protection in what affects the relations between public administrations and the citizens. Such regulations are demanding when it comes to establishing the obligations that are incumbent on those who process or deposit personal data, and it is acceptable that public entities should, first of all, set an example of good management. Rich and complex matter, not yet widely addressed, is matter of such a suggestive case-law.

KEYWORDS

Data protection
Public Administration
European Union

I. NOCIONES PRELIMINARES; ADMINISTRACIÓN ELECTRÓNICA Y PROTECCION DE DATOS EN CLAVE RELACIONAL JURÍDICO-PÚBLICA

La Administración electrónica (también conocida quizás con matices más amplios y ambiciosos como e-Gobernanza) cubre un amplio campo de aplicaciones, entre las cuales, y sin ánimo de ser exhaustivos, podemos referir algunos ejemplos. El primero comprendería las relaciones de los usuarios con las entidades públicas fuera de sus dependencias presenciales al uso. Otro vendría deparado por la contribución de las Administraciones a la animación del debate público, y la consiguiente participación ciudadana, especialmente mediante la difusión de datos públicos esenciales mediante foros públicos, consultas en línea, y más ampliamente, los nuevos mecanismos de consulta a los ciudadanos. Por añadidura vendría al menos un tercer grupo de aspectos esenciales, identificado con las relaciones entre empresas privadas y corporaciones de naturaleza públicas.

Lo cierto es que tan pronto como la Administración electrónica proporcionó a los usuarios servicios tangibles, y que éstos a su vez han percibido como ventajas reales, otra cuestión, la de igualdad de acceso a los beneficios de la e- Gobernanza, emerge cada vez más agudamente. Tales circunstancias son las identificadas con la consabida brecha digital, por la cual la Administración electrónica parece quedar reservada únicamente a personas u hogares tecnológicamente equipados y conectados a internet. Caso de no disponerse de tales medios o habilidades otras soluciones han venido descartándose, tales como el acceso generalizado desde terminales interactivos en edificios administrativos o puntos de acceso público, bien desde cualquier mostrador o con la ayuda de un mediador. Dichas exclusiones son suplidas por la denodada entrega de ciertos servicios asistenciales, especialmente Trabajadores Sociales y Voluntarios, así como con arreglo al recurso intergeneracional deparado por los más jóvenes hacia los más mayores o menos tecnificados. Por lo tanto, un primer problema que debe resolver el de la e-Gobernanza es el de su eventual carácter discriminatorio o excluyente. Pero no es el único. Una vez garantizada la igualdad de acceso, quedaban otros muchos retos, que fueron desvelándose conforme avanzaba la implantación de la e-Gobernanza en el continente europeo.

Efectivamente, desde el comienzo del presente siglo todos los países de la Unión fueron poniendo en marcha programas más o menos ambiciosos. Ya en la lejana fecha de junio de 2000, los Jefes de Estado y de Gobierno adoptaron en el Consejo Europeo de Santa María da Feira el denominado "Plan de Acción e-Europa 2002". Dicha iniciativa dedicaba un capítulo a la Administración electrónica, en virtud del cual se asignaba a las diversas corporaciones públicas de los Estados miembros diversos conjuntos de objetivos a alcanzar, junto con un calendario. Desde entonces, los Directores Generales encargados de la Función Pública de los Estados miembros de la Unión Europea se han venido reuniendo con regularidad para abordar este tipo de cuestiones. En etapas posteriores se procedió principalmente a examinar temas de interés común; aquí se han tocado cuestiones como la identificación electrónica o firma electrónica,

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

las relaciones concernientes a la protección de datos de los europeos con respecto a autoridades de países terceros, etc.) Igualmente se procedió a calibrar los logros alcanzados en clave de mejorar las prácticas de la e-Gobernanza. Aun hoy se considera necesario ir mucho más allá del mero intercambio de puntos de vista para pasar a mecanismos de consulta real entre las Administraciones europeas, lo que pasa por su intercambiabilidad. Pero no es menos cierto que nos enfrentamos con todo este proceso al riesgo tangible derivado del hecho de que la tecnificación aliente tentaciones experimentadas por esos mismos poderes públicos encuadrados en tal e-Gobernanza global, y que podrían abocar a un manejo irresponsable o manipulador de los datos de los ciudadanos. E igualmente se produce el problema inverso, determinado por la enorme dificultad que para unas Administraciones estatales de base territorial supone dar respuesta a una cuestión como la del tratamiento de datos en un medio como internet, que es sustancialmente transnacional. Sobre estas inquietudes expresadas por los justiciables europeos, y las inexcusables garantías jurídicas que aquéllas suscitan, es como significativamente emerge cierta jurisprudencia del Tribunal de Justicia de la UE tocante a salvaguarda de datos personales en el entorno telemático, concretamente en lo concerniente a su trato por las Administraciones nacionales, y también de la UE, versa la presente aportación. Esta inquietud, que reflejamos y ponemos al día en la presente aportación, ya vino expresada por ciertos autores desde los primeros avances de las entonces nuevas tecnologías telemáticas, muy con concreto por las preocupantes resultas que de aquéllas se derivaban para la privacidad de datos. En concreto, se trataría de Problemas derivados de la misma naturaleza de la red, como la aplicación de una ley nacional a un fenómeno esencialmente transfronterizo o incluso la dificultad de conocer la verdadera identidad de los intermediarios, debido a la abstracción de los intercambios, posibilidades de alias y otros signos virtuales susceptibles de ocupar la verdadera personalidad de quién está al otro lado de una terminal (Andrieu; 2000, p. 155).

Consecuentemente, un especial interés suscita conocer (en el ámbito de las relaciones de los ciudadanos, y en cuanto a usuarios que somos de las tecnologías con respecto a las Administraciones) dónde exactamente han de centrarse las principales preocupaciones en materia de privacidad, protección de datos personales y gestión de la identidad. Se volvió necesario garantizar, en particular para los datos o aspectos más sensibles o más confidenciales, que solo la persona interesada pudiese manejarlos y realizar sus trámites en una relación protegida con respecto a las Administraciones públicas, y que éstas por su parte, respondiesen con un tratamiento que respetase idéntico nivel de confidencialidad. A estos efectos se entendió necesario codificar y asegurar los modos de acceso, así como repensar los sistemas de identificación y autenticación. Se tomó una cierta conciencia consistente en equilibrar la facilidad de uso, la ergonomía de los métodos de identificación y los niveles de seguridad. La introducción de la Administración electrónica debería en todo caso permitir a los ciudadanos guardar el control sobre sus datos personales. En este sentido, podría posibilitarse un ejercicio en línea, e incluso en tiempo real, de los derechos de acceso y rectificación de los datos que la Administración tiene sobre los ciudadanos.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

La marcha hacia la e-Gobernanza y sus consecuencias se han podido observar comparativamente en todos los países de la OCDE. Las Tecnologías de la Información y Comunicación (TIC), también denominadas Nuevas Tecnologías (NN TT), han aportado mucho a la vida cotidiana, incluidas las relaciones jurídico públicas; pero también han creado no poca alarma social en cuanto a sus potencialidades negativas en caso de un empleo no idóneo. Cierto es que los puestos administrativos están cubiertos por seres humanos corrientes, y en cuanto tales, no son ni infalibles ni inmunes a toda circunstancia que ponga a prueba su virtud y probidad. Cuenta el viejo proverbio que no existe mejor prédica que el ejemplo; en consecuencia, y por lo que atañe a una cuestión tan controvertida como la protección de los datos personales a través del medio telemático, deberán ser pues las Administraciones públicas las que, en su manejo, deberán ostentar los índices de mayor transparencia y salvaguarda con respecto a los ciudadanos. La preocupación por la privacidad, correlativamente a la proliferación de datos que circulan de forma mucho más fluida, también se está trasladando de las entidades públicas a las empresas.

Un primer hito significativo fue deparado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos reflejó en su momento esta nueva percepción de los riesgos. En aquellas fechas, algunos autores (Guadamuz; 2000, p. 3), propusieron inclusive el término *Habeas Data* rememorando el tradicional *Habeas Corpus* en lo tocante a la necesidad de mantener la privacidad de su titular en las relaciones informáticas, preocupándose muy especialmente en recalcar que el sistema europeo de protección de datos imponía una carga al resto del mundo al imponer restricciones a la transferencia de datos a países que no cuentan con ningún tipo de protección de la privacidad.

La tendencia en la UE se vio consolidada por la aprobación del actual Reglamento 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 (y que denominaremos a partir de ahora RPD). La literatura científica sobre este instrumento es inmensa, destacando tal vez por sus mayores preocupaciones en el terreno de su impacto en el entorno internet y de cara a las Administraciones públicas, especialmente en lo que atañe a su proceso de elaboración, y al modo en que el Legislador europeo muestra con cierto orgullo la experiencia de aprendizaje recibida a lo largo de las casi dos décadas que median entre ambos instrumentos (Brunet; 2016, p. 567).

Desde el prisma de la técnica legislativa se confirma una vez más el proceso de paulatina sustitución en la construcción jurídica europea del instrumento de la Directiva, característico del S. XX, por el del Reglamento en el presente S. XXI. A lo largo del presente estudio podremos calibrar hasta qué punto dichas normativas, como apuesta europea en la materia (y en contraposición a la filosofía de otras partes del mundo, concretamente EE UU, por no hablar de la policía informática exhaustiva existente en la R. P. De China), tienen mucho que aportar en las relaciones entre la Administración electrónica

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

y los ciudadanos, existiendo ya al respecto una no muy abundante, pero sí significativa aportación jurisprudencial a cargo del Tribunal con sede en Luxemburgo.

La gran cuestión inicial versa en concreto hacia qué clase de Administración electrónica se está tendiendo como meta deseable. La idea generalmente compartida es que acabasen siendo realizables únicamente en línea, como así ha sido finalmente, todos los trámites administrativos para personas físicas, asociaciones y empresas, así como el pago de impuestos y seguridad social, entre otros. El objetivo habría sido el de garantizar gradualmente que cada usuario se beneficiase de las TIC en las transacciones con los servicios públicos, y consiguientemente pudiese, (superadas todas las discriminaciones propias de la brecha digital), acceder de forma sencilla y rápida a toda la información y ayuda personalizada sobre servicios públicos y trámites administrativos. Ello incluiría muy especialmente el seguimiento de sus archivos, la definición de calendarios provisionales personalizados, la recepción de recordatorios por correo electrónico el acceso a todos sus trámites anteriores, así como almacenar en línea (a plena discreción y con total seguridad), los resultados desmaterializados resultantes de estos. También podrían los ciudadanos ejercer en línea su derecho de acceso a sus datos personales de los que disponga toda entidad pública, para en su caso, estar al corriente de toda modificación que se produzca con arreglo a toda información que le concierna, y que se halle en poder, o resulte intercambiada entre las diversas Administraciones cuando interactúen con relación a unos mismos ciudadanos.

La e-Gobernanza, en aplicación de todos los deseos o metas acabados de expresar, se construiría a partir de una serie de mecanismos técnicos que, no sólo habrían de dar la talla en términos de mera operatividad técnica, sino además ser capaces de propiciar unas garantías básicas, como serían las de una identidad fehaciente de los ciudadanos o administrados, así como la de un acceso generalizado sin discriminaciones y en salvaguarda de la intimidad representada en sus datos personales. Serían pues unos requisitos técnicos, debidamente fiscalizados (sin exceso ni defecto) respecto de la normativa europea de protección de datos, en lo que atañe al vínculo entre la Administración electrónica y los e-gobernados.

II. CUESTIONES ESPECIALMENTE DEBATIDAS EN MATERIA DE ADMINISTRACIÓN ELECTRÓNICA Y PROTECCIÓN DE DATOS

Toda esta realidad trata de dar respuestas a una serie de inquietantes cuestiones de base, que están en el centro de la implantación y consolidación de la Administración electrónica y sus límites respecto a la salvaguarda de los datos personales del usuario o administrado. Una cosa es desear aspectos como eficacia y prontitud en los servicios, y otra bien distinta asumir hasta qué limites o riesgos son asumibles en todo este proceso. Corresponde pues al Legislador establecer una normativa que asegure el equilibrio. Y en ese debate a la hora de legislar aparecen toda una serie de cuestiones, las cuales son objeto de vivos debates, y que, como veremos, determinan unas pautas diferentes en cuanto a su tratamiento y respuesta según nos ubiquemos a una u otra orilla del Atlántico.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

2.1. El debate sobre la propiedad por parte de los administrados de los datos que les conciernen y que son manejados por las Administraciones

Mientras que la legalidad en materia de protección de datos otorga a las personas unos derechos de acceso, comunicación, rectificación y oposición a sus datos, que a decir verdad en gran parte siguen aún siendo relativamente teóricos, la realidad de la sociedad de la información contempla la recogida y venta de datos con fines comerciales, hasta el punto de que el principal derecho a los datos a veces parecen ser un derecho de propiedad. De prevalecer tal análisis, los cauces de la actividad administrativa *online* y su régimen de control podrían sufrir determinados efectos de parálisis o confusión. De hecho, esto justificaría un enfoque contractual del control de los individuos sobre sus datos, y pondría en entredicho el control ejercido sobre el tratamiento administrativo, que es protector pero también restrictivo para los usuarios y para las corporaciones públicas. Es por esto que debemos preguntarnos cómo se deben analizar jurídicamente los derechos de los usuarios sobre sus datos.

Es tentador a primera vista considerar a las personas como titulares de un derecho real de propiedad sobre sus datos. Efectivamente, aparece enormemente extendida la convicción según la cual, con arreglo a los modelos económicos implantados desde la web en el entorno de los negocios privados, las personas ceden o "venden" sus datos personales, en particular a cambio de servicios gratuitos. Y es cierto que si se debe reconocer un derecho de propiedad sobre los datos personales, este derecho de propiedad debe conferirse más bien a la persona a la que conciernen los datos que al titular de la base de datos. Esta es una excepción al principio de que la información pertenece a la persona que la recopila o formula. En efecto, los datos personales que las Administraciones pueden tener sobre los usuarios (nombre, fecha de nacimiento, domicilio, situación familiar, incluso base imponible o contenido de los antecedentes penales) son datos objetivos, que las corporaciones públicas se limitan a registrar sin añadir una apreciación subjetiva que justificaría una apropiación por su parte. Si existe un derecho de propiedad sobre los datos personales, por lo tanto, solo puede ser el de la persona interesada.

En cualquier estado de causa, argumentos serios llevan a rechazar esta idea de un derecho de propiedad sobre los datos personales. Los datos personales en su contexto telemático, que se basan en una base objetiva, no pueden ser modificados a voluntad por el interesado, salvo, por supuesto, que la modificación de los datos corresponda a una modificación en la situación objetiva correspondiente (domicilio, nombre, etc.). Para un derecho real de dominio ha de existir necesariamente un elemento de libre disposición de la propiedad. No obstante, en la etapa de su formulación, estos datos no son más obra del interesado que de la Administración. Así las cosas, semejante formulación depende de la Ley, o bien se adjunta automáticamente a los actos del sujeto (adquisiciones de bienes inmuebles, estado de cuentas bancarias, etc.). Además, la idea de un derecho de propiedad no es en la que sirve de base a la legislación sobre tratamiento de datos y libertades, la cual aparece mucho más centrada en una perspectiva

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

de protección de las libertades. Este enfoque estaría mucho más cerca de un enfoque estadounidense que europeo, en donde no acaba de cerrarse el sempiterno debate, según el cual, los datos personales pueden asimilarse a un derecho de propiedad susceptible de compraventa. En Europa sin embargo los datos se identifican con derechos humanos, los cuales nunca pueden ser objeto de transacciones. Probablemente la óptica europea tampoco llegue a servir para prohibir aquellas prácticas consistentes en remunerar el tiempo que las personas dedican a comunicar la información que interesa a los administradores de bases de datos. Pero esto prohíbe que la comunicación de datos sea considerada como la transferencia de un derecho de propiedad sobre ellos. Consecuentemente la transferencia a la Administración de datos personales no es puramente discrecional y no puede analizarse desde una perspectiva contractual. Puede imponerse como requisito de la comunidad para hacer posible la vida en común, en una lógica similar a la que está en la base de la tributación.

Con todo, el análisis más riguroso parece conducir, por tanto, a analizar los datos personales no en términos de derechos patrimoniales sino en términos de atributos de personalidad. Debe pues estimarse que, si bien el titular de los datos no es el autor de la información, en el sentido de formato, es el legítimo poseedor de sus elementos. Su vínculo con el individuo es demasiado estrecho para que no sea de otro modo. Cuando el sujeto de los datos es un sujeto de derecho, la información es un atributo de personalidad. Este carácter de atributo de personalidad implica que la comunicación de la información debe derivar o del consentimiento del interesado o de obligaciones legislativas o reglamentarias. Y más allá del debate doctrinario, todo el reto que atañe a la protección de los datos personales de los ciudadanos respecto a la e-Gobernanza consiste entonces en garantizar las condiciones suficientes para que las personas controlen estos datos, reconociendo su derecho real a determinar el uso que debe hacerse de los datos personales en posesión de las Administraciones. Es la puesta en práctica de la teoría de la autodeterminación informacional, por la cual el tribunal constitucional federal alemán proclamó el derecho del individuo a decidir sobre la comunicación y uso de la información relativa a su persona.

2.2. El debate acerca de los límites a los que debe sujetarse el principio de control de los datos personales en la implementación de la e-Gobernanza

El principio de control de los datos personales no puede ser absoluto, y toda pretensión encaminada hacia tal concepción ha de desestimarse como alejada de la realidad. En todo caso la potestad de supervisión habría de ejercerse, por lo que concierne a tan compleja zona de apreciación, en aquellos casos o situaciones en los que la decisión de comunicar o no determinados datos personales, de autorizar su transmisión de una Administración a otra puede dejarse ventajosamente a la iniciativa personal. En semejante zona de laxitud, correspondería a cada persona decidir libremente, según las ventajas que espera o los riesgos que teme, comunicar o no sus datos, lo que

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

incluye asimismo la opción de autorizar o no a la Administración que posee los datos que le conciernen para que los transmita a otra corporación pública, o inclusive a terceros ajenos al marco jurídico público. El principio de control de los datos personales no puede impedir la consecución de fines de interés público o que tengan carácter obligatorio: determinados procedimientos, formularios o recogidas de información por parte del Estado tienen carácter obligatorio. Y de otro tanto, la difusión incondicionada de datos estaría también limitada por las reglas genéricas que estarían de aplicar las oficinas generales supervisoras en la materia de protección de datos designadas por los Estados miembros, destinadas a proteger a las personas, en particular a las más vulnerables, contra la excesiva intromisión de los entes públicos respecto de los ciudadanos.

Desde luego el control sobre datos personales ha de ser un ámbito necesario, pero que debe enriquecerse y detallarse. Debemos considerar que, para salvaguardar la privacidad, todo sistema regulado de protección de datos debe obedecer a un doble enfoque: por un lado, un marco de "arriba hacia abajo", con esquemas de autorización proporcionada por los organismos supervisores específicos, destinados a la creación de archivos administrativos, y por otro lado, que se posibiliten derechos reconocidos a los usuarios para un control "de abajo hacia arriba", con el fin de verificar la licitud del tratamiento y la veracidad de los datos (derechos de acceso, comunicación, rectificación y oposición). En la práctica, es el primer enfoque el que mayoritariamente ha prevalecido. En efecto, el tratamiento de datos se examina rigurosamente en la fase de su creación, pero, y esto es quizás una muestra de confianza en este control, el ejercicio directo de sus derechos por parte de los usuarios se ha mantenido en gran medida teórico. Ello ha determinado pues que los derechos de acceso, comunicación y rectificación se hayan extendido como una potestad irrenunciable del ciudadano en cuanto a administrado telemático. Con el desarrollo de la Administración en línea, ha resultado posible enriquecer estos derechos de los ciudadanos, de modo que permitan un control real de los datos por parte de las personas. Dicho control ha venido significando para los usuarios un acceso real en línea a los sistemas que contienen datos sobre ellos, no solo para verificar su exactitud, sino también para obtener su comunicación en forma digital. Por ejemplo, tal como la cuestión está configurada actualmente, si el acceso y la comunicación por ejemplo de los expedientes de los titulados universitarios tiene como único fin comprobar su exactitud, un derecho de comunicación permitiría a este titulado obtener una copia digital de su título para adjuntar a su currículum. o registrarse en línea para una competencia administrativa. Es pues la operatividad creativa del ciudadano frente a las e-Administradores una fuente inagotable tanto de nuevos retos como de innovaciones relacionales entre unos y otros.

En consecuencia, se trata sólo de una transposición a la sociedad de la información de la práctica de comunicar documentos justificativos. Por lo tanto, si el objetivo ya es perceptible, quedan por definir los métodos de su implementación. Se trata de que este derecho de disposición de los datos, que por su naturaleza implica un consentimiento del interesado ejercido por éste, que aleja ya de toda idea

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

de coacción o de procedencia de consentimiento extorsionado propiciado desde los poderes públicos. Si se trata de una autorización otorgada a una Administración para que otra comunique información, semejante aquiescencia debe ser precisamente delimitada, revocable y ejercida bajo el control de organismos independientes en materia de protección de datos. Aun quedando muchas dudas irresueltas, resulta no obstante concebible que puedan surgir nuevos equilibrios que permitan un control real de las personas sobre sus datos los cuales, lejos de atenuar los controles existentes, pueden ser un cauce susceptible para que les sean reconocidos nuevos derechos.

Tampoco la e-Gobernanza debe pretender, ni puede tener como resultado, permitir a la Administración aumentar el nivel de control y vigilancia de los ciudadanos. El desarrollo de una potestad pública electrónica plena no debería tener por objeto recabar nuevas informaciones sobre los usuarios de manera continuada. El reto consiste, por el contrario, en dar acceso a los usuarios a los datos que les conciernen y que actualmente existen en los sistemas de información de las Administraciones. Todos estos servicios en ningún aumentar así el conocimiento que aquéllas tienen sobre el usuario. Por otro lado, tampoco es menos cierto que aumentan el conocimiento que el propio usuario tiene de lo que le preocupa respecto de la actividad que sobre él ejercen los poderes públicos, mejorando así su autonomía y su capacidad de acción.

Llegados a este punto cabe interrogarnos acerca de si podría hacerse plenamente operativo el principio según el cual todo acceso o modificación de datos personales relativos a un usuario en bases de datos públicas debe dar lugar a una notificación. La reforma de los sistemas de información permite hacer efectivo el derecho a la información. Los ciudadanos deben tener plena visibilidad de la gestión de la información que les concierne por parte de la Administración. De este modo, el ciudadano debería estar en condición de responder a cierta clase de preguntas cuando le asaltan ciertas dudas acerca del tratamiento de su intimidad y datos en el curso de la e-Gobernanza: ¿Quién consultó qué cosa? ¿Cuándo se hizo, y cuáles fueron los motivos para tal consulta? ¿Quién duplicó qué informaciones, cuándo y con qué propósito? ¿Quién modificó la información, en qué fecha, por qué razones y cuáles son las consecuencias dentro de la Administración competente y dentro de las Administraciones usuarias? La Administración tendría a renglón seguido la obligación de informar al ciudadano de estas modificaciones. Cabría plantearse que esta obligación de notificación reviste perfiles diferenciados según el grado de sensibilidad de los datos en cuestión, o incluso según el "ciclo de vida útil" de los datos. A decir verdad, ciertos datos se modifican con frecuencia mientras que otros están inactivos en los sistemas. de información. Es posible prever la obligación de notificar cada modificación. Esta notificación también puede ser mensual o anual. Entonces tomaría el carácter de una "evaluación informativa". Esta notificación permitiría ejercer el derecho de rectificación, si el usuario encuentra que la modificación ha inducido a error.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

III. SUCINTA APROXIMACION A LOS SISTEMAS LEGALES COMPARADOS; CONTRASTE ENTRE ESTADOS UNIDOS Y LA UNIÓN EUROPEA

En los entornos tecnológicamente más avanzados y libres, como son Estados Unidos y la Unión Europea, las claves se plantean en términos del grado de complementariedad que debe existir entre la ley y la tecnología en la protección de la privacidad en el medio telemático. Se hace omisión de aquellos países carentes de un régimen libertades homologable, en los que (como sucede actualmente en la R. P. China), la privacidad ciudadana prácticamente no existe, siendo precisamente la tecnología el medio característicamente más empleado por el poder político para fiscalizar hasta límites intolerables áreas que deben quedar reservadas a la intimidad y libertades de los ciudadanos. Casi desde los inicios de las TIC muy pronto surgió la idea de que aquéllas, lejos de ser una vía de intromisión de los poderes hacia los ciudadanos (como también lo ha sido) podrían por el contrario ser la mejor defensa frente a la curiosidad de las fuerzas de orden público y demás poderes del Estado, así como de cara a los más poderosos agentes económicos. Fue por supuesto en los Estados Unidos, donde en ausencia de un marco verdaderamente protector, tomó forma esta perspectiva de protección a través de la tecnología. Esta acepción combina dos características sobresalientes de la civilización estadounidense cuales son la fe tanto en la tecnología como en la responsabilidad individual (todo el mundo tiene un derecho de autoprotección). En esta búsqueda de tecnologías de protección de la privacidad, sin duda resultaba necesario distinguir entre aquellas cuyo uso depende directamente del usuario (criptografía), aquellas otras que son implementadas por proveedores de servicios especializados (como son aquellos que ofrecen garantizar un sano anonimato que salvaguarde la intimidad de los usuarios de cara al mundo telemático), y finalmente aquellas que formarían parte de la arquitectura de redes y sistemas. Se buscaron así nuevos principios como los relacionados con consentimiento hacia la disposición de datos personales, pero basados no en la legislación, sino en tecnologías accesibles y manejables por los usuarios. Tal es el ejemplo del conocido como estándar P3P, que permite a los usuarios de internet reconocer automáticamente la política de protección de datos del sitio cuando se conectan a un sitio. De la protección "individual" o "de mercado" (encomendada a los proveedores de servicios), se habría pasado, con el citado P3P, a una forma de protección colectiva. Por lo tanto, al otro lado del Atlántico ha venido existiendo un interés creciente en la idea de que los principios de privacidad deben incorporarse a la arquitectura de los sistemas técnicos como un código de conducta cuyos modos de empleo han de estar en todo caso en los ciudadanos. Para los juristas estadounidenses que teorizan alrededor de este enfoque consistente en incorporar el derecho a la tecnología (la tecnología hace que el derecho sea exigible), corresponde al debate público y, en última instancia, a la autoridad política, establecer objetivos; será pues la labor de los ingenieros de programación y de las empresas para traducir estos objetivos en la operación de las redes.

El modo americano se tradujo en su momento en una fuerte tentación de optar por la concepción americana de protección individual (protegerse a sí mismo) frente

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

a la concepción europea de protección por el Derecho legislado y más estandarizado en lo que competía a la protección de datos en el medio telemático, inclusive en las relaciones entre las Administraciones y los ciudadanos. Por ejemplo, durante el debate en Alemania sobre la transposición de la Directiva de protección de datos de 1995, con internet cada vez más adentrado en la vida de los ciudadanos, la llamada escuela de la "modernización ofensiva" (a la que pertenecían los comisionados federales y estatales de protección de datos) pretendía propiciar una reforma sustancial de la legislación alemana, con vistas a mejorar la protección previstas actualmente en su legislación. Esta misma escuela reivindicó la libertad de la criptografía, alegando que cada vez será más responsabilidad de los ciudadanos protegerse mediante el uso de software de criptografía. Sin embargo, estas pulsiones parecen en Europa, al menos por el momento, ampliamente conjuradas o en declive. En concreto en lo que afecta a la UE, como super-Administración pública que ejerce sus competencias decisorias en el territorio de sus Estados miembros (de cara por supuesto a todas sus instancias administrativas y gubernativas, e inclusive con pretensiones de extender sus prerrogativas por lo que afecta al exterior, cuando son intereses de ciudadanos europeos los que resultan afectados) quedaba asumido que se debería contar con una normativa suficiente para tan trascendental misión, y hacerla cumplir de cara a las autoridades nacionales y, como no, respecto a sí misma. Ello ha sido el elemento originario de toda esa preocupación posterior, la cual habría constituido (en teoría) una prioridad irrenunciable para las autoridades tanto de la propia UE como de sus Estados miembros, matices estos que se preocupa en recalcar cierta doctrina especializada ya citada, no sin cierto escepticismo en cuanto a la coherencia entre intenciones iniciales y resultados efectivamente alcanzados (Brunet; 2019, p. 117).

IV. LÍNEAS RECTORAS DE LA NORMATIVA DE LA UNIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS Y SU APLICACIÓN A LA ADMINISTRACIÓN ELECTRÓNICA

El estilo finalmente triunfador entre nosotros fue obviamente, el de origen netamente europeo, es decir, de confiar la tutela a procedimientos legales y con supervisión judicial en vez de que los administrados fueran ellos los que se autodefendiesen con instrumentos tecnológicos adecuados. Pero ello no quiere decir que el entramado legislativo en su aplicación a las relaciones con los e-administrados, estuviese carente de problemas concretos muy acuciantes, fruto precisamente de este prurito garantista. Cierto es que, desde el plano normativo desarrollado por las instituciones europeas, las cuestiones de la protección de datos revistieron, siempre en este estilo à *l'européenne*, un especial interés, a caballo de dos disposiciones trascendentales, que si bien no exclusivas del ámbito telemático, han deparado respecto de dicho entorno un trascendental impacto. Tales fueron inicialmente la Directiva de 1995 de Protección de Datos, la cual resultaría reemplazada por el vigente RPD. A tenor de lo acabado de afirmar, conviene partir del elemento central de la norma europea actual, esto es, del concepto de dato personal.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

De conformidad con el art. 4.1 del RPD, se define dato personal como cualquier información relativa a una persona física identificada o identificable (esto es, cada interesado); el citado instrumento especifica además que la persona física que puede ser identificada, directa o indirectamente, con especial referencia a un identificador como el nombre, un número, se considera identificable la identificación, los datos de ubicación, un identificador en línea o uno o más elementos característicos de su identidad física, fisiológica, genética, psíquica, económica, cultural o social. Cabe señalar que esta lista es meramente un ejemplo y no es exhaustiva. Además, se presta especial atención a los datos obtenidos mediante identificación tecnológica incluyendo la localización a través de la I.P. A ello hay que sumar el particular cuidado en relación con los datos genéticos, biométricos y de salud. Estos datos junto con los datos fiscales, judiciales o cualesquiera otro de índole pública generados en desde las diversas Administraciones se incluyen íntegramente en los datos personales particulares.

Un segundo concepto esencial es el de tratamiento de datos. El RPD define el concepto de tratamiento de cualquier operación o conjunto de operaciones, realizadas con o sin la ayuda de procesos automatizados y aplicadas a datos personales o conjuntos de datos personales, tales como la recolección, registro, organización, estructuración, almacenamiento, adaptación o modificación, extracción, consulta, uso, comunicación por transmisión, difusión o cualquier otra forma de puesta a disposición, comparación o interconexión, limitación, cancelación o destrucción. Fundamental es el concepto de elaboración de perfiles, que se define como cualquier forma de tratamiento automatizado de datos personales consistente en la utilización de dichos datos personales para evaluar determinados aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relativos al desempeño profesional, la situación económica, salud, preferencias personales, intereses, confiabilidad, comportamiento, ubicación o viaje de esa persona con entidad natural. A la luz de la definición anterior, una cadena de tiendas que adquiere información o realiza acciones para comprender mejor los intereses, preferencias, lugares frecuentados o posibilidades de gasto de una persona está realizando una actividad de elaboración de perfiles. A nadie le es extraño que las Administraciones son las primeras entidades que, con la excusa de mejor ajustar el buen gobierno y aplicar por ejemplo las mejores políticas presupuestarias, elaboran amplios y detallados perfiles estadísticos entre las diversas clases de administrados. Este aspecto es puesto de relieve de entrada en la Exposición de Motivos del RPD, la cual aborda la cuestión del interés público en lo concerniente al tratamiento de datos[1]. A mayor abundamiento, tal especificidad también es evidente en el tratamiento de datos sensibles. El principio de prohibición de tratamiento de tales datos, establecido en el art. 9.1 del RPD, encuentra muchas excepciones en el 9.2. Ya en el ámbito de la cooperación policial y judicial, donde el consentimiento de la persona tiende a ceder completamente el paso al único control de legalidad y proporcionalidad por parte de la autoridad pública (Gambardella; 2017, p. 63). En conclusión, la creación de un derecho de protección de datos para el tratamiento de los datos necesarios para el ejercicio de las prerrogativas del poder público podrá por tanto, fomentar la aparición de características específicas y reglas ajustadas. Por lo tanto, hay mucho en juego porque según

las normas jurídicas aplicables a los derechos concedidos a los particulares variarán. El riesgo de tal especificidad es entonces, al dejar de ser materia de derecho de la Unión y la conformidad que implica, excluir todo un régimen jurídico de protección de los derechos fundamentales (Gambardella; 2017, p. 65).

Por lo tanto, es una relación jurídico administrativa la que se construye con respecto al tratamiento de datos cuando hay por un lado poderes públicos y por otro administrados, matices que, como veremos posteriormente, la jurisprudencia comunitaria ha tenido la ocasión de precisar [2]. En dicho modo relacional de naturaleza pública el ciudadano figuraría como presunto titular de sus datos (aspecto que como veremos en su momento, no está ni tan claro ni tan asumido), mientras que cada Administración concernida quedaría como responsable del tratamiento de esos datos. Tal relación debería en principio basarse, de acuerdo con el RPD, con arreglo a un principio de consentimiento en el tratamiento, expresado por dicho ciudadano, dado que un aspecto crucial en el tratamiento de datos personales es, precisamente, el relativo al consentimiento para dicho tratamiento. Es por tanto necesario obtener el consentimiento de la persona para procesar sus datos. Si alguna entidad dispone de datos para los que no se ha prestado o solicitado previamente el consentimiento, será conveniente que contacte con el interesado y le pida dicha conformidad de forma expresa. En su art. 7.2 el RPD especifica a continuación que si el consentimiento del interesado se da en el marco de una declaración escrita que también se refiere a otras cuestiones, la solicitud de consentimiento se presenta de forma claramente diferenciable de los demás aspectos envueltos, de forma comprensible y de fácil acceso, utilizando un lenguaje sencillo y claro. Lo que sucede es que este aspecto suele cada vez más automatizarse por mecanismos de *click wrapping*, como el de aceptación de *cookies* del sitio, en los cuales se juega a menudo con el acto reflejo y no debidamente meditado por el usuario o administrado. Lo deseable tratándose de una relación jurídico-pública que ha de ser transparente sería que fuese imprescindible solicitar al usuario el consentimiento expreso para el tratamiento de datos en una pantalla específica del sitio web, posiblemente mediante la inserción de un botón independiente, sin confundirlo, ni insertarlo, con otros elementos diferentes. Si los datos han sido adquiridos previamente, solicitar de nuevo el consentimiento para el tratamiento. También será conveniente revisar la información facilitada al usuario sobre el uso de los datos ya que el responsable del tratamiento está obligado a indicar de forma clara y expresa para qué finalidades tratará los datos. En todo caso, y como contrapunto a lo acabado de afirmar, es también en la Exposición de Motivos del RPD donde hallamos menciones a ciertos casos o facetas particularmente sensibles con respecto de la actividad administrativa, en las cuales debe haber una óptica de salvaguardia del interés general frente al otro bien jurídicamente protegido de la intimidad, y por añadidura, del consentimiento prestado por parte de los sujetos particulares afectados [3].

El tratamiento de datos debe reportar una conciencia de responsabilidad para aquel que verifica el tratamiento, lo cual implica a su vez dos nociones, la del principio de responsabilidad en el tratamiento y la del titular de dicha responsabilidad, esto es, el responsable del tratamiento. La conformación del principio de responsabilidad constituye una de las novedades más importantes del RPD. Sobre la base de este principio,

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

el controlador de datos, o la persona que adquiere los datos del usuario, implementa medidas técnicas y organizativas adecuadas para garantizar y poder demostrar que el procesamiento se lleva a cabo de conformidad con el instrumento normativo europeo que ahora nos ocupa (art. 24.1). También es la persona responsable de garantizar y comprobar el cumplimiento de los principios relativos al tratamiento de datos personales, establecidos en el art. 5.1 (por ejemplo, licitud, corrección y transparencia, imitación de finalidad, minimización de datos, etc.).

Por su parte el art. 4.7 del RPD define al responsable o encargado del tratamiento como cualquier persona física o jurídica, autoridad pública, servicio u otro organismo que, individualmente o junto con otros, determine los fines y medios del tratamiento de datos personales; cuando los fines y medios de dicho tratamiento estén determinados por el Derecho de la Unión o de los Estados miembros, el responsable del tratamiento o los criterios específicos aplicables a su designación podrán ser establecidos por el Derecho de la Unión o de los Estados miembros. El RPD apoya al controlador de datos, al procesador de datos o a la persona física o jurídica, autoridad pública, servicio u otro organismo que procese datos personales en nombre del procesador de datos, así como también establece la posibilidad, siempre con el debido control, que se puedan estipular acuerdos puntuales y específicos en relación con el tratamiento de datos entre cada controlador de datos (la empresa o entidad pública titular del tratamiento) que pretenda externalizar el tratamiento de datos personales, y el encargado del tratamiento (el proveedor de servicios externalizados, ya sea un *outsourcer* tradicional o un proveedor de servicios en la nube). A mayor abundamiento, el art. 28.3, del RPD establece que el contrato vinculante para el responsable del tratamiento debe prever en particular: a)- la obligación de tratar los datos únicamente de acuerdo con las instrucciones a las que el responsable deba atenerse (y que deberán estar debidamente documentadas y recibidas por aquél), incluso en caso de transferencia de datos fuera de la Unión Europea; b)- la obligación de garantizar que las personas físicas autorizadas para realizar las actividades de tratamiento estén sujetas a obligaciones de confidencialidad, asumidas contractualmente o establecidas por la ley; c)- la obligación de tomar las medidas requeridas de conformidad con el art. 32 del RPD, es decir, las medidas técnicas y organizativas de protección de los datos que se consideren adecuadas para garantizar un nivel de seguridad adecuado al riesgo inherente al tratamiento [4].

Completa el cuadro de personaje implicados en el correcto tratamiento de los datos el Delegado de Protección de Datos o D.P.O., como agente especialmente designado por el responsable del tratamiento para desempeñar funciones específicas en clave de correcto empleo y gestión de los datos. El D.P. O. constituye una figura, parcialmente novedosa y propensa a deparar no poca confusión tras la adopción del RPD [5]. La empresa (y por analogía, el servicio público competente) deberá dotarle de estructuras, medios técnicos y económicos y equipos proporcionales a su cometido. Las funciones del D.P.O. están previstos en los artículos 37 y 39 del RPD y entre los más relevantes se encuentra el deber de informar y asesorar al Responsable del tratamiento y a sus empleados respecto de la legislación de la Unión y de los Estados individuales sobre la materia, verificar la implementación de la citada normativa, actuar como punto de contacto tanto hacia la Autoridad de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

Privacidad como hacia los usuarios, comunicar su opinión en relación con la evaluación de impacto en la protección de datos. Además, sin estar dentro de las funciones de regulación, puede tener encomendado el registro de las actividades de tratamiento.

V. ANALISIS SISTEMÁTICO DE LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UE EN LA MATERIA

Lo interesante es que al respecto disponemos de expresiones en las dos clases de modalidades de cuestiones prejudiciales que existen en el contexto del Derecho europeo, tanto en su variante interpretativa, como con relación a su modalidad de apreciación de validez, y que afectan, según las fechas, tanto a la derogada Directiva de 1995 como al vigente RPD de 2016. Las jurisprudencias anteriores son por lo general aprovechables en el contexto actual, pese a la diferente naturaleza normativa que presentan una y otra expresión del Derecho derivado. A este respecto cierta doctrina reivindica el papel del Juez comunitario como verdadero garante constitucional de los derechos de los administrados frente a las entidades públicas en lo que atañe a la protección de datos con arreglo a la normativa de la UE (Peyrou; 2015, p. 213), elemento que se reivindica como una expresión de un nuevo concepto de seguridad jurídica ligada a las NN TT (Tambou; 2020, p. 43).

Las cuestiones prejudiciales interpretativas responden a una doble problemática, de tal modo:

a) Tenemos desde un extremo casos en los que los particulares que ven limitadas por las Administraciones públicas competentes sus solicitudes de que les sean facilitados sus propios datos personales de los que aquéllas son depositarias. La idea central de todos estos pronunciamientos es que las limitaciones interpuestas por las Administraciones son admisibles, siempre que medie la debida proporcionalidad, nunca con carácter absoluto (criterio a la postre éste jurídicamente indeterminado y que el TJUE dirige al Juez nacional de reenvío) estando presentes ejemplos que afectan tanto a la Directiva[6] como al Reglamento[7]. Destaca en este contexto el refuerzo de la idea, según la cual la I.P. constituye un dato personal de primer orden emn cuanto a los imperativos de su tratamiento informático mediatizado judicialmente (Péronne/ Daoud; 2017, P. 120).
b) Como contraste, hallamos algún ejemplo disperso deparado por algún particular que se opone a las imposiciones que les remiten las autoridades nacionales de facilitar datos personales de terceros, teniendo como elemento dirimente al RPD. Vuelve aquí a imperar un consejo de proporcionalidad dirigido al Juez nacional encargado de entender de la causa[8].

No menos interesantes son los ejemplos recaídos en la variante, mucho menos frecuente de la apreciación de validez, en donde determinadas disposiciones de la propia Unión Europea son puestas en entredicho, para después ser destinadas a ser inaplicadas como inválidas, tras su contraste con respecto de la normativa de protección de

datos. Llaman en el contexto electrónico que afecta a las relaciones dos supuestos especialmente llamativos, que se suceden en contextos tanto internos [9] como externos a la propia UE, pero que afectan a ésta y que, por el devenir del tiempo conciernen tanto a la Directiva de 1995 como al actual RPD. Es aquí donde encuentran su ubicación los complejos avatares de las jurisprudencias Schrems I y II del TJUE, sobre la que tan abundantemente se ha escrito poniendo de relieve sus contradicciones y carencias a cargo de la doctrina tanto internacional (Castests-Renard; 2016, p. 88), como española (Uría Gavilán; 2016, p. 261) [10].

Conclusiones

Con la normalización del fenómeno de la Administración electrónica a múltiple nivel, también conocida como e-Gobernanza, las corporaciones de Derecho público han hecho soportar a los usuarios una nueva forma de complejidad administrativa, como así nuevos deberes en cuanto al tratamiento de sus datos, tanto personales como de terceros. El requisito de privacidad está lejos de ser la causa única o central de la complejidad administrativa construida alrededor de una cierta cultura administrativa basada en la desconfianza, que trata a los usuarios como posibles estafadores, y lleva a exigirles montones de documentos y certificados para justificar su situación. El surgimiento de las TIC, debido a que facilitan considerablemente el intercambio de información que hasta ahora era difícil y costoso de organizar, propicia un caldo de cultivo de colisión entre la eficiencia en la gestión, la seguridad colectiva y el mantenimiento de la privacidad e intimidad del ciudadano mismo. Y si bien queda demostrado que no procede considerar a los ciudadanos como propietarios, en el sentido romanista del término, de sus datos telemáticos en lo que atañe al entorno telemático, tampoco deja de ser admisible que, en correlativa muestra de pedagogía o ejemplo, también las Administraciones públicas deben poner su parte para facilitar una imagen respetuosa y responsable con esos mismos datos, en su rol de tratantes de los datos de los Administrados.

Resulta notoria la tarea de determinar los roles que incumben a las diversas Administraciones públicas nacionales de los Estados miembros de la UE, y que con un plus de exigencia serían contemplables desde el actual RPD. En este ámbito, la presencia de una más que incipiente o inicial jurisprudencia por parte del TJUE (que como hemos podido apreciar, oscila desde la idea de equilibrio y proporcionalidad en las cuestiones prejudiciales interpretativas, hasta un alto grado de exigencia en aquellas otras cuestiones prejudiciales en apreciación de validez, que llegan al extremo de anular inclusive Decisiones de la UE), constituye una vez más un elemento consustancial y necesario a este trascendental entorno, que comparte todos los rasgos y elementos característicos del engranaje jurídico comunitario. Siempre con este trasfondo proteccionista de la normativa europea hacia el administrado, si se quiere podemos transigir con que un nuevo pacto, a renegociar, estaría basado en la confianza de la Administración en los usuarios. La llamada E-Gobernanza también podría, en base a su conocimiento de situaciones personales, informar a los usuarios de los derechos que pueden ejercer. Todos estos

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

deseos deben ponerse a la luz de la compleja casuística analizada en los asuntos jurisprudenciales, contando con que el paradigma deparado por la legalidad ya no es de factura nacional, ni siquiera transponiendo en normas nacionales una Directiva como sucedía con la antigua norma de esta especie de 1995, sino que ahora contamos con un instrumento completo y obligatorio en todos sus elementos, el RPD.

1. Concretamente leemos en el Considerando 111: "Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o, si estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado".

2. STJUE de 9 de julio de 2022 recaída en el As 272/19, VQ contra Estado de Hesse.

3. Leemos en el Considerando 112: "Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, Administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados".

4 Teniendo en cuenta la naturaleza del tratamiento y la información de que dispone, la obligación de asistir al titular consiste: a)- en garantizar la protección de datos a través de medidas técnicas y organizativas apropiadas, de conformidad con el art. 32 del RPD; b)- en la notificación a la Autoridad de cualquier violación de datos (violaciones de datos) que se haya producido, de conformidad con el art. 33 del RPD; c)- en la comunicación a los interesados de las violaciones de datos que se hayan producido, en los casos previstos por el art. 34 del Reglamento; d)- en la realización de la evaluación de impacto exigida por el art. 35 del RPD; y e)- en consultar a la Autoridad, si la evaluación de impacto realizada indica que el tratamiento presentaría un alto riesgo en ausencia de medidas tomadas por el controlador de datos para mitigar el riesgo. Asimismo, el responsable del tratamiento tiene las siguientes obligaciones: primera, cancelar o devolver los datos, a elección del titular, en el momento de la terminación de la relación, salvo que la ley imponga obligaciones específicas de conservación; segunda, poner a disposición del titular toda la información necesaria para demostrar el cumplimiento

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

de las obligaciones establecidas en esta lista; y tercera, permitir al titular la realización de auditorías, directamente o a través de terceros designados al efecto.

5. Configurado en los arts. 37 y siguientes, su traslación al contexto público plantea amplios interrogantes, y eso que en esta normativa comunitaria se prevé la obligatoriedad del D.P.O. en una serie de casos, concretamente: primero, para todas las Administraciones públicas, incluidas las empresas privadas que realicen funciones publicitarias o ejerzan poderes públicos; y segundo, para todas las empresas que realicen un seguimiento regular y sistemático de datos a gran escala (geolocalización con fines estadísticos, análisis de consumo y preferencias, análisis de datos para publicidad dirigida) para quienes procesan datos relacionados con delitos y condenas penales. Cabe señalar que la lista no pretende ser exhaustiva y por tanto debe ser la empresa individual la que evalúe la conveniencia, en función de su tipo de actividad, de nombrar al D.P.O. No obstante, la designación de un D.P.O. sin duda puede constituir una medida importante para demostrar la adecuación y el cumplimiento del responsable del tratamiento en relación con las disposiciones del RPD. A diferencia del responsable del tratamiento y del encargado del tratamiento, el Delegado de Protección de Datos no puede ser una persona jurídica debiendo, necesariamente, siendo una persona natural, además debe reunir los siguientes requisitos; 1º)- poseer un conocimiento adecuado de la legislación y las prácticas de gestión de datos personales; 2º)- desempeñar sus funciones con total independencia y en ausencia de conflictos de intereses; y 3º)- para trabajar para el propietario o gerente o sobre la base de un contrato de servicios.

6. En primer término, y como precedente más remoto a nuestro entender de cuestión prejudicial interpretativa de la Directiva de 1995 en los contextos de litigios en materia de datos personales entre una Administración y un ciudadano, la hallamos la STJUE de 7 de mayo de 2009 Rijkeboer, As 553/07. Aquí el problema versa sobre las limitaciones en el periodo temporal respecto del cual el particular puede reclamar información sobre sus datos personales a la Administración. Sucedía que el interesado, con motivo de un traslado de domicilio, solicitó una relación de todas las comunicaciones a terceros de información relativa a él procedente de la base de datos de padrón municipal, efectuadas durante los dos años anteriores a su petición, y que versaban acerca de su domicilio antiguo. Unas comunicaciones, debe entenderse, que se realizaron por vía telemática. Sin embargo, la Entidad municipal limitaba dicha información a un año. El TJUE entendió que, si bien era competencia nacional, conforme a la Directiva, fijar un plazo suficiente, una normativa que limitaba la conservación de la información sobre los destinatarios al período de un año, limitando correlativamente el acceso a dicha información, si bien los datos se conservan durante mucho más tiempo, no constituía un justo equilibrio entre el interés tutelado y la obligación de mantener la intimidad de los sujetos que habían recibido dicha información. Según el TJUE el campo de aplicación de la entonces vigente Directiva 95/46 resultaba ser muy amplio, de manera que el concepto en sí de dato personal en lo que atañe a su tratamiento por los poderes públicos es muy diverso, y en cualquier caso cuando aquéllos son responsables del tratamiento su desempeño no puede resultar imposible o suponer un esfuerzo desproporcionado (Considerandos 59 a 61).

Un segundo ejemplo de análoga naturaleza lo tenemos en la STJUE de 12 de diciembre de 2013, en As 486/12. En ella vemos que un individuo identificado como X pretendía consultar su domicilio a efecto de notificaciones respecto a multas de tráfico, y veía limitado su derecho por una exigencia de cobro al respecto exigida por la Administración. Considerando la informatización que impera en toda la tramitación de las sanciones derivadas por infracciones de tráfico, un ciudadano multado quiere recurrir para no pagar la infracción aduciendo la posibilidad de que se le haya notificado a una dirección no actualizada o errónea. Con ese objeto solicitó al municipio donde residía la comunicación de sus datos de carácter personal de los años 2008 y 2009, en especial sus sucesivas direcciones y así fundamentar su recurso. Pero el Ayuntamiento reclamaba una tasa de 12,80 euros por suministrar dicha información. Es lo que el interesado intentó recurrir sin éxito ante el orden jurisdiccional administrativo neerlandés. En idéntica línea a la de la proporcionalidad el TJUE indica que la Directiva que no se opone a la percepción de gastos por la comunicación de datos de carácter personal por una autoridad pública. Eso sí, el importe de tales gastos no debe exceder el coste de la comunicación de dichos datos, siendo tarea del tribunal nacional competente realizar las verificaciones necesarias a tal efecto.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

Una tercera muestra que versa acerca de la interpretación de la Directiva de 1995 es la deparada por la STJUE Breyer de 2016 As 582/14. Aquí lo cuestionado es el procedimiento de recopilación sistemática por parte de las Autoridades alemanas de las IP de consulta de páginas de organismos federales por parte de los particulares con fines de seguridad. Ante ello el Sr. Breyer presentó, ante los órganos jurisdiccionales de lo contencioso-administrativo alemanes, un recurso con el objeto de que se prohibiera a la República Federal de Alemania conservar o permitir que terceros conservasen, al final de las sesiones de consulta de sitios accesibles al público de medios en línea de organismos federales alemanes, la dirección IP del sistema principal de acceso del Sr. Breyer, en la medida en que dicha conservación no fuera necesaria, en caso de fallo, para el restablecimiento de la difusión de esos medios. La jurisdicción nacional plantea si una dirección IP registrada por un prestador de servicios o de medios en línea en relación con un acceso a su sitio de internet constituye para éste un dato personal desde el momento en que un tercero (en este caso, un proveedor de acceso) disponga de los datos adicionales que permiten identificar al interesado, a lo que el TJUE respondió afirmativamente. Quedaba por averiguar pues las limitaciones a las que había que someter dicha actividad. Se entendió que la Directiva se oponía a una normativa de un Estado miembro con arreglo a la cual un prestador de servicios de medios en línea sólo podría recoger y utilizar datos personales de un usuario de esos servicios sin mediar el consentimiento de éste, cuando dichas recogida y utilización, entendiéndose necesarias para posibilitar y facturar el uso concreto de dichos servicios por ese usuario, fuesen más allá del objetivo de garantizar el funcionamiento general de esos mismos servicios.

7. Encontramos aquí la solitaria muestra que encarna la STJUE de 9 de julio de 2020 que en el As 272/19 enfrentaba al individuo designado como VQ al Estado de Hesse. Acontece que la Comisión de peticiones del Parlamento de un Estado Federado alemán, que se niega a suministrar las informaciones que posee de un determinado ciudadano, se la considera responsable del tratamiento, incluido el tratamiento informático por sus aplicaciones propias/ Además se define la noción de Autoridad pública a efectos del Reglamento, incluyendo a un organismo como la Comisión de Peticiones. En efecto, tras presentar una petición a la Comisión de peticiones del Parlamento del Estado Federado de Hesse, VQ solicitó a dicha Comisión, basándose en el artículo 15 del RPD, el acceso a los datos de carácter personal que le afectaban, y que consiguientemente quedaban registrados por dicha Comisión en el marco del tratamiento de su petición. El presidente del Parlamento del Estado Federado de Hesse decidió rechazar esa solicitud debido a que el procedimiento de petición constituye una función parlamentaria y que dicho Parlamento no está comprendido en el ámbito de aplicación del RPD. El 22 de marzo de 2013, VQ interpuso recurso ante el *Verwaltungsgerich*t Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden. El TJUE estima que el Reglamento 2016/679 no recoge definición alguna del concepto de "autoridad pública". Según el *Verwaltungsgericht*, a esa expresión se le puede otorgar una acepción funcional o una acepción institucional. Con arreglo a la primera de esas acepciones, serían autoridades públicas "todas las autoridades públicas que ejerzan funciones de Administración pública, incluido, por tanto, el Parlamento del Estado Federado de Hesse cuando lleve a cabo tales funciones. En tal línea la Comisión de peticiones del mencionado Parlamento es un organismo autónomo, y por tanto una autoridad pública, en el sentido institucional". Así las cosas, y con las consideraciones de autoridad pública expresadas por la jurisdicción contenciosa germana de reenvío, el TJUE responde que el art. 4.7 del RPD debía interpretarse, "en la medida en que una comisión de peticiones del Parlamento de un Estado federado de un Estado miembro determina, sola o junto con otros, los fines y los medios del tratamiento, esa comisión debe calificarse de responsable del tratamiento a efectos de dicha disposición, de modo que el tratamiento de datos personales efectuado por la mencionada comisión está comprendido en el ámbito de aplicación de dicho Reglamento, en particular de su art. 15".

8. En concreto se trataba de una obligatoriedad de remisión a Hacienda del número de bastidor de los vehículos que se vendían en un portal de internet gestionado por una empresa. En efecto, SS es un proveedor de servicios de publicación de anuncios en internet con domicilio social en Letonia. La Administración tributaria letona remitió a SS una solicitud de información en la que instaba a la citada sociedad a renovar el acceso de que disponía dicha Administración tributaria a los números de bastidor de los vehículos anunciados en el portal de Internet de la sociedad mencionada y a los números de teléfono de los vendedores y a facilitarle información sobre los anuncios publicados en la sección relativa a los turismos del referido portal durante cierto período comprendido entre los me-

ses de julio y agosto de 2018. La información que debía remitir el requerido consistían en la marca, el modelo, el número de bastidor y el precio del vehículo, así como el número de teléfono del vendedor. Tal conjunto de informaciones debía facilitarse por vía electrónica, en un formato que permitiera filtrar o seleccionar los datos. Al considerar que la solicitud de información de la Administración tributaria letona no era conforme con los principios de proporcionalidad y de minimización de datos personales, establecidos en el RPD, SS presentó un recurso en vía administrativa contra dicha solicitud ante el director general en funciones de la Administración tributaria letona. En sucesivas fases la cuestión llega a máximo tribunal de lo contencioso administrativo letón, el cual consideraba no discutible que la ejecución de la solicitud de información controvertida estuviese intrínsecamente vinculada a un tratamiento de datos personales, ni que la Administración tributaria letona tuviese derecho a obtener la información a disposición de un proveedor de servicios de publicación de anuncios en Internet, por cuanto resultase necesaria para la ejecución de medidas específicas en materia de recaudación de impuestos. El problema versaba en realidad sobre la cantidad y el tipo de información que podía solicitar la Administración tributaria letona, sobre su carácter limitado o ilimitado, y sobre la cuestión de si la obligación de información a la que estaba sujeta la empresa requerida debía conocer asimismo una limitación en el tiempo. El TJUE entiende que la recogida, por parte de la Administración tributaria de un Estado miembro, de información que implique una cantidad considerable de datos personales de manos de un operador económico está sujeta a los requisitos de dicho Reglamento, en particular a los enunciados en su art.5.1, las cuales sólo pueden ser obviadas si la Administración en cuestión tiene respaldo legislativo expreso. Consideradas todas estas cuestiones, por motivos de salvaguarda de la soberanía fiscal, se proclama que "nada se opone a que la Administración tributaria de un Estado miembro exija a un proveedor de servicios de publicación de anuncios en internet que le facilite información relativa a los contribuyentes que hayan publicado anuncios en alguna de las secciones de su portal de internet siempre que, en particular, tales datos sean necesarios a la luz de los fines específicos para los que se recaban y que el período de recogida no exceda del estrictamente necesario para alcanzar el objetivo de interés general perseguido".

9. La muestra interna, tocante a la Directiva del 1995, viene representada por la STJUE de 9 de noviembre de 2010, que en los As Acum. 92/09 y 93/09 opusieron a Volker y otros al Estado Federado de Hesse. Resultaba aquí que en estos asuntos agrupados por el TJUE, y relativos a la PAC, ciertas empresas agrícolas alemanas interesadas contestaban como inadecuada la práctica, según la cual, se les obligaba a firmar y reconocer para percibir las ayudas, a instancias de la *Bundesanstalt* (Administración Federal competente) que habían sido informadas de que en virtud de los Reglamento 1290/2005 y 259/2008 era obligatorio publicar los datos de los beneficiarios de fondos procedentes de FEAGA y FEADER, concretando los importes recibidos por cada beneficiario. Por lo que leemos en el relato fáctico, "dichos datos se colgaban en el sitio web de la *Bundesanstalt*, donde se ponían a disposición del público los nombres de los beneficiarios de ayudas del FEAGA y del FEADER, la localidad en la que están establecidos o en la que residen y el código postal de dicha localidad, así como los importes anuales percibidos" Y por añadidura dicho sitio web disponía de una función de búsqueda. Los interesados consideraban que dicha publicidad de datos contradecía los estándares de protección de la entonces vigente Directiva de 1995. El problema es que dicha obligación procedía de otras normas europeas, lo que planteaba su colisión e incompatibilidad en el contexto típico de la cuestión prejudicial de invalidez. El TJUE acuerda declarar que los referidos Reglamentos son inválidos en la medida en que obligan, por lo que respecta a las personas físicas beneficiarias de ayudas del FEAGA y del FEADER, a publicar datos de carácter personal de todos los beneficiarios, sin establecer distinciones en función de criterios pertinentes, tales como los períodos durante los cuales dichas personas han percibido estas ayudas, su frecuencia o, incluso, el tipo y magnitud de las mismas. Pero el alcance de esta invalidación no tiene efectos retroactivos. Se declara que la invalidez de los referidos Reglamentos no permite impugnar los efectos de las publicaciones de las listas de beneficiarios de ayudas del FEAGA y del FEADER llevadas a cabo por las autoridades nacionales, en virtud de dichas disposiciones, en el período anterior a la fecha de pronunciamiento de la presente sentencia. Y en idéntica línea, para el período antes de la sentencia, se excluye por tanto imponer al encargado de la protección de los datos personales la obligación de llevar el registro contemplado en esta disposición con anterioridad a la realización de un tratamiento de datos personales.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

10. Hablamos de las STJUES respectivamente de 6 de octubre de 2015 As 362/14 y de 16 de julio de 2020 As 311/18, correspondientes a los conocidos como casos Schrems I y II, los cuales conocen el tránsito, como norma de referencia para anular ciertas Decisiones de la Comisión, de la Directiva de 1995 al Reglamento de 2016 en materia de protección de datos. Ambos casos han determinado una prolija literatura, pues en ella entraban en colisión los modos de protección de datos personales de los ciudadanos de cara a las Administraciones públicas que imperan en la UE en un lado y en EE UU por otro.

Ya en el primer asunto, el TJUE declaró la invalidez de la Decisión 2000/520 sobre los principios de puerto seguro, mediante la cual la Comisión Europea estimaba que las transferencias de datos personales entre la Unión Europea y los Estados Unidos tenían un nivel de protección adecuado. Los motivos esenciales son no respeto del contenido esencial de derechos fundamentales consagrados en la Carta Europea de Derechos Fundamentales (en concreto sus art. 7 y art. 47), mientras que por añadidura desproveería a las autoridades nacionales del poder de evaluar la solicitud de una persona que cuestiona la compatibilidad de esa Decisión con aquellos derechos. Aparte, es la Directiva de protección de datos de 1995 entonces en vigor la otra norma esencial manejada por el TJUE en este otro ejemplo de cuestión prejudicial de apreciación de validez.

El contexto de la materia (resumido en los considerandos 27 y 28 de la STJUE Schrems I) eran que, al estar "toda persona residente en el territorio de la Unión que desee utilizar Facebook obligada a concluir en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos (…) traía por consecuencia que los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento". En 2013 el Sr. Schrems, nacional austriaco residente en Austria, es usuario de la red Facebook desde 2008 presentó ante el comisario irlandés de protección de datos (pues es en ese Estado miembro donde está la filial europea de la red social) "una reclamación en la que le solicitaba en sustancia que ejerciera sus competencias estatutarias, prohibiendo a Facebook Ireland transferir sus datos personales a Estados Unidos", siendo lo aducido que "que el Derecho y las prácticas en vigor en este último país no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas en él por las autoridades públicas". En el caso Schrems I se considera que la normativa de la Comisión controvertida, la Decisión 2000/520, cotejada con arreglo a la Directiva 95/46, y todo ello en consideración a la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes (que fueron publicadas por el Departamento de Comercio de Estados Unidos de América, y por la que la Comisión Europea constató que dicho tercer país garantiza un nivel de protección adecuado), no impediría en ningún caso que una autoridad de control de un Estado miembro pudiese examinar, y en su caso acoger favorablemente, la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que van a conocer en un país tercero (EE UU), para así denegar en consecuencia la transferencia a aquél de tales datos personales. Ello llevó a la declaración de invalidez de la Decisión 2000/520, la cual habría de quedan inaplicada en el caso de especie.

El asunto conoció una secuela en el pronunciamiento Schrems II, en donde resultaron cuestionadas otras Decisiones diversas a las del caso anterior, pero de la misma naturaleza en su condescendencia al envío a las autoridades norteamericanas de datos de ciudadanos europeos desde la sede irlandesa de Facebook. En concreto, el TJUE sostuvo que otras Decisiones, conocidas como CPT, son válidas en principio, pero puede requerir garantías adicionales para garantizar un nivel de protección sustancialmente equivalente pero no idéntico al de la UE. Es posible que un importador de datos fuera de la UE no pueda hacer mucho, si es que puede hacer algo, para proteger los datos transferidos de los programas de vigilancia del gobierno, pero cualquier protección contractual que se pueda agregar puede ayudar tanto al exportador como al importador de datos a documentar sus esfuerzos para cumplir con un entorno legal incierto, en caso de que una autoridad reguladora de la UE cuestione una transferencia en particular y/o en caso de disputa. El TJUE declaró específicamente que, en los casos apropiados, un importador de datos de EE. UU. podría tomar diversos posicionamientos, así: declarar que no tiene motivos para creer que las personas afectadas por la transferencia de datos desde la UE están sujetos a los programas de vigilancia del gobierno de EE. UU.; declarar que no tiene

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

motivos para creer que su legislación nacional le impediría cumplir con sus obligaciones en virtud de las CPT modificadas; comprometerse a implementar medidas técnicas y organizativas adicionales para garantizar la seguridad de los datos (como el uso de cifrado o el conocido como modo de transmisión VPN); comprometerse a verificar e informar al exportador de datos de la UE sobre la existencia de leyes locales que puedan comprometer la seguridad de los datos; comprometerse a informar inmediatamente al exportador de datos de la UE si tiene conocimiento de cualquier modificación de la legislación o normativa susceptible de tener consecuencias negativas sobre las garantías y obligaciones ofrecidas por las CPT, modificadas; o si se ve obligado a revelar datos personales a las autoridades gubernamentales, se comprometen a notificar al exportador de datos de la UE su incumplimiento de las CPT modificadas.

Se consideró en esta segunda ocasión, aplicando el RDP ya en vigor, que "está comprendida dentro de su ámbito de aplicación una transferencia de datos personales realizada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, a pesar de que, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado". Debe así garantizarse que "los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea por el referido Reglamento, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país". En la medida que las Decisiones de la Comisión que garantizan suficiente o insuficientemente dichos requerimientos de estándar europeo en la transferencia a un país tercero, como EE UU, así resultan unas validadas y otras declaradas inválidas por el TJUE.

BIBLIOGRAFÍA

ANDRIEU, E. (2000) Internet et la protection des données personnelles, *Legicom* 2000, núm. 21-22. Recuperado el 22 de diciembre de 2022 de https://www.cairn.info/revue-legicom-2000-1-page-155.htm

BRUNET E. (2016), Règlement général sur la protection des données à caractère personnel – Genèse de la réforme et présentation globale*, Récueil Dalloz* París. pp. 567 y sigs.

BRUNET, E. (2019), Les mécanismes de coopération des autorités de contrôle au sein de l'Union européenne et le Comité européen de la protection des données, *Revue de Droit International d'Assas* 2019, núm 2, pp. 117- 128. Recuperado el 22 de diciembre de 2022 de https://www.u-paris2. fr/sites/default/files/document/cv_publications/rdia_ndeg2_2019.pdf

CASTETS-RENARD, C. (2016) Invalidation du *Safe Harbor* par la CJUE: tempête sur la protection des données personnelles aux États-Unis, *Recueil Dalloz*. Paris, pp. 88 y sigs.

GAMBARDELLA, S. (2017) La protection des données sensibles à l'ère du numérique: regard sur le droit de l'Union Européenne, en KARLSSON-TALEB A., DE DAVID BEAUREGARD-BERTHIER O. *Protection des données personnelles et sécurité nationale: quelles garanties juridiques dans l'utilisation du numérique*, 1ère édition, Bruylant, Bruselas, pp. 56-134.

GUADAMUZ A. (2000), Habeas Data vs. the European Data Protection Directive, *The Journal of Information, Law and Technology*, Conventry, Reino Unido, Recuperado el 22 de diciembre de 2022 de https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz/

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

PÉRONNE G. y DAOUD, E. (2017) L'adresse IP est bien une donnée à caractère personnel, *Recueil Dalloz* Paris, pp. 120 y sigs.

PEYROU, S. (2015) La protection des données à caractère personnel: un droit désormais constitutionnalisé et garanti par la CJUE, en *La protection des droits fondamentaux dans l'Union européenne*, dir. R. Tinière et C. Vial, Bruylant, Bruselas.

TAMBOU, O. (2020) *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, Bruselas.

URIA GAVILAN, E. (2016) Derechos fundamentales *versus* vigilancia masiva Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems, *Revista Electrónica de Estudios Internacionales (REEI)*, Madrid pp. 261-282, Recuperado el 22 de diciembre de 2022 de https://www.cepc.gob.es/sites/default/files/2021-12/37636elisauriagavilanrdce53.pdf

Documentos

La protection des données à caractère personnel dans l'Union européenne: le rôle des autorités nationales chargées de la protection des données Renforcement de l'architecture des droits fondamentaux au sein de l'UE, Edición de 2012. Recuperado el 22 de diciembre de 2022 de https://fra.europa.eu/sites/default/files/tk3109265frc_fr_web.pdf

Manual de legislación europea en materia de protección de datos, Edición de 2018. Recuperado el 22 de diciembre de 2022 de https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 23-45
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.03

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

El abordaje de ChatGPT: el "Rinoceronte Gris" de la IA conversacional[1]

THE CHATGPT APPROACH: THE "GREY RHINO" OF CONVERSATIONAL IA

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

Recibido: 09 de mayo de 2023 | Aceptado: 12 de junio de 2023

RESUMEN

Desde que hizo su aparición en noviembre de 2022, ChatGPT ha ocupado la atención tanto de medios en línea como tradicionales. Un "rinoceronte gris" que venía dando signos de su presencia en las últimas décadas, pero que no ha sido ni atendido ni abordado adecuadamente antes de convertirse en una realidad. Esta laguna ha propiciado diferentes reacciones ante un modelo que, si bien puede ser útil en determinados contextos y haciendo un uso responsable del mismo, no se haya exento de riesgos. En el presente estudio, examinaremos el estado de la cuestión del fenómeno de ChatGPT en diferentes entornos –Italia, España y la Unión Europea– con la finalidad de apreciar la apremiante necesidad de contar con unas líneas básicas regulatorias para que una IA de este tipo pueda implementarse en el mercado sin atentar contra los derechos fundamentales de los usuarios y minimice los potenciales peligros inherentes a su uso.

PALABRAS CLAVE

ChatGPT
Inteligencia Artificial
Chatbot
Derechos fundamentales
Reglamento IA
Protección de datos

ABSTRACT

Since its emergence in November 2022, ChatGPT has captured the attention of both online and traditional media. A "gray rhino" that had been showing signs of its presence in recent decades, but was neither adequately addressed nor approached before becoming a reality. This gap has led to different reactions towards a model that, although it can be useful in certain contexts with responsible use, is not without risks. In this study, we will examine the status of the issue of the ChatGPT phenomenon in different environments - Italy, Spain, and the European Union - with the aim of appreciating the urgent need for basic regulatory guidelines to allow for the implementation of such AI in the market without infringing upon the fundamental rights of users and minimizing the potential risks inherent in its use.

KEYWORDS

ChatGPT
Artificial Intelligence
Chatbot
Fundamental rights
AI Regulation
Data protection

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

I. Introducción

El desarrollo de la Inteligencia Artificial (IA) ha experimentado en las últimas décadas un desarrollo exponencial sin precedentes y se encuentra cada vez más presente en nuestra vida cotidiana.

Si bien es cierto que la IA venía siendo una reincidente en las noticias, el 30 de noviembre de 2022 tuvo lugar el lanzamiento de uno de los productos tecnológicos con mayor crecimiento de la historia: ChatGPT[2]. Desde entonces, no deja de acaparar la atención de medios tanto tradicionales como digitales.

El fenómeno de ChatGPT ha vuelto a poner sobre la mesa los efectos tanto positivos como negativos del empleo de este tipo de herramientas por parte de la sociedad, así como las ambivalentes opiniones de la ciudadanía y diversos sectores: los que la consideran como el mejor chatbot creado hasta la fecha y presentado al público general (Roose, 2022) y los que lo aprecian como la más catastrófica creación, prediciendo incluso efectos dramáticos para los sistemas democráticos (Cowen, 2022).

En cualquier caso, lo que no puede obviarse es que nos encontramos ante una tecnología que tiene y tendrá un gran impacto y, de no ser abordada y regulada adecuadamente, puede implicar unos riesgos relevantes para el conjunto de la sociedad.

Estamos ante un fenómeno conocido metafóricamente como "rinoceronte gris"[3], que ha venido dando señales de su inminente presencia y manifestación en las últimas décadas (Ruíz Arébalo, 2022). En efecto, como consecuencia del imparable y exponencial avance en los últimos años de la IA, en general, y de los chatbots, en particular, una tecnología de tal magnitud podía encontrarse perfectamente sobre la mesa[4]. Pero lo cierto es que la eventualidad de una Inteligencia Artificial Conversacional –IAC– de este calibre no ha sido atendida[5] y ha acabado convirtiéndose en una realidad que, los diferentes

2. En los primeros 5 días alcanzó un millón de usuarios.
Vid., ChatGPT logró, en sólo cinco días, obtener un millón de usuarios (27 de febrero de 2023). Recuperado de https://www.eleconomista.com.mx/tecnologia/ChaGPT-logro-en-solo-cinco-dias-obtener-un-millon-de-usuarios-20230227-0020.html

3. Un "rinoceronte gris" es una metáfora para describir aquellas situaciones de extremo riesgo que se sabe que son posibles o incluso probables de suceder, pero que se descartan o pasan por alto. Son eventos probables que tienen impactos potencialmente catastróficos, pero siempre con un elemento de incertidumbre. El término fue ideado por la analista Michele Wucker en la cumbre de Davos de 2013 y desarrollado en su obra *The gray rhino: how to recognize and act on the obvious dangers we ignore*, en contraposición al concepto de "cisne negro", apuntalado por Nassim Taleb, para describir situaciones de alto riesgo e impacto imposibles de anticipar y que cambian por completo nuestro paradigma (como por ejemplo el 11-S).

4. El mercado de chatbots se valoró en 525.7 millones de dólares en 2021 y, actualmente, se espera que alcance un valor de 3.99 millones de dólares en 2030. Esto representa una tasa de crecimiento anual compuesto –CAGR– de alrededor del 25.7 %. *Vid.*, Grand view research (2023), *Chatbot Market Size, Share & Trends, Analysis Report By Application (Customer Services, Branding & Advertising), By Type, By Vertical, By Region (North America, Europe, Asia Pacific, South America), And Segment Forecasts, 2023 – 2030*. https://www.grandviewresearch.com/industry-analysis/chatbot-market

5. O una respuesta muy débil pues, cuando ChatGPT fue presentado al mundo, únicamente contábamos con una propuesta de Reglamento Europeo sobre IA y disposiciones genéricas en materia

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

países e instituciones desconocen cómo abordar adecuadamente. Prohibirlas, a nuestro juicio, de nada sirve, pues no sería más que un torpe intento de frenar un tsunami que ya ha comenzado.

A la vista de lo anterior, en el presente estudio examinaremos determinadas reacciones en diferentes entornos a este fenómeno de ChatGPT.

Pero primero, nos detendremos brevemente en perfilar su funcionamiento para, después, poner de relieve sus riesgos más relevantes.

II. Ideas básicas sobre el funcionamiento de ChatGPT

Diseñado por la empresa OpenAI[6], se trata de un prototipo de chatbot inteligente, manifestación de la IAC, esto es, aquellas que utilizan un conjunto de datos recopilados y estructurados por programadores de software para crear bases de datos que alimentan y capacitan a los sistemas con un repertorio de posibles preguntas y respuestas que intercambian con los usuarios (Rodríguez Spinelli, 2022, p.95).

Los sistemas de chatbots se basan en grandes modelos lingüísticos, esto es, una técnica de aprendizaje automático[7] que utiliza una ingente cantidad de textos disponibles para aprender patrones y generar nuevos textos a partir de ellos. En otros términos, estos modelos calculan qué palabra es más probable que vaya a continuación, en relación a un conjunto de ellas o una frase y, mediante este sistema, son capaces de generar frases, párrafos e incluso páginas completas en relación a lo consultado por un usuario (Shah, 2023).

Más concretamente, este chatbot ha sido desarrollado empleando la tecnología *Generative Pre-trained Transformer 3* (GPT-3), un modelo de lenguaje que utiliza aprendizaje profundo (*deep learning*) y es capaz de genera un texto similar al humano, pudiendo incluso mantener una conversación realista. Pero no es solo capaz de producir texto: también crea códigos de computación, historias, poemas, discursos, guiones de teatro, ensayos…

Lo que hace la aplicación es recoger información y datos de millones de sitios web a partir de textos estructurados *(data scraping* o *web scraping)*[8] para generar nuevos contenidos que, en apariencia, son tan coherentes como si los hubiese escrito una persona (Alonso-Arévalo y Quinde-Cordero, 2023, p.137).

---

de protección de datos. Una normativa – y proyecto de normativa– aún insuficientes para atender a una tecnología de este calado.

6. Esta compañía de investigación de IA que se anuncia como sin ánimo de lucro, fue fundada en octubre de 2015 por Elon Musk, Sam Altman y otros inversores.

7. El aprendizaje automático o *machine learning* conforma un subconjunto de IA que permite a un sistema mejorar y aprender de forma autónoma a través de redes neuronales y aprendizaje profundo (*deep learning*), sin tener que ser programado explícitamente y con un contacto humano mínimo o nulo.

8. Recibe esta denominación el proceso de recopilación y extracción de contenidos y datos de Internet de manera automática. Esto puede ser muy lesivo para la privacidad o para la información que ya estuviera colgada.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

Todo ello, a través de un sencillo proceso gratuito[9] de registro que nos dirige a una interfaz que sigue el modelo imperativo, donde el usuario plantea una petición y el sistema devuelve un resultado en un contexto multilingüe (García-Peñalvo, 2023, p.2) y omnipresente -24 horas al día, 7 días a la semana–, lo que posibilita una retroalimentación rápida y simultánea.

Lo que singulariza a ChatGPT del resto de chatbots es el elevado número de parámetros que han sido empleados en su entrenamiento. En concreto, dispone de más de 175.000 millones de parámetros[10] y constituye uno de los modelos más grandes entrenados hasta la fecha[11], y el mayor abierto al público mundial (Maslej et al., 2023). No obstante, cuantos más parámetros tenga un modelo, más datos se necesitarán para entrenarlo. De acuerdo con sus creadores, el modelo GPT-3 ha sido entrenado con 45TB de datos de texto procedentes de múltiples fuentes hasta septiembre de 2021. Es decir, el modelo actual de ChatGPT puede hacernos una redacción sobre el descubrimiento de América, pero no va a poder decirnos quien ganó Eurovisión en 2022. De hecho, si le hacemos esa pregunta nos contestará:

> Lo siento, pero como modelo de lenguaje, mi conocimiento se detiene en septiembre de 2021 y no tengo acceso a información en tiempo real. Según mi información más reciente, no puedo proporcionarte el resultado de Eurovisión en 2022. Te sugiero consultar fuentes confiables de noticias o buscar en Internet para obtener la información más actualizada sobre el ganador de Eurovisión en 2022.

9. En la actualidad, existe también ChatGPT Plus, la versión de pago de ChatGPT. A diferencia de la versión gratuita, la de pago dispone de un motor diferente: GPT-4, más avanzado. En nuestro estudio, no obstante, nos centraremos en la versión gratuita pues, precisamente por su libertad de acceso, es previsible que la disrupción social y los potenciales riesgos lleguen a ser mayores.

10. "Los parámetros son valores numéricos que emplean los modelos de aprendizaje automático durante el entrenamiento. El valor de los parámetros en los modelos de aprendizaje automático determina cómo puede interpretar los datos de entrada y predicciones.

(...) A lo largo del tiempo, ha habido un incremento constante en el número de parámetros, que se ha hecho especialmente pronunciado desde principios de la década de 2010. El hecho de que los sistemas de IA aumenten rápidamente sus parámetros refleja la creciente complejidad de las tareas que se les pide que realicen, la mayor disponibilidad de datos, los avances en el hardware subyacente y, lo que es más importante, el rendimiento de los modelos más grandes" –traducción propia– *Vid*., Maslej, et al., 2023, p. 54.

11. Para dotar estos datos de contexto, de acuerdo con el *Artificial Intelligence Index Report de 2023*, GPT-2, lanzado en 2019, considerado por muchos como el primer gran modelo lingüístico, tenía 1.500 millones de parámetros y su entrenamiento costó unos 50.000 dólares.

ChatGPT, solo es superado en la actualidad por PaLM (*Pathways language model*), la IA desarrollada por Google –e integrado en su bot conversacional *Google Bard*– para hacer frente a OpenAI. PaLM ha sido entrenada con un cuerpo de 540 millones de parámetros. Pero, a diferencia de Chat GPT que es de libre acceso y, por tanto, con un potencial mayor de incidencia en la población por la universalización de su uso, *Google Bard* no es accesible en todos los países (como es el caso de España, donde aún no se encuentra disponible).

Nos encontramos ante el claro ejemplo de cómo el entrenamiento y capacidad de estos chatbots crece de manera exponencial en cuestión de meses. *Íbidem* p. 60.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

Asimismo, tampoco es posible pedirle que elabore un razonamiento, puesto que no se halla programado para tal finalidad[12] y carece de la capacidad para discriminar la información cierta de la que no lo es (lo que origina no pocas situaciones en las que la respuesta a la petición del usuario es incorrecta).

A pesar de que, como hemos indicado previamente, la interfaz de este modelo puede llevar a cabo interacciones que le permiten ir construyendo palabras para mantener una conversación similar a un ser humano, es evidente que la comprensión de las expresiones naturales y los matices del lenguaje pueden ser difíciles de interpretar para un sistema de IA. Entonces, ¿cómo se logra este comportamiento y comunicación cuasihumana del chatbot?

Pues bien, para conseguirlo, los desarrolladores de ChatGPT emplearon, al igual que en otros chatbots existentes en el mercado, varios principios de lenguaje:

— El procesamiento del Lenguaje Natural (NLP, por las siglas en inglés *Natural Language Processing*). Se trata de un área de la IA que explora la manipulación de textos de lenguaje natural o discursos por parte de los ordenadores. De esta forma, el conocimiento de la comprensión y uso del lenguaje humano se reúne para desarrollar técnicas que permitan a estos sistemas comprender y manipular expresiones naturales para llevar a cabo las tareas deseadas. En concreto, la mayoría de las técnicas de NPL están basadas en *machine learning* (Adamopoulou y Moussaiadesm, 2020, p. 377).

— La comprensión del Lenguaje Natural (NLU, por las siglas en inglés, *Natural Language Understanding*). Conforma el núcleo de cualquier tarea de NLP. Su objetivo es extraer contexto y significado de las entradas del usuario en lenguaje natural. De esta forma, se identifica su intención y se extraen entidades específicas de dominio. Más concretamente, una intención representa una correspondencia entre lo que un usuario dice y la acción que debe realizar el chatbot. Por su parte, las acciones corresponden a los pasos que dará el chatbot cuando el usuario introduzca intenciones específicas y pueden tener parámetros para especificar información detallada sobre ellas (Adamopoulou y Moussaiadesm, 2020, p. 377). En otras palabras, se trata de la parte en la que el chatbot trata de comprender el significado de lo que quiere el usuario apoyándose en algoritmos, reglas, bases de datos y temas internos, que indicarán cual es la manera correcta de contestar.

— La Generación de Lenguaje Natural –NLG, por las siglas inglesas *Natural Language Generation*-, esto es, la construcción de una contestación consultando los repositorios de datos para ofrecer una respuesta adecuada a un fin específico (Wigmore, 2023).

12. Como sí sería el caso de PaLM.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

Los procedimientos anteriores posibilitan a la herramienta, además de humanizar su interacción con los usuarios, contextualizar lo que estos preguntan y poder continuar una conversación, puesto que "recordará" la información previamente proporcionada y la tendrá en cuenta en sus futuras interacciones.

En esta línea, otro aspecto que hace destacar a ChatGPT del resto de tecnologías hasta la fecha, es su habilidad para manejar los *feedbacks* de las respuestas y revisarlas sobre la marcha (Pearl, 2022).

En definitiva, nos encontramos ante un sistema al que es posible preguntar cualquier cosa susceptible de ser contestada mediante un texto y que, a diferencia del buscador de Google, no nos proporcionará un listado de enlaces en los que puede hallarse contenida la información que buscamos, sino que dará una respuesta concreta a nuestra petición. Incluso cabe pedirle que module el tono de su respuesta, haciéndolo más informal, profesional o solemne en función de las demandas del usuario.

Las posibilidades de lo que podemos solicitarle a ChatGPT son casi infinitas, como también lo son sus usos y, por esta misma razón, la incidencia real de sus potenciales riesgos es sumamente difícil de predecir.

III. Retos y riesgos de ChatGPT

No obstante las múltiples ventajas que el uso de este sistema puede suponer para el usuario –en términos de ahorro de tiempo y esfuerzo a la hora de cribar multitud de datos u obtener una respuesta precisa a una petición determinada-, hemos de tener presente que su uso debe venir revestido de numerosas cautelas derivadas de su principales riesgos.

Tanto es así, que es la propia herramienta la que nos informa de sus mayores limitaciones en la pantalla principal desplegada para introducir la petición concreta.

3.1. Información incorrecta y sesgos

En particular, nos advierte que "puede ocasionalmente generar información incorrecta" y "producir instrucciones dañinas o contenido sesgado".

En cuanto a la primera de ellas, en la propia política de privacidad de OpenAI[13]se previene expresamente del riesgo de inexactitud de los datos recabados de Internet[14] en las contestaciones proporcionadas por la herramienta. En este sentido, se informa de que, en ciertos casos –dado que el servicio genera respuestas leyendo la solicitud de

13. OpenAI (27 de abril de 2023), *Política de privacidad,* https://openai.com/policies/privacy-policy

14. Sobre este particular, en el campo que nos ocupa (el derecho español), la herramienta es particularmente imprecisa. En primer lugar, dado que su entrenamiento llega hasta 2021, no podremos preguntarle por reformas legislativas posteriores a dicha fecha. Pero, además, cuenta con grandes vacíos desde el punto de vista de los pronunciamientos jurisprudenciales, con respecto a los cuales se encuentra tremendamente desactualizada.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

un usuario y prediciendo las siguientes palabras que podrían aparecer en la réplica con mayor probabilidad-, los términos más probables pueden no ser los más exactos. Por ello, insta a no confiar en la exactitud de los resultados de sus modelos.

Del funcionamiento con el que opera este modelo lingüístico también se deriva que no sea capaz de entender las premisas incorrectas de una pregunta y termine respondiendo, de todos modos, a cuestiones erróneas.

Por ejemplo, si le preguntamos "¿Qué recurso no devolutivo puede interponerse ante una sentencia firme en Derecho español?", nos responderá –tomando como base la premisa (errada) de nuestra pregunta-, que "el recurso no devolutivo que puede interponerse ante una sentencia firme es el recurso extraordinario de revisión". Respuesta que, como sabemos, no es correcta, pues si bien es cierto que el recurso de revisión puede interponerse frente a sentencias firmes, este es un recurso devolutivo.

Por esta razón, un uso responsable de la herramienta pasaría por contrastar y verificar, en otros sitios webs confiables adicionales y/o con bibliografía específica, los resultados proporcionados. Asimismo, para minimizar la posibilidad de obtener respuestas incorrectas, sería conveniente dotar nuestras peticiones de un contexto claro y preciso (*prompt*) pues, si el mismo es ambiguo o escaso, el programa puede interpretar la petición de diferentes maneras y, como resultado, generar una contestación que no sea certera.

Otro riesgo importante es la aportación de contenido sesgado.

En efecto, como ya hemos precisado, ChatGPT ha sido entrenado con multitud de datos procedentes de Internet, los cuales pueden contener información inconsistente, incompleta o incorrecta, reflejando sesgos inherentes en este contenido[15]. Esto implica que las respuestas generadas por el modelo pueden reflejar prejuicios implícitos en el texto con el que ha sido entrenado, tales como sesgos raciales, de género o culturales.

Lo expuesto lleva aparejado el riesgo de arraigar conceptos o ideas errados o fomentar un pensamiento sesgado. De esta forma, se facilita la implantación de patrones silenciosos de discriminación sistemática que pasen inadvertidos para la mayoría de las personas, desconocedoras de estos peligros.

Con el fin de paliar las limitaciones puestas de manifiesto, el cuidado tanto de la precisión como de la objetividad de los datos que se introducen en el modelo algorítmico reviste suma importancia[16]. Y, no solo para agregar valor a los sistemas y procedimientos que los incorporan, sino, fundamentalmente, para asegurar que sean lo más correcto posibles a la hora de abordar temas sensibles amparados por derechos fundamentales: la dignidad de las personas, el derecho a la privacidad y la prohibición de cualquier tipo

15. Es lo que se conoce con la denominación de *dirty data*.

16. Por esta razón, la *Resolución del Parlamento Europeo sobre las implicaciones de los macrodatos en los derechos fundamentales* dispone que "serán necesarias evaluaciones periódicas sobre la representatividad de los conjuntos de datos, así como examinar la exactitud e importancia de las predicciones" (consideración general 22).

Vid., *Resolución del Parlamento Europeo sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley*, 14 de marzo de 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.html

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

de discriminación por motivos de género, raza, edad, etnia, discapacidades, creencias políticas o religiosas…

Sin embargo, asegurar la calidad de los datos que alimentan estas herramientas algorítmicas se torna una tarea extremadamente compleja, pudiendo plantearse cuestiones relativas a la concreción y selección de aquellos que efectivamente van a introducirse, la razón de incorporar estos y no otros, o la manera en que va a llevarse a cabo su análisis. Tales cuestiones repercuten y condicionan la legitimidad y fiabilidad de la respuesta proporcionada por el programa.

En definitiva, para un uso adecuado, consciente y responsable de este modelo algorítmico, hay que tener en cuenta la eventual presencia de errores y sesgos en el material recabado para su entrenamiento, así como en las respuestas generadas, siendo especialmente crítico al evaluar estas últimas.

3.2. Uso inadecuado

Tampoco debe perderse de vista la posibilidad de que, como una herramienta potente de lenguaje, sea empleada con fines malintencionados (engañosos, difamatorios o discriminatorios).

Así, aun cuando ChatGPT contaba con mecanismos de seguridad incorporados para evitar un uso inadecuado en el momento de su lanzamiento, resulta imposible prever todos los escenarios inapropiados que un usuario final pueda concebir.

A modo de ejemplo, se descubrió que ChatGPT podía ser engañado para que diera instrucciones detalladas sobre cómo construir una bomba si se le pedía que lo hiciera desde la perspectiva de un investigador que afirmaba trabajar en proyectos de seguridad relacionados con bombas (Korda, 2023). Sin embargo, un día después de la publicación del artículo en el que se evidenciaba este defecto, el mensaje exacto empleado para engañar al sistema dejó de funcionar. En su lugar, ChatGPT respondió que no podía proporcionar información sobre cómo llevar a cabo actividades ilegales o peligrosas.

El caso anterior evidencia la naturaleza evasiva de este modelo algorítmico. Es decir, sus desarrolladores intentan incorporar salvaguardas antes de tiempo, los usuarios finales tratan de romper el sistema y eludir sus políticas, y los desarrolladores reaccionan parcheando las lagunas una vez que salen a la luz… y así *ad infinitum*.

Finalmente, en torno a este uso inadecuado de ChatGPT, hay otra cuestión interesante desde el punto de vista ético que ha de ser tenida en cuenta en su funcionamiento: cuando el programa proporciona una respuesta que implica una muestra de conocimiento, lo hace sin indicar las fuentes de las que ha sido extraída la información suministrada[17].

17. Si se le solicita expresamente, el sistema proporcionará un listado de enlaces de los cuales ha sido obtenida la información para elaborar la respuesta, pero lo hará sin indicar de dónde ha sido extraída expresamente cada elemento de la contestación aportada.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

3.3. Problemas de privacidad y confidencialidad

Puesto que ChatGPT –como hemos visto- ha sido desarrollado con los contenidos disponibles en la Red hasta septiembre de 2021, dentro de ellos sería posible encontrar datos personales, tanto de usuarios como de no usuarios, recabados, en su mayoría, sin el consentimiento previo de sus titulares.

Pero hay que tener en cuenta que no solo se nutre de la información con la que ha sido inicialmente entrenado, sino también de la suministrada por los usuarios cada vez que emplean la aplicación. ChatGPT da respuesta a sus demandas, pero a la vez estos alimentan el algoritmo directa e indirectamente. De esta manera, los datos que recopile no serán solo los personales identificativos que son facilitados al crear la cuenta (nombre, credenciales…), sino también los de conexión como la IP, la ubicación aproximada, el navegador o el móvil desde el que se emplea la herramienta.

Así, durante las "conversaciones" con el sistema, es posible que se recopilen y almacenen los mensajes intercambiados, lo que puede incluir información personal y confidencial que sea revelada durante su uso. Además, si bien la interacción es anónima, existe el riesgo de que los datos proporcionados sean utilizados para identificar a los individuos, lo que puede amenazar su privacidad y confidencialidad.

Por otro lado, también hay que tener presente que, si las conversaciones con el chatbot se almacenan indefinidamente, existe un mayor riesgo de que el contenido sensible o confidencial permanezca en manos de los proveedores de servicio y que estos lo compartan con terceros u otros proveedores[18] –con fines de investigación o desarrollo de productos-, o sean objeto de hackeos o brechas de seguridad en el futuro.

Es cierto que, una vez abierta la cuenta, el sistema advierte de que las propias conversaciones que los usuarios tengan con el chat pueden ser reutilizadas para su entrenamiento e insta a no introducir información sensible. Sin embargo, más allá de esta somera referencia, no se facilita información alguna a los interesados cuyos datos hayan sido recogidos por OpenAI, y manejados por ChatGPT, sobre el modo en que serán tratados.

A día de hoy, aun cuando buceemos en la política de privacidad, no es posible conocer qué ocurre detrás de la herramienta. No obstante, recientemente –como veremos- se ha incorporado a dicha política la indicación expresa de los datos personales de los usuarios que van a ser recabados en sus interacciones con ChatGPT, así como el uso que se dará a los mismos, con la posibilidad de oponerse específicamente a que sean empleados para entrenar al algoritmo.

A pesar de encontrarnos ante un fenómeno con entidad suficiente para ocasionar riesgos tan relevantes, este se ha manifestados en un contexto legal, tanto nacional como europeo, que no se encontraba preparado para asumir una irrupción tecnológica de este calibre. Un "rinoceronte gris" que ya ha hecho acto de presencia y cuyos efectos, dada la carencia de una regulación suficiente, ha sido necesario abordar sobre la marcha y calibrar con la normativa en vigor, con evidentes carencias.

18. Eventualidad de la que se advierte en la propia política de privacidad de OpenAI.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

IV. Estado de la cuestión: reacciones a ChatGPT

Las reacciones a ChatGPT no se han hecho esperar. En efecto, como consecuencia de los riesgos anteriores, son cada vez más las autoridades de protección de datos que cuestionan la licitud de estos sistemas debido a que su funcionamiento no resulta, en muchos puntos, conforme con la normativa de privacidad y protección de datos personales.

4.1. Italia

En particular, ha sido la autoridad de control italiana de protección de datos –*Garante per la Protezioni dei Dati Personali*-, la primera en investigar a ChatGPT por una posible infracción de las leyes de protección de datos. Esto es, tanto del Reglamento General de Protección de datos (RGPD[19])-, en sus arts. 5, 6, 8, 13 y 25 (principios de transparencia, limitación de finalidad, exactitud y confidencialidad e integridad de los datos), como del Código italiano en materia de protección de los datos personales[20].

Así, el 30 de marzo de 2023, cuatro meses después del lanzamiento de la herramienta y en pleno apogeo y expansión de esta tecnología, la autoridad italiana de protección de datos emitió una resolución en el que instó al bloqueo inmediato y temporal[21] de ChatGPT (*Garante per la Protezioni dei Dati Personali* [GPDP], 2023a), a la espera de la conclusión de la investigación preliminar necesaria sobre los controvertidos asuntos surgidos en relación con OpenAI[22]. En particular se alegaron los siguientes motivos:

1. La falta de claridad sobre la forma en que se recopilan y emplea la ingente cantidad de datos que proporcionan cada día los usuarios.
2. La carencia de una base jurídica adecuada y suficiente para poder alimentar y entrenar al algoritmo con los datos de los usuarios.

19. *Reglamento 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, de 27 de abril de 2016 (Reglamento General de Protección del Datos –RGPD-) https://www.boe.es/doue/2016/119/L00001-00088.pdf

20. *Codice in materia di protezione dei dati personali,* 30 de junio de 2003, n.196. https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=6.0

21. Con base en la vía ofrecida por el art. 58, apartado 2, letra f) del Reglamento General de Protección de Datos: "2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación: (…) f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición."

22. En concreto, la decisión de la autoridad de control italiana constituye una reacción a la noticia del 20 de marzo de 2023 sobre un fallo de seguridad en la herramienta (*data breach*) que ocasionó la difusión de varias conversaciones privadas e información relativa al pago de los abonos al servicio de pago (ChatGPT 4).

Vid., OpenIA (24 de marzo 2023), *March 20 ChatGPT outage: Here's what happened.* https://openai.com/blog/march-20-chatgpt-outage

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

3. La ausencia de sistemas de verificación de edad que permitan proteger a los sujetos especialmente vulnerables.

Con motivo de las mencionadas insuficiencias en el funcionamiento de la herramienta, la autoridad italiana requiere a OpenAI[23] para que, en un plazo de 20 días[24], comunique qué medidas ha adoptado para dar respuesta a estas cuestiones, con la consecuencia, en el caso de no hacerlo, de enfrentarse a una cuantiosa sanción[25].

A este comunicado, siguió una respuesta de OpenAI expresando su disposición inmediata a colaborar con la autoridad italiana para cumplir con la normativa europea sobre privacidad y alcanzar una solución compartida capaz de resolver los perfiles críticos planteados por la GPDP en relación con el tratamiento de los datos de los ciudadanos italianos (GPDP, 2023b).

Esta voluntad colaborativa de OpenAI, culminó con una reunión celebrada el 5 de abril entre la empresa americana y la autoridad italiana, donde la primera se comprometió a reforzar la transparencia en el uso de los datos personales de los afectados, los mecanismos existentes para el ejercicio de los derechos y las garantías para los menores (GPDP, 2023c).

Tras el aludido encuentro, la GPDP emitió una nueva orden (GPDP, 2023d) en la que comunicaba que OpenAI dispondría hasta el 30 de abril para cumplir los requisitos impuestos en materia de información, derechos de los interesados –usuarios y no usuarios-, base jurídica del tratamiento de los datos personales para el entrenamiento de algoritmos con datos de usuarios y tutela de los menores. Solo entonces, al dejar de existir los motivos de urgencia, se suspendería la medida de bloqueo y ChatGPT podría volver a ser accesible desde Italia.

En particular, la empresa habría de adoptar, entre otras, las siguientes medidas (sin perjuicio de otras que puedan acordarse una vez concluía la investigación):

1. Preparar y publicar en su sitio web un aviso en el que se indique a los interesados –incluidos los que no sean usuarios del servicio de ChatGPT, cuyos datos

23. Que si bien no tiene oficina en la Unión ha designado un representante en el Espacio Económico Europeo.

24. Con fundamento en el art. 58 apartado 1, del Reglamento General de Protección de Datos: "1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación: a)ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones; b)llevar a cabo investigaciones en forma de auditorías de protección de datos; c)llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7; d)notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento; e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones; f)obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros".

25. De hasta 20 millones de euros o de hasta el 4% del volumen de negocios anual actual, de acuerdo con el art. 83, apartado 5, letra e) del Reglamento General de Protección de Datos.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

hayan sido recogidos y tratados con la finalidad de entrenar a los algoritmos-, los métodos de tratamientos, la lógica subyacente al tratamiento necesario para el funcionamiento del servicio, sus derechos como interesados y cualquier otra información exigida por el RGPD, en los términos y en la forma establecidos en su art. 12. Dicha información tendría que ser fácilmente accesible y colocarse en un lugar donde pueda leerse antes de proceder a cualquier registro en el servicio (GPDP, 2023e)[26].

2. Garantizar los derechos reconocidos en el RGPD a los interesados y, en especial, los derechos de oposición y supresión. Así, al menos para aquellos que se conecten desde Italia, habrá de establecer una herramienta a través de la cual puedan ejercer su derecho a oponerse al tratamiento de sus datos personales, obtenidos con la finalidad de entrenar a los algoritmos y para la prestación del servicio. E, igualmente, deben poder solicitar y obtener la rectificación de los datos personales y los que hayan sido tratados de forma inexacta en la generación de contenidos o, en caso de imposibilidad debido al estado de la técnica, la supresión de estos.
3. Modificar la base jurídica del tratamiento de los datos personales de los usuarios con fines de formación de algoritmos, eliminando cualquier referencia a la ejecución de un contrato e indicar, en su lugar, el consentimiento o el interés legítimo, para tal entrenamiento.
4. En el momento de cualquier reactivación del servicio desde Italia, incluir una solicitud, a todos los usuarios que se conecten desde el país, incluidos los ya registrados, para que pasen, en el momento del primer acceso, una verificación de edad que excluya, sobre la base de la edad declarada, a los usuarios menores de edad (13 años).
5. Presentar a la GPDP, antes del 31 de mayo de 2023, un plan de acción que prevea, a más tardar el 30 de septiembre de 2023, la puesta en marcha de un sistema de verificación de la edad capaz de excluir el acceso a los usuarios menores de 13 años y a los menores que carezcan del consentimiento paterno.
6. Y, finalmente, promover, a más tardar el 15 de mayo de 2023, una campaña informativa, de carácter no promocional en todos los principales medios de comunicación italianos (radio, televisión, periódicos e Internet), con el fin de informar a las personas de que sus datos personales son susceptibles de ser recogidos para la formación de algoritmos, y de que se ha puesto a su disposición en el sitio web de OpenAI una herramienta a través de la cual todas las partes interesadas pueden solicitar y obtener la eliminación de sus datos personales.

26. En concreto, para los usuarios que se conecten desde Italia, el aviso se presentará antes de completar el registro y, de nuevo, antes de completar el registro, se les pedirá que declaren que son mayores de edad. Por otro lado, para los usuarios que ya se han registrado, el aviso informativo deberá presentarse en el momento de su primer acceso tras la reactivación del servicio y, en la misma ocasión, deberá pedírseles que pasen una verificación de edad que excluya, sobre la base de la edad declarada, a los usuarios menores de edad.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

Finalmente, el 28 de abril de 2023 la GDPD emite un comunicado (GPDP, 2023f) en el que informa que ChatGPT vuelve a estar disponible en Italia, tras recibir una nota de OpenAI en la que ilustra las medidas introducidas en el cumplimiento de sus peticiones. En concreto, entre ellas se adoptan, esencialmente, las siguientes:

— Proporcionar información detallada sobre cómo se alimenta el algoritmo. Esta puede ser consultada en la correspondiente actualización de la política de privacidad de OpenAI que tuvo lugar el 27 de abril de 2023. En concreto, en ella se establece un apartado relativo a la información personal recolectada por la compañía, con indicación expresa tanto de la proporcionada directamente por el usuario como de la recibida automáticamente por la empresa norteamericana cada vez que se emplea el servicio. Asimismo, se reserva otra sección para indicar los diversos usos que pueden darse a la información anterior y se advierte de la eventual facilitación de los datos a terceros (vendedores y otros proveedores de servicios) por razón de transmisión de empresas o el cumplimiento de requisitos o exigencias legales, entre otros.
— Reconocer el derecho de todas las personas residentes en Europa, incluidos los no usuarios, a oponerse al tratamiento de sus datos personales para entrenar al modelo, pudiendo excluir las conversaciones y su historial de dicho entrenamiento algorítmico.
— Para ello, basta con acudir a nuestro perfil de ChatGPT y, en el apartado *Settings*, pulsar *Data controls* y deseleccionar *Chat History & Training*. Al desactivar esta opción, las nuevas conversaciones no se emplearán para entrenar y mejorar el algoritmo y tampoco aparecerán en el historial. No obstante, se advierte que, para evitar abusos, estas serán conservadas durante 30 días antes de ser eliminadas definitivamente. Anteriormente, para evitar que los datos recopilados durante la interacción con ChatGPT fueran empleados para mejorar el modelo, era necesario solicitarlo a través de un formulario concreto (*User Content Opt Out Request*)[27]. Con esta nueva actualización, resulta mucho más sencillo desactivar el uso compartido de los datos.
— Por otro lado, en ejercicio del derecho de supresión, dado que la compañía se declara en la actualidad técnicamente incapaz de corregir los errores debido a la complejidad del modelo[28], se posibilita la eliminación de datos personales

27. El formulario al que nos referimos puede ser consultado en: https://docs.google.com/forms/d/e/1FAIpQLScrnC-_A7JFs4LbIuzevQ_78hVERlNqqCPCt3d8XqnKOfdRdQ/viewform

28. En particular, en la política de privacidad de OpenAI, en un nuevo apartado relativo a los derechos de los usuarios, con expresa alusión a ChatGPT, se indica expresamente que, si los usuarios aprecian que los resultados del programa contienen información personal inexacta que se desee corregir, el interesado puede enviar una solicitud de corrección a dsa@openai.com. Sin embargo, se advierte que, dada la complejidad técnica del funcionamiento de estos modelos, es posible que dicha inexactitud no pueda ser corregida, en cuyo caso, cabe solicitar la eliminación de la información personal de los resultados de ChatGPT rellenando el formulario enlazado en la página para tal finalidad (*OpenAI Personal Data Removal Request*).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

inexactos o información incorrecta mediante un formulario especial que puede cumplimentarse en línea, fácilmente accesible[29].

— Incluir en la pantalla de bienvenida reservada a los usuarios ya registrados, un botón a través del cual, para volver a acceder al servicio, deberán declarar que son mayores de edad o mayores de 13 años y, en este último caso, contar con consentimiento paterno. En esta línea de protección de los menores, cuando se lleve a cabo el registro, se solicitará la fecha de nacimiento y se establecerá un bloqueo del registro para los menores de 13 años y, en el caso de los mayores de 13 años, pero menores de edad, deberán confirmar que disponen de consentimiento paterno para utilizar la herramienta.

A pesar de todas las medidas anteriores, hemos podido apreciar que uno de los requerimientos principales de la autoridad italiana no ha sido atendido. Nos referimos al hecho de que no se ha eliminado la referencia a la ejecución de un contrato. Así, en la política de privacidad de OpenAI, se continúa incluyendo entre las bases legales para el procesamiento de la información, la referencia al cumplimiento de un contrato con el usuario cuando se proporcionan los servicios. Sin embargo, esta persistente referencia se equilibra con la posibilidad de ejercer el derecho de oposición al tratamiento de los datos personales con la finalidad de entrenar al algoritmo sobre la base del interés legítimo.

Tras todo lo anterior, puede apreciarse como a partir de la medida de bloqueo temporal inmediato acordada por la GDPD, OpenAI ha redoblado sus esfuerzos por hacer más compatible el uso de la herramienta con las exigencias en materia de protección de datos personales y privacidad –tanto europeas como italianas- incorporando nuevas premisas esenciales para operar en el territorio comunitario. Italia ha sentado las nuevas líneas que, como base, habrán de adaptarse a las particularidades normativas de cada país (por ejemplo, en lo que respecta a la minoría de edad en Internet y para el uso de las aplicaciones *online* que, si bien en Italia se fija en 13 años, en España se eleva a 14 años[30]).

Este bloqueo también ha tenido eco fuera del territorio italiano. Así, a raíz del mismo, el Comité Europeo de Protección de Datos anunció, tras una reunión en sesión plenaria, su propósito de crear un grupo de trabajo sobre ChatGPT, con el fin de cooperar e intercambiar información sobre acciones que las autoridades de protección de datos

29. En concreto, el formulario puede ser consultado en el siguiente recurso *online* (*OpenAI Personal Data Removal Request*): https://share.hsforms.com/1UPy6xqxZSEqTrGDh4ywo_g4sk30

30. Tal previsión la encontramos en el art. 7 de la Ley Orgánica 3/2018, de Protección de Datos Personales, relativo al consentimiento de los menores de edad, donde se dispone que: "El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años".

Vid., *Ley Orgánica 2/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (BOE núm. 294, de 6 de diciembre de 2018). https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

pudiesen emprender en relación con dicha cuestión[31] (de acuerdo con el principio de coherencia recogido en el Reglamento General de Protección de datos).

La iniciativa italiana también ha hecho que otros países de la UE, entre ellos España, decidan seguir su ejemplo.

4.2. España

Siguiendo la estela de Italia, el 13 de abril de 2023, la Agencia Española de Protección de Datos –AEPD- anunció que iniciaba de oficio actuaciones de investigación contra OpenAI[32], por un posible incumplimiento de la normativa de privacidad y protección de datos personales.[33]

Al igual que la GPDP, la AEPD actúa en el marco de las potestades y competencias que, como autoridad nacional de supervisión y control, le atribuye el art. 58 del Reglamento General de Protección de Datos para llevar a cabo actividades de investigación. Sin embargo, la autoridad española, a diferencia de la italiana, no ha ejercitado su potestad para bloquear temporalmente la herramienta (si bien es una opción que no descarta).

Por su parte, con fecha de 21 de abril, la Autoridad Catalana de Protección de Datos –APDCAT– emitió la Recomendación 1/2023[34] para advertir a la Generalitat, los municipios, las escuelas, las universidades y demás entidades de su ámbito de actuación, sobre las dudas existentes en Europa de que esta herramienta de IA cumpla con el Reglamento General de Protección de Datos. Se recomienda, por tanto, no incorporar la herramienta de ChatGPT en el ejercicio de funciones y prestación de servicios públicos cuando se traten datos personales hasta que el Comité Europeo de Protección de Datos se pronuncie al respecto.

31. European Data Protection Board (13 de abril 2023), *EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT.* https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en.

32. Agencia española de protección de datos (13 de abril de 2023), *La AEPD inicia de oficio actuaciones de investigación a OpenAI, propietaria de ChatGPT*. https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-inicia-de-oficio-actuaciones-de-investigacion-a-openai

33. La Red Iberoamericana de Protección de Datos (RIPD), cuya secretaría permanente ostenta la AEPD, también se ha propuesto iniciar una labor de supervisión sobre ChatGPT y coordinar sus acciones en el marco de la Red. Así, la RIPD considera que este servicio puede conllevar riesgos para los derechos y libertades de los usuarios en relación con el tratamiento de sus datos personales.

A estas acciones, como ya hemos apuntado, se suman las realizadas por el Comité Europeo de Protección de Datos, del que la AEPD forma parte junto con otras autoridades de protección de datos del EEE, que ha creado un grupo de trabajo para fomentar la cooperación e intercambiar información sobre las acciones llevadas a cabo por las autoridades de protección de datos. De esta forma, la AEPD, al ser parte de ambas organizaciones, actuará como enlace entre la RIPD y el Comité Europeo. *Vid.*, Agencia española de protección de datos (11 de mayo de 2023), *Las autoridades de la Red Iberoamericana de Protección de Datos Personales inician una acción coordinada en relación con el servicio ChatGPT.* https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/autoridades-ripd-inician-accion-coordinada-servicio-chatgpt

34. *Recomanació 1/2023 en relació amb la utilització de ChatGPT i el seu impacte en la protecció de dades personals*, 21 de abril de 2023. Autoridad catalana de protección de datos. https://apdcat.gencat.cat/web/.content/01-autoritat/normativa/documentos/Recomanacio12023_ChatGPT.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

Asimismo, recuerda que, actualmente, la tecnología permite dibujar perfiles y patrones a partir de datos personales, los cuales pueden servir para influir directamente en las personas, y alerta de que, ante el uso masivo e intenso de datos, es necesario contar con las herramientas adecuadas para proteger los derechos y libertades.

En la misma línea, recientemente saltaba en nuestro país la noticia[35] de que grandes empresas españolas –como Telefónica[36], BBVA[37] o Redeia[38]- han resuelto limitar, e incluso prohibir, a sus empleados el uso de ChatGPT. Las razones de dicha decisión descansan en la alta probabilidad de que la información generada por la herramienta tenga sesgos o aporte información errónea, así como el peligro de introducir datos personales y corporativos y que se produzcan filtraciones[39].

Otras compañías, tales como Naturgy y Enagás, han enviado a sus empleados recomendaciones para utilizar este y otros sistemas de IA y, en particular, la segunda apuesta por introducir unos principios de uso correcto de la IA en su nuevo código ético, así como en un programa de formación de empleados[40].

4.3. Unión Europea

En el ámbito de la UE, el 21 de abril de 2021 fue publicada la *Propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial* (Reglamento IA)[41]. Su objetivo descansa en mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular en lo que concierne al desarrollo, la comercialización y la utilización de la IA de conformidad con

35. *Grandes empresas españolas ya prohíben a sus empleados el uso de ChatGPT: "Contine información errónea"* (mayo 2023). Recuperado de https://www.elmundo.es/economia/empresas/2023/05/21/64679873e4d4d863428b45a9.html

36. La compañía no permite el uso de la herramienta para tratar información de la empresa, salvo que la cuenta sea contratada y controlada por Telefónica. Asimismo, para garantizar que la IA se utilice de forma segura, incorpora en su organigrama un Comité de IA Ética para que evalúe casos de uso de alto riesgo, y está trabajando en un reglamento interno de gobernanza de la IA, que abordará tanto ChatGPT como otras inteligencias artificiales generativas.

37. La entidad bancaria, prohíbe el uso de ChatGPT con carácter general, aunque para aquellos profesionales que crean que puede serles de utilidad, ha habilitado un proceso de autorización.

38. Redeia (Red Eléctrica), por su parte, ha bloqueado el uso de la versión pública por posibles riesgos vinculados a la protección de la información. Cuestión especialmente relevante, puesto que nos encontramos ante una empresa que gestiona infraestructuras estratégicas.

39. Fuera de España, en empresas como Deloitte, JPMorgan, Verizon, Apple o Microsoft (siendo llamativo el caso de esta última por tratarse de uno de los principales inversores de OpenAI), también se ha desaconsejado el uso de datos confidenciales o sensibles en ChatGPT.

La revolución de ChatGPT y el temor de las grandes empresas españolas, (junio 2023). Recuperado de https://gdempresa.gesdocument.com/noticias/chatgpt-grandes-empresas

40. En el mismo sentido, Mapre y Repsol, trabajan con protocolos para garantizar que la IA se emplee de forma ética y segura.

41. *Propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial), y se modifican determinados actos legislativos de la Unión*, 21 de abril de 2021. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

la normativa de la UE. Asimismo, persigue varios fines de interés general, tales como asegurar un nivel elevado de protección de la salud, de la seguridad y los derechos fundamentales reconocidos y protegidos por el derecho de la Unión, y garantiza la libre circulación transfronteriza de bienes y servicios basados en la IA[42].

En particular, para lograr que una normativa de este tipo puede regular tecnologías disruptivas en constante transformación (y no quede obsoleta incluso antes de su entrada en vigor), la propuesta de Reglamento IA no se articula en base a tecnologías concretas, sino que parte de una estructura organizada en niveles de riesgo que se pueden derivar del uso de estos sistemas. De esta manera, se distingue entre modelos que conlleven un riesgo inaceptable (que directamente se prohíben), un alto riesgo (que se permiten, pero sujetos a rigurosos controles para evitar que puedan afectar a las libertades y a los derechos fundamentales), un riesgo limitado y un riesgo mínimo.

En la actualidad, los avances en la tramitación del Reglamento IA siguen su curso, estando prevista, en principio, su aprobación para enero de 2024 (Garvi Carvajal, 2023).

Uno de los hitos más recientes en este proceso ha sido el compromiso alcanzado en mayo por el Parlamento Europeo sobre un Borrador de enmiendas[43] en torno a la propuesta inicial del Reglamento IA. En concreto, a los efectos de nuestro estudio, en este Borrador de enmiendas se introducen obligaciones para los proveedores de modelos fundacionales y sistemas de IA generativa[44] (entre los que se encontraría ChatGPT).

4.3.1. Sistemas de IA de propósito general

Antes del Parlamento Europeo, la propuesta del Consejo de la Unión Europea de 25 de noviembre de 2022[45] introdujo el concepto de sistema de IA con propósito general. Por tal se entienden aquellos sistemas algorítmicos que puede ser empleados para realizar funciones de aplicación general –como el reconocimiento de imagen/voz–, en una pluralidad de contextos[46]. Además, se advierte que estos pueden ser empleados como sistemas de alto riesgo por sí mismos o ser componentes de otros sistemas de alto riesgo.

---

42. Con lo que se impide que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistema de IA, a menos que el Reglamento lo autorice expresamente.

43. *Borrador de enmiendas del Parlamento Europeo a la Propuesta de Reglamento sobre normas armonizadas relativas a la Inteligencia Artificial*, 9 de mayo de 2023. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf

44. La propuesta inicial del Reglamento IA no incluía definición alguna en la que pudieran englobarse los sistemas de IA generativa como una subcategoría concreta dentro de los sistemas algorítmicos. No obstante, la aparición de ChatGPT –entre otros–, ha llevado a los legisladores europeos a abordar una regulación específica.

45. *Propuesta del Consejo de la Unión Europea para un Reglamento sobre normas armonizadas de Inteligencia Artificial*. Documento 2021/0106 (COD), de 25 de noviembre de 2022. https://artificialintelligenceact.eu/wp-content/uploads/2022/12/AIA-%E2%80%93-CZ-%E2%80%93-General-Approach-25-Nov-22.pdf

46. Más concretamente, el art. 1b) de la Propuesta del Consejo de la UE, define a los sistemas de IA de propósito general como "un sistema de IA que, independientemente de cómo se comercialice

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

En consecuencia, debido a su naturaleza particular y con el objetivo de garantizar un reparto equitativo de responsabilidades a lo largo de la cadena de valor de la IA, dichos sistemas han de estar sujetos a requisitos y obligaciones proporcionados y más específicos en base al Reglamento IA, garantizando, al mismo tiempo, un alto nivel de protección de los derechos fundamentales, la salud y la seguridad. Con esta finalidad, los proveedores de sistemas de IA de propósito general[47] deberán cooperar con los proveedores de los respectivos sistemas de alto riesgo, para permitirles cumplir las obligaciones pertinentes en virtud del Reglamento IA y con las autoridades competentes establecidas en el mismo[48].

Es el art. 4b de la propuesta del Consejo sobre el Reglamento IA el que recoge los requisitos de los sistemas de propósito general y las obligaciones de sus proveedores. Así, se dispone que determinados requisitos establecidos para los sistemas de IA de alto riesgo –en concreto los señalados en el Capítulo 2 del Título III[49]- han de ser aplicados

o ponga en servicio, incluso como software de código abierto, está destinado por el proveedor para realizar funciones de aplicación general, como el reconocimiento de imagen, voz y generación de audio, detección de patrones, respuesta a preguntas, traducción y otras; un sistema de IA de propósito general puede ser utilizado en una pluralidad de contextos e integrarse en una pluralidad de otros sistemas de IA" (traducción propia), *op., cit*.

47. Independientemente de que puedan ser utilizados como sistemas de alto riesgo como tales o como componentes de sistemas de alto riesgo.

48. De esta forma, para poder tomar en consideración las características específicas de los sistemas de IA de propósito general y la rápida evolución de la técnica y el mercado en este campo, habrá de conferirse a la Comisión competencias de ejecución para especificar y adaptar la aplicación de los requisitos establecidos en el Reglamento a los sistemas de IA de propósito general y para especificar la información que han de compartir los proveedores de estos sistemas para que los proveedores de los respectivos sistemas de IA de alto riesgo puedan cumplir sus obligaciones en virtud del Considerando 12c de la Propuesta del Consejo de la UE.

49. Tales requisitos incluyen: el establecimiento, implantación, documentación y mantenimiento de un sistema de gestión de riesgo asociados a estos sistemas (es decir, un proceso iterativo continuo que se lleva a cabo durante todo el ciclo de la vida de un sistemas de IA de alto riesgo que requerirá actualizaciones sistemáticas periódicas); en el caso de sistemas de este tipo que utilicen técnicas que implican el entrenamiento de modelos con datos, se desarrollarán a partir de conjuntos de datos de entrenamiento, validación y prueba que se someterán a técnicas adecuadas de gobernanza y gestión de datos, que sean pertinentes y representativos, carezcan de errores y estén completos, que dispongan de las propiedades estadísticas adecuadas y que tengan en cuenta los elementos particulares del contexto geográfico, conductual o funcional específico en el que se pretenda utilizar el sistema; antes de la entrada al mercado del sistema de IA de alto riesgo o su puesta en servicio, se preparará su documentación técnica –que demuestre que cumple los requisitos anteriores– y se mantendrá actualizada; estos sistemas se diseñarán y desarrollarán con capacidades de registro que garantizarán un nivel de trazabilidad del funcionamiento del sistema de IA durante su ciclo de vida; se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida e irán acompañados de las instrucciones de uso correspondiente de forma concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios; se diseñarán y desarrollarán de manera que puedan ser vigilados de manera efectiva por personas físicas durante el periodo que estén en uso; y se diseñarán y desarrollarán de modo que, en vista de su finalidad prevista, alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera consistente en estos sentidos durante todo su ciclo de vida.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

también a los de propósito general. Pero no mediante una aplicación directa de los mismos, sino a través de un acto de ejecución adoptado por la Comisión[50] que especificaría cómo deben aplicarse estos requisitos a dichos sistemas de IA sobre la base de una consulta y una evaluación de impacto que tenga en cuenta sus específicas características y su cadena de valor, la viabilidad técnica y el desarrollo tecnológico y del mercado[51].

4.3.2. Modelo fundacional

Posteriormente, a la definición anterior de sistemas de IA de propósito general, el Borrador de enmiendas del Parlamento Europeo añade la noción de "modelo fundacional", como subcategoría de los sistemas de propósito general, e incluye la IA generativa[52], esto es, aquella desarrollada a partir de algoritmos entrenados con una amplia gama de fuentes y datos capaces de realizar una gran variedad de tareas posteriores, incluidas algunas para las que no han sido desarrollados o entrenados[53].

Entre las obligaciones impuestas por el Reglamento IA a los proveedores de modelos fundacionales se encuentran, esencialmente, la demostración (a través de un diseño, prueba y análisis adecuados) de la identificación, reducción y mitigación de los riesgos razonablemente previsibles para la salud, seguridad, derechos fundamentales, medio ambiente, democracia y Estado de Derecho; procesar e incorporar únicamente datos que estén sujetos a medidas apropiadas de gobierno de datos, en particular, examinar la idoneidad de las fuentes y posibles sesgos; y diseñar y desarrollar un modelo base sólido para lograr niveles adecuados de rendimiento, previsibilidad, interpretabilidad, corregibilidad, seguridad y ciberseguridad. Además, deberán diseñar sus modelos aplicando las normas concebidas para reducir el consumo de energía, el uso de recursos y residuos y para aumentar la eficacia energética y la eficiencia global del sistema[54].

En particular, el art. 28 b. 4 del Borrador de enmiendas del Parlamento Europeo regula específicamente los modelos fundacionales utilizados en sistemas de IA generativa, esto es, aquellos destinados específicamente a generar, con distintos niveles de autonomía, contenidos como texto complejo, imágenes, audio o video, estableciendo un último nivel más estricto de obligaciones y requisitos.

De esta forma, además de los requisitos generales exigidos a los proveedores de un modelo fundacional, estos deberán: a) cumplir las obligaciones de transparencia del art. 52.1 del Reglamento IA esto es, la necesidad de que los sistemas algorítmicos que interactúan con personas estén diseñados y desarrollados de forma que las mismas estén

50. A través de este acto de aplicación, se garantizaría que los Estados miembros participaran adecuadamente y mantuvieran la última palabra sobre cómo se aplican los requisitos en este contexto.

51. Además de cumplir con tales requisitos, los proveedores de estos sistemas están obligados a implementar un sistema de gestión de calidad, conservar al menos la documentación relevante durante 10 años y someter a evaluación de conformidad al sistema de IA sobre el impacto que puedan estos sistemas tener sobre la seguridad, los derechos fundamentales o el medio ambiente, entre otros.

52. ras el auge de ChatGPT y otros modelos.

53. Considerando 60 d) del Borrador de enmiendas del Parlamento Europeo.

54. Art. 28 b) del Borrador de enmiendas del Parlamento Europeo.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

informadas de que están actuando con un sistema de IA[55]; b) formar y, en su caso, diseñar y desarrollar el modelo para que garantice las salvaguardias adecuadas contra la generación de contenidos contrarios al Derecho de la Unión, en consonancia con el estado de la técnica generalmente reconocido y con el ejercicio de los derechos fundamentales, incluida la libertad de expresión; c) y documentar y poner a disposición del público un resumen suficientemente detallado del uso de los datos de entrenamiento protegidos por la legislación sobre derechos de autor.

No obstante este más estricto nivel de obligaciones y requisitos para los modelos fundacionales empleados en sistemas de IA generativa, el considerando 60 g) del Borrador de enmiendas señala expresamente que tales requisitos y obligaciones específicos no equivalen a considerar los modelos fundacionales como sistemas de IA de alto riesgo –aun cuando deban cumplir determinados requisitos establecidos para los sistemas de IA de alto riesgo–, sino que deben garantizar que se cumplan los objetivos del Reglamento IA para asegurar un alto nivel de protección de los derechos fundamentales, la salud y la seguridad, el medio ambiente, la democracia y el Estado de Derecho.

Esta apreciación es compatible con lo previsto para los sistemas de IA de propósito general, en el sentido de que los modelos generativos de IA, *per se*, no pueden ser clasificados como sistemas de IA de alto riesgo, pero sí pueden ser usados como tales –en función de su finalidad–, o pueden integrarse en un modelo de IA que sí sea calificado como de alto riesgo. Como consecuencia de lo apuntado, los requisitos y obligaciones exigidos no resultarán de aplicación si el proveedor excluye expresamente todos los usos de alto riesgo en las instrucciones que elabore para su sistema de IA. Exclusión que solo será permisible si el proveedor tiene motivos suficientes para considerar que este no será objeto de un uso indebido una vez comercializado[56].

No obstante, a nuestro juicio, se trata de una previsión criticable, pues es difícil (por no decir imposible) excluir plenamente todo uso indebido que un tercero pueda llegar a hacer de la herramienta, incluso aun cuando el proveedor haya aplicado un grado de diligencia adecuado de conformidad con el estado de la técnica.

V. Breve reflexión final

ChatGPT ha supuesto un gran impacto social y ha contribuido a que la IA, en su máxima expresión, se convierta en *mainstream*.

Es cierto que toda nueva tecnología genera, en mayor o menor medida un impacto y viene acompañada de potenciales riesgos, directamente proporcionales a su nivel de desarrollo y complejidad técnica. Por ello, tratar de minimizarlos *ex ante* resulta crucial para fomentar la evolución de la IA al tiempo que se preservan adecuadamente los derechos fundamentales tanto de los usuarios de la herramienta en cuestión como de los no usuarios.

55. Excepto en las situaciones en las que ello resulte evidente debido a las circunstancias y al contexto de utilización.

56. Art. 4 c) de la Propuesta del Consejo de la Unión Europea.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

En concreto, para paliar los peligros asociados a ChatGPT (entre los que encontrábamos la posibilidad de que proporcione contenido incorrecto o sesgado, su uso inadecuado por los usuarios y los problemas de confidencialidad y privacidad), consideramos que los proveedores de servicios de IA deberían implementar medidas de seguridad y privacidad sólidas, tales como el cifrado de extremo a extremo (con el que cuentan varias aplicaciones de mensajería como Whatsapp) y políticas claras de anonimización y transparencia en el uso de datos.

A pesar de los riesgos inherentes al desarrollo tecnológico –en especial de la IA–, prohibirlo devendría una tarea completamente estéril. El tsunami tecnológico es imparable. Se trata, por tanto, de aprender a surfear las olas. Pero para ello, hemos de contar con una base estable y una técnica adecuada que nos permita lograr el equilibrio necesario para mantenernos a flote sobre la tabla.

Por ello, resulta apremiante establecer las reglas del juego. La incertidumbre siempre ha sido fiel compañera de cualquier cambio, pero con unos fundamentos sólidos elementales y unas líneas rojas inapelables, consideramos que sería posible minimizar o paliar sus riesgos.

El Reglamento de la IA promete atender a dicha necesidad de contar con una regulación básica y general en la materia que nos permita navegar el tsunami algorítmico y tratar de alcanzar el arduo equilibrio entre el desarrollo tecnológico, la minimización de los riesgos y el respeto de los derechos fundamentales de los usuarios y no usuarios. Sin embargo, aún se encuentran en fase de aprobación y, dado el rápido y exponencial desarrollo de la IA hacia sistemas cada vez más potentes y eficaces, conviene que esta se produzca cuanto antes.

ChatGPT es solo la punta del iceberg. Vendrán muchísimas más tecnologías de este tipo, más eficientes, pero también con mayor potencial lesivo. Y, para evitar que nos encontremos –otra vez– frente a nuevos "rinocerontes grises" cuyo impacto nos termine arrollando y haya que reaccionar *ex post* ante eventuales peligros para la seguridad, los derechos fundamentales y la sociedad global, conviene estar preparados con antelación. Pero no solo para abordar directamente las consecuencias de las tecnologías venideras, sino para controlarlas y adecuarlas desde su diseño y desarrollo a un marco normativo respetuoso con los derechos fundamentales, la transparencia, la seguridad y el medio ambiente, analizando sus futuribles contingencias.

Finalmente, además de esta base legislativa, consideramos que se hace indispensable empoderar a la población en el uso de las nuevas tecnologías, educándola en un empleo adecuado, ético y responsable de las herramientas digitales y en unas nociones elementales –al menos– de ciberseguridad.

Bibliografía

Adamopoulou, E., Moussaiades, L., (2020) "An Overview of Chatbot Technology", *AIAIA 2020: Artificial Intelligence Applications and Innovations*. IFIP Advances in Information and Communication Technology, vol. 584. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-49186-4_31

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

Agencia Española de Protección de Datos (13 de abril de 2023), *La AEPD inicia de oficio actuaciones de investigación a OpenAI, propietaria de ChatGPT*. https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-inicia-de-oficio-actuaciones-de-investigacion-a-openai

Agencia Española de Protección de Datos (11 de mayo de 2023), *Las autoridades de la Red Iberoamericana de Protección de Datos Personales inician una acción coordinada en relación con el servicio de ChatGPT,* https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/autoridades-ripd-inician-accion-coordinada-servicio-chatgpt

Alonso-Arévalo, J., Quinde-Cordero, M., (2023) "ChatGPT: La creación automática de textos académicos con inteligencia artificial y su impacto en la comunicación académica y educativa", *Revista Desiderata*, nº22. https://gredos.usal.es/handle/10366/152505

Borrador de enmiendas del Parlamento Europeo a la Propuesta de Reglamento sobre normas armonizadas relativas a la Inteligencia Artificial, 9 de mayo de 2023. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf

Cowen, T., (diciembre 2022), "ChatGPT Could Make Democracy Even More Messy", *The Washington Post*. https://www.washingtonpost.com/business/chatgpt-could-makedemocracy-even-more-messy/2022/12/06/e613edf8-756a-11ed-a199-927b334b939f_story.html

Garante per la protezioni dei dati personali:

a) *Provvedimento* del 30 marzo 2023 [9870832]. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9870832
b) Comunicado de 4 de abril de 2023. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9872284
c) Comunicado de 6 de abril de 2023. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9872832
d) *Provvedimento* del 11 de abril 2023 [9874702]. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9874702
e) Comunicado de 12 de abril de 2023. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9874751
f) Comunicado de 28 de abril de 2023. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9881490

García-Peñalvo, F.J., (2023) "La percepción de la Inteligencia Artificial en contextos educativos tras el lanzamiento de ChatGPT: disrupción o pánico", *Education in the Knowledge Society,* Vol. 24. https://revistas.usal.es/tres/index.php/eks/article/view/31279

Garvi Carvajal, A., (mayo de 2023), *La UE se prepara para endurecer el uso de ChatGPT.* EL PAÍS. https://cincodias.elpais.com/cincodias/2023/04/28/legal/1682678408_904956.html

Grand View Research (2023), *Chatbot Market Size, Share & Trends, Analysis Report By Application (Customer Services, Branding & Advertising), By Type, By Vertical, By Region (North America, Europe, Asia Pacific, South America), And Segment Forecasts, 2023 – 2030*. https://www.grandviewresearch.com/industry-analysis/chatbot-market

Korda, M., (enero 2023), "Could a Chatbot Teach you how to build a dirty bomb?", *OUTRIDER*. https://outrider.org/nuclear-weapons/articles/could-chatbot-teach-you-how-build-dirty-bomb

Ley Orgánica 2/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018). https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

Maslej, N., Fattotini, L., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyon, T., Manyika, J., Ngo, H., Niebles, J.C., Parli, V., Shoham, Y., Wald, R., Clark, J., Perrault, R., (2023) *The AI Index 2023 Annual Report*, AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA. https://aiindex.stanford.edu/report/

Pearl, M., (diciembre 2022), "The ChatGPT chatbot from OpenAI is amazing, creative, and totally wrong. Need ideas? Great! Need facts? Stay away!", *Mawshable* https://mashable.com/article/chatgpt-amazing-wrong

Propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial), y se modifican determinados actos legislativos de la Unión, 21 de abril de 2021. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

Propuesta del Consejo de la Unión Europea para un Reglamento sobre normas armonizadas de Inteligencia Artificial. Documento 2021/0106 (COD), de 25 de noviembre de 2022. https://artificialintelligenceact.eu/wp-content/uploads/2022/12/AIA-%E2%80%93-CZ-%E2%80%93-General-Approach-25-Nov-22.pdf

Recomanació 1/2023 en relació amb la utilització de ChatGPT i el seu impacte en la protecció de dades personals, 21 de abril de 2023. Autoridad Catalana de Protección de Datos https://apdcat.gencat.cat/web/.content/01-autoritat/normativa/documentos/Recomanacio12023_ChatGPT.pdf

Reglamento 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de 27 de abril de 2016. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Resolución del Parlamento Europeo sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley, 14 de marzo de 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.html

Rodríguez Spinelli, F., (2022), "Bots, tenemos que hablar", en *FODERTICS 10.0* (dir. Bueno de Mata, F.), Comares, Granada.

Roose, K., (diciembre 2022), "The Brilliance and Weirdness of ChatGPT", *The New York Times*. https://www.nytimes.com/2022/12/05/technology/chatgpt-ai-twitter.html

Ruíz Arébalo, J., (enero 2022) "Cisnes negros, rinocerontes grises, pandemias y meteoritos", *Global Strategy- Geopolítica y Estudios Estratégicos*. https://global-strategy.org/cisnes-negros-rinocerontes-grises-pandemias-y-meteoritos/

Shah, C., (marzo 2023), "Is ChatGPT Closer to a Human Librarian Than It Is to Google?", *Gizmodo*, https://gizmodo.com/chatgpt-ai-openai-like-a-librarian-search-google-1850238908.

Wigmore, I., (abril 2023), "Natural language generation (NLG)", *TechTarget*. https://www.techtarget.com/searchenterpriseai/definition/natural-language-generation-NLG.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 46-68
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.04

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

Theorizing a human rights- based approach to biodiversity and its justiciability in domestic and international jurisprudence

UNA TEORIZACIÓN DE UN ENFOQUE FUNDAMENTADO EN LOS DERECHOS HUMANOS A LA PROTECCIÓN DE LA BIODIVERIDAD Y SU JUSTICIABILIDAD EN LA JURISPRUDENCIA NACIONAL E INTERNACIONAL

Simona Fanni[1]
Universidad de Sevilla
simona.fanni@outlook.it 0000-0001-6865-6530

Recibido: 31 de mayo de 2023| Aceptado: 11 de junio de 2023

ABSTRACT

This paper sets out the results achieved in the framework of a research project dealing with the protection of biodiversity from the perspective of international human rights law. In particular, this study draws inspiration form the environmental case law on the rights of Nature and from a rising climate litigation wave that stands out for several prominent features, namely: the use of human rights and constitutional rights as a standard for assessing States' compliance with their obligations under international human rights law and international environmental law; the narrative of intragenerational and intergenerational equity; a renewed reading of extraterritoriality. In this respect, the most significant domestic and international decisions are analyzed, and some viable ways in which the results achieved by the case law under consideration may benefit the protection of biodiversity and its justiciability are suggested, including multi-level judicial dialogue.

KEYWORDS

Biodiversity
Human rights
Intragenerational and intergenerational equity
Extraterritoriality
Climate change
Rights of Nature

RESUMEN

El presente artículo expone los resultados conseguidos en el marco de un proyecto de investigación sobre la protección de la biodiversidad desde el punto de vista de los derechos humanos. En particular, el presente estudio se inspira en la jurisprudencia ambiental sobre los derechos de la Naturaleza y en la jurisprudencia climática que se destaca por una serie de rasgos emblemáticos, tales como: el empleo de los derechos humanos y

PALABRAS CLAVE

Biodiversidad
Derechos humanos
Equidad intrageneracional e intergeneracional
Cambio climático
Derechos de la Naturaleza

1. This research was developed in the framework of the "Margarita Salas" Postdoctoral Program, Universidad de Sevilla, and in the framework of the Research Project PID2021-122143NB-I00, of the Ministerio de Ciencia e Innovación, "Medio ambiente, seguridad y salud: nuevos retos del Derecho en el siglo XXI", whose Principal Researcher is Prof. Dr. María Isabel Torres Cazorla.

constitucionales para evaluar el cumplimento de las obligaciones estatales que se derivan del derecho internacional de los derechos humanos y del derecho ambiental internacional; el lenguaje de la equidad intrageneracional e intrergeneracional; una novedosa concepción de la extraterritorialidad. A este respecto, el presente estudio analiza las decisiones nacionales e internacionales más significativas, y teoriza que los resultados obtenidos por la jurisprudencia considerada podrían ser beneficiosos para la protección de la biodiversidad y su justiciabilidad, incluso mediante el diálogo judicial multinivel.

I. Introduction: international law and biodiversity

The international community has not overlooked the importance of tackling biodiversity The Convention on Biological Diversity 1992 and the recently adopted 'Biodiversity Beyond National Jurisdiction' Treaty are clear evidence for that Prominently, in December 2022 the UN Biodiversity Conference (COP 15) adopted the historic Kunming Montreal Global Biodiversity Framework, a landmark agreement which set "measurable goals and targets, with complete monitoring, reporting, and review arrangements to track progress complemented by a robust resource mobilisation package". The restoration of nature for present and future generations and its sustainable use are two key components of the agreement. Nevertheless, tackling the biodiversity loss remains an urgent task for the international community as, for instance, the WWF's Living Planet Report 2022 demonstrates.

Since there is an inherent interconnection between climate change and biodiversity loss, this study theorizes that the results achieved by climate litigation, as the definition of intertemporal and extraterritorial States' obligations under international human rights law and environmental law, as well as under constitutional law, may be helpful for addressing the protection of biodiversity.

In particular, Section II focuses on the innovative results that the rising climate litigation wave has been achieving, and also expands on some significant perspectives developed by environmental case law, such the recognition of the rights of Nature and its legal standing.

Subsequently, in Section III, some viables ways in which the results achieved by the jurisprudence under consideration may be beneficial for the protection of biodiversity and its justiciability are theorized.

Finally, some brief conclusions are formulated.

II. Climate litigation and its innovative results

An interesting climate litigation trend has been gaining ground at both the domestic and international level. Some prominent features can be identified: first of all, the affirmation of specific States' obligations that rely on a combined reading of international human rights law and constitutional rights, and international environmental law. Human rights and constitutional rights are used as a standard to assess States' compliance with their mitigation obligations under international environmental law, especially under the Paris

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

Agreement. *Neubauer*[2], *Urgenda*[3], *Leghari*[4] and *Shrestha*[5] are paradigmatic examples of this approach (also see, significantly, *Torres Strait Islanders*[6]; see: Leijten, 2019; Desierto, 2021; Giménez & Petit de Gabriel, 2022).

In *Neubauer*, the German Constitutional Court 'unanimously declared the Federal Climate Protection Act partly unconstitutional because it does not sufficiently protect people against future infringements and limitations of freedom rights in the wake of gradually intensifying climate change' (Kotzé, 2021, 1424; see Neubauer, especially paras. 183 ff., 195 ff. and 243), especially since it did not provide specific steps for the achievement of Germany's post-2030 goals to reduce GHG and mitigate climate change. The Court found that the indetermination of the measures to be adopted for the post-2030 period amounted to a breach of fundamental rights (Bäumler, 2021, 2).

In mid-2022, the Brazilian Constitutional Court went even further, and said that environmental treaties are human rights treaties[7] (*PBS et al.*[8]; for some comments on the judgment, see: Barroso, 2022; Neumann Ciuffo, 2022).

Reliance on human rights for tackling climate change is not a completely new approach in the landscape of international human rights law (see Voigt, 2022, Mayer, 2021a, 410). In fact, as some commentators have stressed (see Mayer, 2021a, 410), international human rights bodies have elucidated the inherent interconnection between human rights and States' obligation to mitigate climate change. In particular, the CESCR has 'suggested that '[i]n order to act consistently with their human rights

2. *Neubauer, et al. v. Germany*, Bundesverfassungsgericht [BVerfG], 24 March 2021, Case No. BvR 2656/18/1, BvR 78/20/1, BvR 96/20/1, BvR 288/20.

3. *Staat der Nederlander v. Urgenda*, Hoge Raad 20 December 2019, ECLI:NL:HR:2019:2006. *Urgenda* was the game-changer in the framework of climate litigation, as it was the first case in which a Court ordered a State to reduce its GHG emissions (by at least 25% below 1990 levels before the end of 2020) by relying on a human rights framework and on the European Convention on Human Rights – in particular, Article 2 and Article 8, which imply a positive duty for States to 'to take appropriate steps if there is a real and immediate risk to persons and the state in question is aware of that risk', including mitigation measures, consistently with the precautionary principle (*Urgenda*, para 5.2.2) (Bergkamp, 2020; Leijten, 2019).

4. *Ashgar Leghari v. Federation of Pakistan et al.*, Case No: W.P. No. 25501/2015, a September 2015, paras. 12 ff.

5. *Shrestha v. Office of the Prime Minister et al.*, Supreme Court of Nepal, December 25, 2018, Decision no. 10210, p. 12, para. 5, and p. 13 para. 6.

6. *Billy Daniel et al. v. Australia*, Human Rights Committee, CCPR/C/135/D/3624/2019 (22 September 2022).

7. The *ratio decidendi* of the judgment is emblematic, where the Court said that '[t]he Executive Branch has the constitutional duty to ensure the Climate Fund remain operational, and to annually allocate its resources for the purpose of mitigating climate change. The withholding of such resources is prohibited due to the government's constitutional duty to protect the environment […], to affirm the fundamental right to a healthy environment, and to uphold its international commitments […], as well as the constitutional principle of separation of powers' (Barroso, 2022; Neumann Ciuffo, 2022).

8. *Partido Socialista Brasileiro (PSB), Partido Socialismo e Liberdade (PSOL), Partido dos Trabalhadores (PT) e Rede Sustentabilidade v. União Federal*, ADPF 708, 2020.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

obligations,'[9] States parties should revise the nationally determined contributions (NDCs) to global mitigation action that they have communicated under the Paris Agreement' (Mayer, 2021a, 410) and the CEDAW has clarified that States have an obligation 'to effectively mitigate… climate change in order to reduce the increased disaster risk'[10].

Despite some criticism was expressed (see, for instance, Fanny Thornton and Lavanya Rajamani), also in scholarship the idea that human rights treaties are a source of mitigation obligations has progressively gained ground and, as such prominent commentators as Michael Burger and Jessica Wentz have said, there is a 'growing consensus that a mitigation obligation does exist under international human rights law' (Burger & Wentz, 2015, 205; again, see Mayer, 2021a). This view seems to even strengthen the hermeneutic importance[11] of the incorporation of the reference to human rights in the Preamble of the Paris Agreement that, as Diane Desierto stressed, 'emphasizes further that these duties form part of the objects and purposes of the treaty, and should be used as part of the interpretation of the Paris Agreement' (Desierto, 2021).

Moreover, the climate jurisprudence under consideration is characterized by the narrative of intragenerational and intergenerational equity, of sustainability, of distributive justice[12], in a fashion that recalls the words of the late Judge Cançado Trindade, who authoritatively said that '[h]uman solidarity manifests itself not only in a spatial dimension [...] but also in a temporal dimension – that is, among the generations who succeed each other in the time, taking the past, present, and future altogether'[13].

The *Neubauer* judgment offers, once again, a paradigmatic view in this respect – that might be successfully applied to the conservation of biodiversity – where the German Constitutional Court clarified that 'one generation must not be allowed to consume large portions of the CO2 budget while bearing a relatively minor share of the reduction effort, if this would involve leaving subsequent generations with a drastic reduction burden and expose their lives to serious losses of freedom' (*Neubauer*, para. 192). This statement also echoes the very core of sustainable development as wells as the principle of distributive environmental justice.

Although to a lesser extent, extraterritoriality is another prominent feature of the innovative climate litigation wave under consideration (for a thorough analysis on the extraterritorial application of multilateral environmental treaties, see Vordermayer, 2018;

9. Mayer (2021a, 410) refers to the Committee on Economic, Social and Cultural Rights (CESCR), Statement: Climate Change and the International Covenant on Economic, Social and Cultural Rights, para. 6, UN Doc. E/C.12/2018/1 (October 31, 2018).

10. Committee on the Elimination of Discrimination Against Women (CEDAW), General Recommendation No. 37 on the Gender-Related Dimensions of Disaster Risk Reduction in the Context of Climate Change, para. 14, UN Doc. CEDAW/C/GC/37 (March 13, 2018).

11. Consistently with Article 31 of the Vienna Convention on the Law of the Treaties.

12. In this respect, for example, also see: *Sacchi et al.*, para. 10.13, and *Billy Daniel et al.*, para. 8.3.

13. *Bamaca-Velasquez v. Guatemala*, Judgment, Inter-Am. Ct. H.R. (ser. A) No. 11.129, ¶ 23 (2002), (Separate Opinion of Trindade, J.).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

also see Mayer, 2021a). In this regard, this shift of paradigm is the result of the efforts of the Inter-American Court of Human Rights that, in its Advisory Opinion OC-23/17 on the Environment and Human Rights, has adopted the jurisdictional extraterritorial link of effective control[14] – which derives from a broad application of the principle of due diligence (see: Berkes, 2018; Besson, 2020; Voigt, 2022; for a wider analysis, see: Laukkanen & Laukkanen, 2022), and goes beyond the spatial and personal model that, for instance, is commonly found in the case law of the European Court of Human Rights (Oloo & Vandenhole, 2021).

The Committee on the Rights of the Child has taken up this conception in *Sacchi et al.*[15], to affirm that 'when transboundary harm occurs, children are under the jurisdiction of the State on whose territory the emissions originated for the purposes of article 5 (1) [jurisdiction] of the Optional Protocol [to the Convention on the Rights of the Child on a communications procedure (OPCP)] if there is a causal link between the acts or omissions of the State in question and the negative impact on the rights of children located outside its territory, when the State of origin exercises effective control over the sources of the emissions in question' (Sacchi et al., para. 10.7).

Significantly, also an interesting view on the interconnection between human beings, on the one hand, and the Nature as a whole and animals[16], on the other hand, can be observed in some cases in this case law, which seems to incorporate the conception of "one rights" (Stuckl, 2023) and the universal scope of the "global solidarity" inherent to the protection of Nature (*Atrato River* case[17] and *Los Cedros* case[18]; see Wesche, 2021; Prieto, 2021. In the context of environmental litigation an early view of this kind had been adopted by *Minors Oposa,* pp. 7-8, where it recalled the "'rhythm and harmony of nature" [where] [n]ature means the created world in its entirety')[19]. This may be a helpful view to protect biodiversity, even in those cases when the domestic legal order does not specifically recognize Nature as a rights bearer, which has personhood and the legal standing. In this respect, the language of conservation, sometimes with explicit reference to biodiversity,

14. More specifically, this conception is based on the State of origins' exercise of 'effective control over the activities carried out that caused the harm and consequent violation of human rights' (Advisory Opinion n. 23, para. 104(h)).

15. *Chiara Sacchi, et al v Argentina, Brazil, France, Germany and Turkey*, Committee on the Rights of the Child, CRC 104/2019-108/2019 (23 September 2020). The excerpts cited in this chapter are taken from *Chiara Sacchi, et al v Argentina*, Committee on the Rights of the Child (CRC/C/88/D/104/2019) (8 October 2021).

16. An in-depth analysis of the concept of the constitutional protection of Nature would go beyond the scope of this study; on this issue, see Wesche, 2021.

17. Corte Constitucional, Sentencia T-622/16, *Acción de Tutela Interpuesta por el Centro de Estudios para la Justicia Social "Tierra Digna" en Representación del Consejo Comunitario Mayor de la Organización Popular Campesina del Alto Atrato (Cocomopoca), el Consejo Comunitario Mayor de la Asociación Campesina Integral del Atrato (Cocomacia), la Asociación de Consejos Comunitarios del Bajo Atrato (Asocoba), el Foro Interétnico Solidaridad Choco´ (FISCH) y otros*, Bogotá, DC, diez (10) de Noviembre de Dosmil Dieciséis (2016).

18. Corte Constitucional del Ecuador, Sentencia No. 1149-19-JP/21, de 10 de Noviembre de 2021, Caso No. 1149-19-JP/20.

19. *Minors Oposa v. DENR*, Supreme Court of the Philippines, 33 I.L.M. 173 (1994).

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

was adopted on various occasions, sometimes in relation to the duties of the present generations towards future generations (in scholarship, the views of Brown Weiss, 1992, stand out), in terms of sustainability (*Neubauer*, para. 192, and *Minors Oposa*, pp. 7-8; see Kotzé, 2021; Bäumler, 2021) and intertemporality (e.g. *Atrato River*, *Future Generations*[20], *Sacchi et al.*; see: Wesche, 2021; Sandvig, Dawson, & Tjelmeland, 2023), sometimes with regard to States' mitigation obligations, in light of the threats that climate change poses to biodiversity and the irreversibility of its impact (e.g. *Atrato River*; the *D.G. Khan Cement* case[21] also referred to climate democracy). In this sense, an interesting application of the precautionary principle was made, consistently with a "re-dimensioning of the guiding principles of environmental protection" and, therefore, the application of the criterion of *in dubio pro ambiente* or *in dubio pro nautra* (*Atrato River* case).

Last but not least, this climate case law stands out for its approach to the *locus standi* (see Slobodian, 2020)[22] that, especially with reference to the intertemporality of States' obligations, has interestingly tackled the difficulties related to the non-identity of future generations (as Derek Parfit has defined it; see Parfit, 1984) (see *Future Generations*). In the context of environmental litigation, *Minors Oposa* adopted an interesting concept of 'class', that allowed the Supreme Court of the Philippines to consider '[p]etitioners minors […] [as] represent[atives] [of] their generation as well as generations yet unborn' based on the principle of intergenerational equity (*Minors Oposa*, p. 8; see: *Minors Oposa*, p. 16, Separate Concurring Opinion of Judge Feliciano). This conception could be beneficial from several viewpoints: firstly, because it may help overcome the difficulties related to the non-identity and non-existence of future generations, while also enhancing the legal standing of young generations. Secondly, but not less importantly, the view adopted in *Minors Oposa* may be particular helpful when *actiones populares* are not allowed at the domestic level or when restrictive requirements are provided with respect to environmental class actions.

With respect to the legal standing of future generations, it seems relevant to also recall the public trust doctrine and the planetary trust doctrine, which have provided a particularly effective paradigm for addressing the *locus standi* of future generations.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

20. *Luis Armando Tolosa Villabona*, Corte Suprema de Justicia [C.S.J.] [Supreme Court], Sala Civ. 5 de abril de 2018, STC4360-2018, Radicación no. 11001-22-03-000-2018-00319-01 (Colom.).

21. Supreme Court of Pakistan, *D. G. Khan Cement Company Ltd v. Government of Punjab through its Chief Secretary, Lahore, etc.*, C.P.1290-L/2019.

22. Also *Juliana – Juliana v. United States*, 217 F. Supp. 3d 1224, 1260 (D. Or. 2016) – and, again, *Urgenda* deserve special attention, although the Courts' approach in *Juliana* might have desirably been more incisive where it considered 'unnecessary to address standing of future generations plaintiffs because the youth plaintiffs had adequately alleged current harm' (Juliana, para. 252). In *Urgenda*, the Dutch Supreme Court emphasized the issue of intertemporality by stressing that 'it is without a doubt plausible that the current generation of Dutch nationals, in particular but not limited to the younger individuals in this group, will have to deal with the adverse effects of climate change in their lifetime' (*Urgenda*, para. 37), while in *Future Generations*, the Colombian Supreme Court more prominently tackled the collective dimension of the *acción de tutela*, by recognizing that it 'can be filed as long as it […] shows the connection between the violation of collective and fundamental or individual rights' (pp. 12-13).

In this respect, significantly, in *Robinson Township*[23] the Supreme Court of Pennsylvania said that '[t]he Commonwealth's obligations as trustee to conserve and maintain the public natural resources for the benefit of the people, including generations yet to come, create a right in the people to enforce the obligations' (Slobodian, 2020, 580).

A prominent achievement of environmental case law is the recognition of the personhood and of the *locus standi* of Nature, in particular of rivers, and can be found in various recent important judgments, such as *Atrato River* and *Los Cedros*, consistently with a wider trend (see, e.g., the Mar Menor legislation, and how this doctrine is gaining ground in Courts in such countries as New Zealand, Ecuador and India).

From an historic perspective, Justice Douglas' Dissenting Opinion in *Sierra Club v. Morton*[24] (and the judgment in general with respect to the *locus standi* of legal persons in environmental cases) contained an outstanding and innovative statement, which is still suggestive decades later: 'The ordinary corporation is a "person" for purposes of the adjudicatory processes, whether it represents proprietary, spiritual, aesthetic, or charitable causes. So it should be as respects valleys, alpine meadows, rivers, lakes, estuaries, beaches, ridges, groves of trees, swampland, or even air that feels the destructive pressures of modern technology and modern life'.

III. How this approach may benefit the protection of biodiversity

This case law may be beneficial from several viewpoints.

First off, because it can help to develop and to ensure the justiciability of a renewed approach to the interconnection between the human world, on the one hand, and nature – including of course, animals – on the other hand.

In this sense, the view that this case law adopts provides a coherent legal framework for the unity conveyed by the idea of "global bioethics" supported by Van Rensselear Potter and Fritz Jahr (see D'Aloia, 2019), and which is enshrined in the idea of "one rights".

This perspective is of crucial importance for the tackling the biodiversity loss and to provide an effective legal framework for the implementation and the justiciability of the Kunming-Montreal Biodiversity Framework, by also translating it into specific States' obligations, legislation and policies[25].

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

23. *Robinson Twp. v. Commonwealth*, 83 A.3d 901, 974 (Pa. 2013).
24. *Sierra Club v. Morton*, 405 U.S. 727 (1972).
25. For instance, with regard to States' obligation related to ecosystem and species health, including to halt human-induced species extinction, an interesting statement can be found in *Shresta*, where the Nepali Supreme Court found that State's failure to adopt a climate change law amounted to a breach of the constitutional right to a healthy environment, and affirmed that '[t]o address the effects of climate change through adaptation and mitigation and the high risks seen in the ecology of, *inter alia*, higher mountainous areas and to restore, including but not limited to, its ecology, accommodating following topics, a consolidated law related to climate change Act needs to be necessarily enacted' (*Shresta*, p. 13, para. 6).

What is more, the approach that the case law analyzed adopts may be crucial for the effective promotion of an ecocentric approach, that should overcome and replace the anthropocentric view that, as some commentators have stressed, still affects the international legal perspective, including the Convention on Biodiversity (without underestimating its importance. For an interesting analysis on the Convention, see Brizioli, 2019).

The narrative of intragenerational and intergenerational equity, as understood by this body of jurisprudence, may contribute to rethink our idea of sustainable development – that, as some prominent commentators have stressed, is still focused on an anthropocentric idea of the exploitation of the resources that "our common home", the Earth, offers.

For instance, this could promote an effective and consistent understanding of the ecosystem and ecosystem services, on which the human survival inherently depends.

What is more the perspective developed by the case law analyzed, through its idea of intertemporality and extraterritoriality of States' obligations under international human rights and law and environmental human rights law – as well as, importantly, constitutional law – may help to reconsider our productive system accordingly (the challenges posed by the energy crisis and energy transition deserve special mention, as well as their exacerbation due to the impact of the conflict in Ukraine and the associated international sanctions imposed on Russia. In this regard, see Sourgens, 2022). The view expressed by the German Constitutional Court in *Neubauer* (para. 192), which was recalled above, is one of the most significant examples. This is crucial for defining an appropriate framework of accountability, that may be successfully used also for addressing the role of corporations, that often operate in a transnational dimension, not only by relying on the paradigm of due diligence but by also using the idea of extraterritoriality of States' obligations as defined by the body of jurisprudence analyzed.

This may help to bridge the gaps that still need to be tackled; indeed, for instance, the theory of *forum necessitatis* and the use of such tools as, for example, the Alien Tort Statute, are not sufficient (as *Kiobel* and *Nestlé* demonstrate).

Last but not least, judicial dialogue could be a powerful tool for the improvement of the results so far achieved by both international and domestic courts.

For example, the idea of extraterritoriality promoted by this innovative climate jurisprudence may help the European Court of Human Rights (ECtHR) to reconsider the limitations of the approach it adopted in the *Banković* judgment (see Milanovic, 2011; Keller & Heri, 2022, 161; Besson, 2021), which relies on a narrower concept of jurisdiction. As was stressed in scholarship, indeed, '[s]ince its judgment in *Banković v Belgium*, it has largely displayed two models of jurisdiction: one based on territorial control, and one based on personal control' (Keller & Heri, 2022, 161; Besson, 2021). Although in *Ilascu v Russia and Moldova*, the ECtHR held that a 'State's responsibility may […] be engaged on account of acts which have sufficiently proximate repercussions on rights guaranteed by the Convention, even if those repercussions occur outside its jurisdiction' (as recalled by Clark, Liston & Kalpouzos, 2020, 4), some major changes in its approach to extraterrioriality would be desirable. The adoption of a conception of the jurisdictional extraterritorial link inspired by the idea of 'effective control' adopted by the IACtHR

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

could be crucial for effectively tackling the rising wave of climate cases in Strasbourg, for dealing with such cases as, for instance, *Duarte Agostinho and Oth. v. Portugal and Oth*, *Greenpeace Nordic and Oth. v. Norway*[26] and *Soubeste and Oth. v. Austria and Oth*. (for a broader analysis of these cases, see: Clark, Liston & Kalpouzos, 2020; Nordlander & Monti, 2022) and to pave the way for the protection of biodiversity and its justiciability in human rights terms.

Possibly, it would be desirable that also the Court of Justice of the European Union relied on the results achieved by this innovative climate litigation wave: the need to reconsider the locus standi the Court's environmental litigation may really benefit from reference to the climate case law and its conception of legal standing. It seems particularly true in light of the quite recently unsuccessful *Carvalho* case (despite the appellants had provided an interesting reading of the European Union's mitigation obligation in terms of human rights; see Pagano, 2019), and it would be important in light of the significant normative framework that the European Union has adopted in the field of biodiversity.

IV. Conclusions

The international community has taken important steps to grapple with biodiversity, in order to prevent its loss and to promote its conservation. Nevertheless, the challenges are still huge, and this study suggests that relying on the results achieved by climate litigation – and, to some extent, those achieved by environmental litigation – may help to develop effective responses. In this respect, justiciability may be an effective way to address some of the major challenges to be met, and multi-level judicial dialogue may be crucial for ensuring a wide and successful protection not only to human rights, but also to Nature and animals' rights when biodiversity is at stake, ensuring a genuine "one rights" approach.

Bibliografía

Barroso, L. J. (2022, December 5). Facing climate change in the Brazilian Supreme Court: The right to a healthy environment as a human right. *I·CONnect*. http://www.iconnectblog.com/2022/12/facing-climate-change-in-the-brazilian supreme court-the-right-to-a-healthy-environment-as-a-human-right/

Bäumler, J. (2021, June 8). Sustainable Development made justiciable: The German Constitutional Court's climate ruling on intra- and inter-generational equity. *EJIL:Talk!*. https://www.ejiltalk.org/sustainable-development-made justiciable-the-german constitutional-courts-climate-ruling-on-intra-and inter-generational-equity/

26. Th ECtHR has the chance to take a different approach than the Norwegian Constitutional Court did at the domestic level when it adopted its decision in *Arctic Oil* – which has been seen by some commentators as a missed opportunity.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

Bergkamp, L. (2020). The Dutch Supreme Court's Climate Judgment: Its Consequences and Implications for Business – Revolution Through Litigation. *European Energy and Environmental Law Review*, *29*(3), 89-97. https://doi.org/10.54648/eelr2020032

Berkes, A. (2018, March 28). A New Extraterritorial Jurisdictional Link Recognised by the IACtHR. *EJIL:Talk!*. https://www.ejiltalk.org/a-new-extraterritorial jurisdictional-link-recognised-by the-iacthr/

Besson, S. (2020). Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!. *ESIL Reflection*, *9*(1). https://esil-sedi.eu/esil-reflection-due diligence-and-extraterritorial human-rights-obligations-mind-the-gap/

Besson, S. (2021). The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts To'. *Leiden Journal of International Law*, *25*(4), 857-884. https://doi.org/10.1017/S0922156512000489

Brizioli, S. (2019). Shifting variables in regulating genetic resources: definition, legal and access. *Diritto e Processo*, 411-440.

Brown Weiss, E. (1992). In Fairness To Future Generations and Sustainable Development. *American University International Law Review*, *8*(1), 19-26.

Burger, M., & Wentz, J. (2015). Climate Change and Human Rights. In M. Faure (Ed.), *Elgar Encyclopedia of Environmental Law* (pp. 198-212). Edward Elgar Publishing.

Clark, P., Liston, G., & Kalpouzos, I. (2020, October 6). Climate change and the European Court of Human Rights: The Portuguese Youth Case. *EJIL:Talk!*. https://www.ejiltalk.org/climate change-and-the-european-court-of-human rights-the-portuguese-youth-case/

D'Aloia, A. (2019). Bioetica ambientale, sostenibilità, teoria intergenerazionale della Costituzione. *BioLaw Journal-Rivista di BioDiritto*, 2S, 645-678. https://doi.org/10.15168/2284-4503-491

Desierto, D. (2021, October 8). Just Transitions in Climate Change Actions: Are States Respecting, Promoting, and Considering Human Rights Obligations in Setting and Implementing NDCs?. *EJIL:Talk!*. https://www.ejiltalk.org/respecting human-rights-obligations-in-climate-change actions-are-states-evaluating-ndcs human-rights-impacts/

Feria-Tinta, M. (2021). Climate Change Litigation in the European Court of Human Rights: Causation, Imminence and Other Key Underlying Notions. *Europe of Rights & Liberties/Europe des Droits & Libertés*, *1*(3), 52-71.

Giménez, I. A., & Petit de Gabriel, E. W. (2022, October 24). Cambio climático y derechos humanos: el caso de los Isleños del Estrecho de Torres. *Aquiescencia. Blog de derecho internacional*. https://aquiescencia.net/2022/10/24/cambio climatico-y-derechos-humanos-el-caso-de-los-islenos-del-estrecho-de-torres/

Heri, C. (2020, December 22). The ECtHR's Pending Climate Change Case: What's Ill Treatment Got To Do With It?. *EJIL:Talk!*. https://www.ejiltalk.org/the ecthrs-pending-climate-change case-whats-ill-treatment-got-to-do-with-it/

Keller K., & Heri, C. (2022). The Future is Now: Climate Cases Before the ECtHR. *Nordic Journal of Human Rights*, 40(1), 153-174. https://doi.org/10.1080/18918131.2022.2064074

Keller K., Heri, C., & Piskóty, R.(2022). Something Ventured, Nothing Gained? Remedies before the ECtHR and Their Potential for Climate Change Cases. *Human Rights LawReview*, *22*, 1-26. https://doi.org/10.1093/hrlr/ngab030

Kotzé, L. J. (2021). Neubauer et al. versus Germany: Planetary Climate Litigation for the Anthropocene?. *German Law Journal*, *22*, 1423-1444. https://doi.org/10.1017/glj.2021.87

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

Laukkanen, V., & Laukkanen, V. (2022, November 2). The Point of No Return: The Inadequacy of the Law of State Responsibility in Finding International Responsibility for the Adverse Effects of Climate Change. *International Law Blog*. https://internationallaw.blog/2022/11/02/the point-of-no-return the inadequacy-of-the-law-of-state-responsibility-in-finding international responsiblity-for-the-adverse-effects-of-climate-change/

Leijten, I. (2019). Human rights v. Insufficient climate action: The *Urgenda* case. *Netherlands Quarterly of Human Rights*, *37*(2), 112-118. https://doi.org/10.1177/0924051919844375

Mayer, B. (2021a). Climate change mitigation as an obligation under human rights treaties?. *The American Journal of International Law*, *115*(3), 409-451. https://doi.org/10.1017/ajil.2021.9

Mayer, B. (2021b, June 3). Milieudefensie v Shell: Do oil corporations hold a duty to mitigate climate change?. *EJIL:Talk!*. https://www.ejiltalk.org/milieudefensie-v-shell-do-oil-corporations hold-a duty-to-mitigate-climate-change/

Milanovic, M. (2011). *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy*. Oxford University Press.

Neumann Ciuffo, L. (2022, 7 July). Brazil's High Court First to Declare Paris Agreement a Human Rights Treaty. *Yale Environment 360*. https://e360.yale.edu/digest/paris-agreement-human rights-treaty-brazil

Nordlander, L., & Monti, A. (2022, June 30). A new variety of rights-based climate litigation: a challenge against the Energy Charter Treaty before the European Court of Human Rights. *EJIL:Talk!*. https://www.ejiltalk.org/a-new-variety of-rights-based-climate-litigation-a challenge-against-the-energy-charter-treaty before-the-european-court-of-human-rights/

Oloo, A., & Vandenhole, W. (2021). Enforcement of extraterritorial human rights obligations in the African human rights system. In M. Gibney, G. Erdem Türkelli, M. Krajewski, W. Vandenhole (Eds.), *The Routledge Handbook on Extraterritorial Human Rights Obligations* (pp. 140-150). Routledge.

Pagano, M. (2019, October 16). Climate change litigation before EU Courts and the 'butterfly effect'. *Blogdroiteuropéen*. https://blogdroiteuropeen.com/2019/10/16/climate-change-litigation-before-eu courts-and-the-butterfly-effect-by-mario-pagano/

Parfit, D. (1984). *Reasons and Persons*. Oxford University Press.

Prieto, G. (2021). The Los Cedros Forest has Rights. *Verfassungblog*. https://verfassungsblog.de/the-los-cedros-forest-has-rights/

Rajamani, L. (2018). Human Rights in the Climate Change Regime. In J. Knox & R. Pejan (Eds.), *The human rights to a healthy environment* (pp. 236-251). Cambridge University Press.

Sandvig, J., Dawson, P., & Tjelmeland, M. (2021, June 23). Can the ECHR Encompass the Transnational and Intertemporal Dimensions of Climate Harm?. Can the ECHR Encompass the Transnational and Intertemporal Dimensions of Climate Harm?. *EJIL:Talk!*. https://www.ejiltalk.org/can-the-echr-encompass-the transnational-and-intertemporal dimensions-of-climate-harm/

Savaresi, A., & Setzer, J. (2022). Rights-based litigation in the climate emergency: mapping the landscape and new knowledge frontiers. *Journal of Human Rights and the Environment*, *13*(1), 7-34. https://doi.org/10.4337/jhre.2022.01.01

Selmi, D. (2022). *Dawn at Mineral King Valley: The Sierra Club, the Disney Company, and the Rise of Environmental Law*. University of Chicago Press.

Setzer, J., & Benjamin, H. (2019). Climate Litigation in the Global South: Constraints and Innovations. *Transnational Environmental Law*, *9*(1). 77-101. https://doi.org/10.1017/S2047102519000268

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

Setzer, J., & Higham, C. (2022). *Global trends in climate change litigation: 2022 snapshot*. Grantham Research Institute on Climate Change and the Environment and Centre for Climate Change Economics and Policy, London School of Economics and Political Science, London. https://www.lse.ac.uk/granthaminstitute/publication/global-trends-in-climate change litigation-2022/

Slobodian, L. (2020). Defending the Future: Intergenerational Equity in Climate Litigation. *The Georgetown Environmental Law Review*, *32*, 569-589.

Sourgens, F. G. (2022, February 24). Energy Lessons from the Ukraine Crisis. *EJIL:Talk!*. https://www.ejiltalk.org/energy-lessons-from-the-ukraine-crisis/

Stuckl, S. (2023). One Rights: Human and Animal Rights in the Anthropocene. Springer.

Tigre, M. A. (2021). COVID-19 and Amazonia: Rights-based approaches for the pandemic response. *RECIEL, Review of European, Comparative and International Environmental Law*, *30*(2), 162-172.

Voigt, C. (2022). The climate change dimension of human rights: due diligence and states' positive obligations. In N. Kobylarz & E. Grant (Eds.), *Human Rights and the Planet* (pp. 152-171). Edward Elgar Publishing.

Vordermayer, M. (2018). The Extraterritorial Application of Multilateral Environmental Agreements *Harvard International Law Journal*, *59*(1), 59-124.

Wang, W. (2017). The Non-Precluded Measure Type Clause in International Investment Agreements: Significances, Challenges, and Reactions. *ICSID Review*, *32*(2), 447-456.

Wesche, P. (2021). Rights of Nature in Practice: A Case Study on the Impacts of the Colombian Atrato River Decision. *Journal of Environmental Law*, *33*, 531–556.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 69-80
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.05

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

Ciberpatrullaje en el medio virtual. Delimitando conceptos

CYBERPATROL IN THE CYBERSPACE. DELIMITING CONCEPTS

Manuel Tavora Serra
Universidad de Sevilla
mtavora@us.es 0009-0002-0460-623X

Recibido: 25 de mayo de 2023 | Aceptado: 14 de junio de 2023

RESUMEN

Con el presente trabajo, queremos realizar una aproximación conceptual a la actividad que desarrollan en el medio virtual las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de sus funciones de prevención e investigación de los comportamientos delictivos sin control jurisdiccional previo, distinguiendo entre el *ciberpatrullaje*, cuando dicha actividad tiene lugar con carácter previo a un proceso penal, y la *ciberinvestigación*, cuando tiene lugar en el marco de un proceso penal previamente incoado.

PALABRAS CLAVE

Ciberpatrullaje
Ciberinvestigación
Diligencias de investigación tecnológica
Ciberespacio

ABSTRACT

With this article, we want to make a conceptual approach to the activity carried out in the cyberspace by the police forces in compliance with their functions of prevention and investigation of criminal behavior without prior judicial review, distinguishing between *cyberpatrolling*, when such activity takes place prior to a criminal process, and *cyberinvestigation*, when it takes place in the context of criminal proceedings previously initiated.

KEYWORDS

Cyberpatrolling
Cyber investigation
Technological investigation proceedings
Cyberspace

I. Palabras previas

1.1. Delimitación del objeto de estudio

El objeto de este trabajo es el examen de la actividad desarrollada en el medio virtual por las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de sus funciones de prevención e investigación de los comportamientos delictivos. En concreto, nos centraremos en los casos en que no existe control jurisdiccional previo, con el fin de verificar si es posible que, en el desarrollo y ejecución de dicha actividad de *ciberpatrullaje* y *ciberinvestigación*, los derechos fundamentales de quienes sean objeto de las mismas (fundamentalmente, quienes ocupen la posición procesal de investigado) resultan afectados.

Dentro del objeto de nuestra investigación, hemos distinguido, por un lado, la actividad de investigación policial que se verifica en un momento anterior a la incoación de un proceso penal –el denominado *ciberpatrullaje*–, y, por otro lado, la actividad de investigación policial que tiene lugar en el marco de un proceso penal ya incoado, pero que continúa sin precisar de autorización judicial previa, que nos hemos atrevido a denominar, en un intento meramente funcional y con el ánimo de diferenciarla de la anterior, como *ciberinvestigación*.

1.2. Trascendencia del objeto de estudio

Ese nuevo medio virtual común, denominado ciberespacio, encuentra sus orígenes en el proyecto ARPANET (*Real Academia de Ingeniería*, 2020). Supone uno de los hitos más trascendentales de nuestra época y, acaso, de nuestra historia, que influye en todos los ámbitos de la existencia individual y social (González Hurtado, 2013, pp. 17-57).

A pesar de los avances que comporta, y en la medida en que los sujetos que actúan en él siguen siendo –por el momento (*Müller and Bostrom AI Progress Poll*, 2014)– los mismos que en la realidad material, las modificaciones e influencias no dejan de suponer sino modalidades de conductas ya existentes con anterioridad. En el medio virtual se verifican, por tanto, unas mismas conductas que en el medio material, pero con variaciones debidas al ambiente en que se desarrollan. De esa manera, y siguiendo la misma lógica expuesta, el *ciberpatrullaje* no deja de ser una modalidad de una actividad bien conocida por la doctrina respecto de las Fuerzas y Cuerpos de Seguridad del Estado –la de prevenir e investigar la comisión de delitos–, que ha debido adaptarse a las particularidades y exigencias del medio virtual.

Ahora bien, la aplicación de las innovaciones tecnológicas a las conductas tradicionales puede aumentar su intensidad y alcance hasta tal punto que pueda entenderse que ha mutado su condición o que, al menos, sea precisa una regulación específica que garantice su encaje en el marco jurídico. Es lo que sucede con la criminalidad y la investigación policial y sus contrapartidas virtuales: el cibercrimen, por un lado, y el ciberpatrullaje y la ciberinvestigación, por otro (Ortiz Pradillo, 2013, pp. 317-319).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

Así, la magnitud cuantitativa y cualitativa de los daños que originan los *ciberdelito*s es innegable, como lo es su potencialidad global para afectar a la economía y el desarrollo tecnológico de todo el mundo(*The Economic Impact of Cybercrime and Cyber Espionage*, 2020). De igual modo, la digitalización de la información y la generación de bases de almacenamiento y tratamiento de datos, suscitan cuestiones en materia de investigación policial a un ritmo que desborda el aparato público, que se encuentra limitado por los tiempos de su propia burocracia. En este contexto, además, la necesidad de responder de manera inmediata a la realidad social ha justificado, en ocasiones, que se admita cierta relajación en determinadas garantías, lo que hace resurgir peligrosamente la idea de que las Fuerzas y Cuerpos de Seguridad pueden infringir los derechos fundamentales para desarrollar con eficiencia y eficacia sus funciones de prevención e investigación(Asencio Mellado, 2019, p. 3).

Lo cierto es que, de manera especialmente destacada en el ámbito del *ciberespacio*, la constante búsqueda de la seguridad nacional por los poderes públicos, persiguiendo una mayor eficiencia en la evitación, persecución y represión de los delitos (en especial, en la lucha contra el terrorismo), parece justificar una creciente actitud invasora en el ámbito de las telecomunicaciones que, consecuentemente, restringe gravemente los derechos fundamentales de los ciudadanos, llegando a apreciarse, incluso, la existencia de una suerte de toque de queda digital (Cabezudo Rodríguez, 2016). En este sentido, existen numerosos ejemplos: el espionaje masivo de las comunicaciones por parte la Agencia de Seguridad Nacional revelado por Snowden, otras redes tradicionales de espionaje internacional de las comunicaciones como *Echelon*; programas para la interceptación de mensajes trasmitidos por correo electrónico, como el *Carnivore* del FBI norteamericano; o, incluso, el proyecto europeo *Enfopol*. A todo ello hay que añadir las coincidentes propuestas o aprobaciones de iniciativas legislativas para dar cobertura a tales prácticas, como la *Patriot Act*, en Estados Unidos o la *Investigatory Powers Act*, en Inglaterra, la Loi relative au renseignement en Francia, o la *Gesetz zur Beschränkung des Brief, Post– und Fernmeldegeheimnisses*, en Alemania.

Todo ello ha dado forma a un nuevo paradigma calificado como de "sociedad del riesgo", en el que se abandona la idea del "Estado del bienestar" para adoptar la del "Estado de la seguridad", con la consiguiente expansión, no ya de la jurisdicción penal –que también–, sino de los poderes investigadores del Estado (Jiménez Mejía, 2014, p. 3). Esta tendencia ha trascendido al modelo económico vigente, llegando a identificarse como capitalismo de la vigilancia (Zuboff, 2019) o capitalismo de control (Lloveras Soler, 2020, p. 10).

II. Algunos conceptos preliminares

2.1. Ciberespacio y ciberdelincuencia

El *ciberespacio* es un medio que surge con la propia existencia de internet, posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas, estimula

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

el emprendimiento y el crecimiento socioeconómico y transforma a escala global los procesos productivos, especialmente con las nuevas herramientas de inteligencia artificial, robótica, *big data*, *blockchain* e *internet of things*.

En relación con las conductas delictivas, el ciberespacio, a su vez, se caracteriza por su inherente ausencia de soberanía, su débil ejercicio de la jurisdicción, la facilidad de acceso a los comportamientos delictivos y la dificultad de atribución de la autoría de las conductas que en él se desarrollan.

La doctrina, apoyándose en estudios realizados por diversas instituciones, ya ha distinguido un doble impacto de la ciberdelincuencia. Por un lado, encontraríamos el coste económico directo y mensurable, computado en función del perjuicio que ocasionara a las víctimas, que ya en 2013 se admitía entre los 100.000 y 500.000 millones de dólares (*The Economic Impact of Cybercrime and Cyber Espionage*, 2020). Por otro lado, incluso con mayor trascendencia a la hora de determinar el impacto real de las formas de ciberdelincuencia en nuestra sociedad, también se atiende a los efectos indirectos, como son las interrupciones de los servicios, la disminución de la confianza de las actividades en línea, el coste de protección de las redes, de seguros y de trabajos de recuperación de ataques informáticos, así como el daño reputacional a la marca de la empresa atacada.

El cibercrimen ya genera más beneficios que el narcotráfico -según refiere Interpol (*La ciberdelincuencia, un gran negocio*, 2022)-, y tiene unos costes que crecen un 15% anual a nivel global. Junto a lo anterior, quizás sería debido reconocer, igualmente, que un nuevo mercado de productos y servicios, el de la seguridad informática, surge por la propia existencia del peligro del cibercrimen y los ciberataques, cifrado en 2023 en 182 mil millones de dólares (*Cybersecurity Market Size & Share Analysis - Industry Research Report - Growth Trends*, 2023).

En España, el Instituto Nacional de Ciberseguridad, ha realizado diversos estudios del estado de la sociedad de la información en el escenario español y los riesgos de ciberseguridad que se detectan (*Guias Y Estudios | INCIBE-CERT | INCIBE*, 2023).

2.2. Prueba electrónica y dato informático

La LO 16/1994, de 8 de noviembre, introdujo la posibilidad, si bien genérica, de utilizar medios técnicos, electrónicos e informáticos en los órganos judiciales, modificando para ello la Ley Orgánica 6/1985, de 1 de julio. Posteriormente, La Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, fue la que de modo expreso incorporó la regulación de las nuevas tecnologías en materia probatoria al proceso (Bonet Navarro, 2020, p. 279). Así, los artículos 382 y 384 regulan la incorporación de información y datos relevantes al proceso a través de la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y similares. Seguidamente, la Ley 18/2011, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, y la Ley 42/2015, de reforma de la LEC, terminaron por consolidar la aplicación de las TICs en la administración de justicia.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

En síntesis, por prueba electrónica, informática o digital cabe entender "toda la información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio" (Bonet Navarro, 2020, p. 279). También puede definirse como "aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal" (Sanchís Crespo, 2012, p. 713).

Por su parte, el concepto de "dato informático" se define en el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001 como "toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función", así como el de "medio electrónico", que se define en el anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, como "mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía fija y móvil u otras".

Es necesario poner también en correlación estas distinciones con la oportuna diferenciación entre datos de tráfico y datos de abonado. Los primeros pueden definirse como "todos aquellos relativos a la comunicación por medio de sistema informático, generados por el sistema informático que forma parte de la cadena de comunicación, indicando origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente" (Calvo López, 2017, p. 7), mientras que los segundos quedan definidos en el artículo 18.3 del Convenio de Budapest, que indica que por datos de abonado "se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar: a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios".

La distinción es fundamental porque la ley y la jurisprudencia vienen considerando los datos de tráfico como parte del proceso comunicativo, quedando por tanto incluidos en la protección dispensada por el artículo 18.3 CE, que establece el monopolio jurisdiccional sobre su limitación. Por el contrario, los datos de abonado, en tanto que no se consideran como parte de un proceso de comunicación, quedan protegidos únicamente por el artículo 18.4 CE, que permite su afección sin necesidad de previa autorización judicial (Calvo López, 2017, p. 8).

No podemos finalizar este capítulo sin hacer una referencia, siquiera breve, a la situación en la que actualmente se encuentra el instituto de la prueba ilícita y la consiguiente regla de exclusión, de acuerdo con la doctrina de nuestro Tribunal Constitucional. Si

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

las SSTC 114/1984, de 29 de noviembre, y 85/1994, de 14 de marzo, supusieron hitos fundamentales en el régimen de la prueba ilícita en nuestro país, la STC 97/2019, de 16 de julio, ha supuesto una modificación radical de dicho instituto, declarando que la garantía de ilicitud de las pruebas obtenidas con vulneración de derechos fundamentales no está contenida por sí misma, y de forma autónoma, en el resto de las garantías del artículo 24.2 CE -como debería suceder a consecuencia de la supremacía de los derechos fundamentales en el ordenamiento jurídico- sino que, en realidad, está integrada dentro del concepto de un proceso justo y equitativo. De este modo, la obtención de pruebas con vulneración de derechos fundamentales ha pasado a ser meramente instrumental y únicamente atendible si, además, se entiende vulnerada dicha idea de un proceso justo y equitativo (Asencio Mellado, 2021, p. 192). La consecuencia natural de este giro no puede ser otra que la relajación de la regla de exclusión de la prueba ilícita, al concluir que, en la actualidad, no resulta necesario mantener un estímulo disuasorio de tal magnitud (Armenta Deu, 2020, p. 128).

2.3. Derechos fundamentales

La obtención de la prueba digital afecta a los derechos fundamentales declarados en el artículo 18 CE, esto es, la intimidad personal, el secreto de las comunicaciones, la inviolabilidad domiciliaria (en los supuestos en que el dispositivo electrónico sea hallado en el marco de una entrada y registro en domicilio), y el derecho a la autodeterminación informativa en el ámbito de la protección de datos personales.

El derecho fundamental a la intimidad personal y familiar está reconocido en el artículo 18.1 CE, junto con los derechos fundamentales al honor y a la propia imagen, y también en el artículo 8 CEDH. Su régimen se desarrolla en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Es un derecho personalísimo, exclusivo de las personas físicas, irrenunciable y que se extingue con el fallecimiento, y tiene una doble dimensión, la personal y la familiar, reconociéndose ambas intimidades como merecedoras de protección, como destacan las SSTC 124/1985, de 17 de octubre y 69/1999, de 26 de abril, y la STS 592/2011, de 12 de septiembre. En según qué circunstancias, sus fronteras respecto de otros derechos fundamentales, como los de no declarar sobre la ideología, religión o creencias propias del artículo 16.2 CE, la inviolabilidad del domicilio del artículo 18.2 CE o el secreto de las comunicaciones del artículo 18.3 CE, pueden quedar difuminadas, como, de hecho, advierte la doctrina (Etxeberria Guridi, 2011, p. 393). En definitiva, protege el ámbito personal y familiar de dignidad de los ciudadanos frente a la acción, el conocimiento y la divulgación de terceros, Como se extrae de las SSTC 231/1988, de 2 de diciembre; 197/1991, de 17 de octubre, 142/1993, de 22 de abril, 57/1994, de 28 de febrero, 98/2000, de 10 de abril, 186/2000, de 10 de julio, 70/2002, de 3 de abril, 218/2002, de 25 de noviembre, 127/2003, de 30 de junio, 23/2007, de 30 de junio o STS 882/2011, de 7 de diciembre.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

El derecho a la inviolabilidad del domicilio queda reconocido en el artículo 18.2 CE. En cuanto a su relación con el derecho fundamental a la intimidad, en la STC 94/1999, de 31 de mayo, se ha afirmado que el derecho fundamental a la inviolabilidad domiciliaria protege de forma instrumental la vida privada de una persona (Arrabal Platero, 2019, p. 130)hasta su valoración judicial, pasando por su aportación al proceso a través de los medios de prueba legalmente previstos. Para ello, son objeto de examen las diligencias de investigación, incluyendo aquellas tecnológicas, susceptibles de utilizarse en el proceso penal para la obtención de este tipo de prueba; así como la ilicitud probatoria, en general y la exclusión de la prueba tecnológica, en particular, habida cuenta de la posible vulneración de los derechos fundamentales clásicos (privacidad, secreto de las comunicaciones, inviolabilidad del domicilio. Por lo que se refiere a su contenido, constituye el poder de su titular de impedir la agresión, entrada o permanencia de un tercero en su domicilio, por ser un ámbito reservado a su libertad más íntima. En ese sentido, se ha afirmado que "el domicilio constituye el espacio físico cerrado en el que el individuo puede ejercer su libertad más amplia e íntima, quedando formalmente protegido o inmune frente a toda clase de injerencia externa" (Rives Seva, 2022, p. 55).

El derecho al secreto de las comunicaciones se encuentra reconocido en el artículo 18.3 CE. Este derecho protege el proceso de comunicación que se encuentre en marcha entre dos titulares del mismo, que pueden ser personas físicas o jurídicas, nacionales o extranjeras, tanto en cuanto a su existencia como en cuanto a su contenido, respecto de injerencias de terceros. Sin embargo, una vez que se finaliza la comunicación, la protección constitucional se tiene que realizar a través de otros derechos fundamentales, como el derecho a la intimidad. El criterio para determinar si el secreto de las comunicaciones resulta o no afectado parece ser, por tanto, si los datos de la comunicación a que se accede han sido obtenidos con interferencia o sin interferencia del proceso de comunicación (Vegas Torres, 2015, p. 6).

El derecho fundamental a la protección de datos, también conocido como derecho a la autodeterminación informativa, queda previsto en el artículo 18.4 CE –lo que, habida cuenta del momento histórico en que fue aprobada, es calificado como un hito por la doctrina (Ortega Giménez & González Martínez, 2009)–, y desarrollado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Se ha definido como "la facultad de toda persona para ejercer control sobre la información personal almacenada en medios informáticos tanto por las administraciones públicas como entidades u organizaciones privadas" (Lucena Cid, 2012). El derecho fundamental en cuestión ya fue abordado por las SSTC 290/2000 y 292/2000, de 30 de noviembre (Arrabal Platero, 2019, p. 165)hasta su valoración judicial, pasando por su aportación al proceso a través de los medios de prueba legalmente previstos. Para ello, son objeto de examen las diligencias de investigación, incluyendo aquellas tecnológicas, susceptibles de utilizarse en el proceso penal para la obtención de este tipo de prueba; así como la ilicitud probatoria, en general y la exclusión de la prueba tecnológica, en particular, habida cuenta de la posible vulneración de los derechos fundamentales clásicos (privacidad, secreto de las comunicaciones, inviolabilidad del domicilio.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

Finalmente, debemos referirnos al derecho fundamental al propio entorno virtual. En nuestro ordenamiento jurídico no existe previsión de un derecho fundamental a la privacidad informática que se considere de manera autónoma y diferenciada de la manifestación genérica del derecho a la intimidad (Martín Ríos, 2020, p. 126). En consecuencia, el derecho al propio entorno virtual es un derecho fundamental de creación jurisprudencial y recientísimo origen, concebido para amparar al conjunto de información cibernética que configura el perfil de un ciudadano en particular.

No está previsto explícitamente en nuestro ordenamiento jurídico, sino que ha sido la práctica de nuestros tribunales la que lo ha configurado, sin perjuicio de la silueta que marcan los artículos 588 y siguientes LECrim. En general, este derecho interviene cuando se accede al conjunto de información digital que acumula una persona en su dispositivo personal (Fuentes Soriano, 2020, p. 725).

Generalmente, viene a señalarse como primer reconocimiento del mismo la sentencia del Tribunal Constitucional alemán dictada el 27 de febrero de 2008, en la que, tras comprobar la insuficiencia de la protección que dispensaban frente a investigaciones tecnológicas los derechos fundamentales al libre desarrollo de la personalidad, al secreto de las comunicaciones y a la inviolabilidad del domicilio, reconoció la existencia de un nuevo derecho, que entendió como "el derecho fundamental a la garantía de confidencialidad e integridad de los grupos informáticos", cuyo objeto era "proteger la vida privada y personal de los sujetos de los derechos fundamentales contra el acceso por parte del Estado en el ámbito de las tecnologías de la información, en la medida en que el Estado posea acceso al sistema de tecnologías de la información en su conjunto y no sólo a los acontecimientos de comunicación individuales o a los datos almacenados" (Cabezudo Rodríguez, 2016, p. 42).

III. Actividad autónoma previa al proceso penal

3.1. Delimitación conceptual

En este apartado, es nuestra intención analizar esa actividad de prevención de la criminalidad que, mediante el rastreo de la red y, en general, el uso de la informática, pueden acometer las Fuerzas y Cuerpos de Seguridad del Estado sin necesidad de autorización judicial, sin que exista un destinatario específico de las averiguaciones y, en consecuencia, sin que exista un procedimiento penal incoado. Nos referimos aquí, por tanto, a la actividad de "mantenerse a la escucha" por parte de la policía, en una conducta paralela a la de que aquellos agentes que patrullan físicamente un terreno o territorio, como las calles de una ciudad, lugares con mayor densidad de personas, etc.

En la lucha contra la ciberdelincuencia, la necesidad de conseguir la máxima eficacia y precisión técnica ha obligado tanto a crear grupos especializados dentro de las Fuerzas y Cuerpos de Seguridad nacionales como a la constitución de organismos internacionales expertos en la materia. A nivel nacional, los cuerpos expertos de que disponemos son, por un lado, la Unidad de Investigación Tecnológica de la Policía Nacional y, por otro lado, el Grupo de Delitos Telemáticos de la Guardia Civil.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

La doctrina se ha venido refiriendo al *ciberpatrullaje* como aquella actividad de rastreo y sondeo de contenidos que desarrollan habitualmente las Fuerzas y Cuerpos de Seguridad del Estado en el medio *cibernético* abierto en cumplimiento de los fines preventivos e investigativos encomendados por el legislador (este matiz entendemos que es fundamental, habida cuenta de la evidente falta de legislación en materia de *ciberpatrullaje* y demás actividad "autónoma" de la policía o del Ministerio Fiscal). Es decir, se trata de la definición de la actividad de patrullaje tradicional, a la que se le han añadido las modificaciones que el medio virtual requiere.

Como hemos referido, en nuestro ordenamiento jurídico se distinguen, desde una perspectiva general, dos funciones policiales realizadas por los Cuerpos y Fuerzas de Seguridad del Estado: la prevención de la delincuencia, mediante el mantenimiento de la seguridad ciudadana y el orden público, y la investigación de delitos, que es la actividad dirigida a la búsqueda de evidencias que permitan esclarecer los hechos delictivos ya cometidos y que están siendo objeto de investigación (Velasco Núñez, 2010, p. 161). Pues bien, dentro de la primera categoría se encuentra el denominado *ciberpatrullaje*, entendido como el conjunto de actuaciones de vigilancia, prevención y evitación de ilícitos penales llevadas a cabo por la policía en el ámbito del *ciberespacio*.

Dos grandes factores intervienen en la aparición del *ciberpatrullaje* como uno de los principales interrogantes de nuestro tiempo. Por un lado, la denominada *war on terror* (Martínez Santos, 2013), término que se emplea para designar a la política desarrollada desde los atentados del 11S por Estados Unidos y el bloque occidental y que, en plena evolución de la "sociedad del riesgo" (Beck, 2013) y con la inestimable ayuda de la corriente que defiende el "Derecho penal del enemigo" ha provocado que, paulatinamente, se vayan relajando las garantías del Estado de derecho por entender que, en determinados supuestos, el fin justifica los medios. Por otro lado, el hecho de que las herramientas que se utilizan para las actividades de *ciberpatrullaje* –por naturaleza, menos intrusivas que las diligencias de investigación, que precisan de autorización judicial como regla general– son, en realidad, las mismas herramientas que se utilizan para llevar a cabo diligencias de investigación, conservando la potencialidad lesiva del derecho fundamental afectado y presentando como única diferencia el fin al que se las destina en ese momento concreto.

Estas circunstancias nos hacen concluir que es fundamental que se establezcan deberes de transparencia respecto de las herramientas utilizadas y del modo en que lo son. Ejemplo de ello es la iniciativa desarrollada por la *Public Oversight of Surveillance Technology Act*, en Nueva York (POST), que pretende obligar al departamento de policía a publicar información básica sobre las herramientas de vigilancia que utiliza y las medidas de seguridad adoptadas para proteger la libertad y derechos civiles de los ciudadanos (*The Public Oversight of Surveillance Technology (POST) Act*, 2021).

3.2. Escasa previsión normativa

Las Fuerzas y Cuerpos de Seguridad del Estado en el desempeño de sus funciones como Policía Judicial, tienen entre sus atribuciones las de garantizar la seguridad ciudadana,

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

averiguar la autoría y circunstancias de los delitos, y recoger los efectos, instrumentos y pruebas de ellos, poniéndolos a disposición de la autoridad judicial. Estas previsiones se establecen en los artículos 104 CE y 549.1 LOPJ.

Pues bien, si la función de averiguación de los delitos y puesta a disposición de sus efectos a la autoridad judicial sí goza de una regulación expresa -y, en especial, respecto de las diligencias de investigación tecnológicas desde la entrada en vigor de la LO 13/2015-, con el *ciberpatrullaje* no sucede lo mismo, no existiendo un cuerpo normativo específico y siendo necesario acudir, por analogía, a la regulación existente acerca del "patrullaje físico", que tampoco es muy abundante. Los preceptos que regulan esta actividad por parte de los Cuerpos y Fuerzas de Seguridad del Estado son los artículos 282 LECrim, 11.1 LOFFCCSS y 22.2 de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente conforme a la disposición transitoria de la Ley Orgánica 3/2018, de 5 de diciembre).

En tal sentido se pronunciaba la STC 115/2013: "En segundo término, los agentes policiales actuaron en el presente caso con el apoyo legal que les ofrecen el artículo 282 de la Ley de enjuiciamiento criminal, el artículo 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de fuerzas y cuerpos de seguridad, y el artículo 14 de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana, que conforman "una habilitación legal específica que faculta a la policía para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente" (SSTC 70/2002, FJ 10, y 173/2011, de 7 de noviembre, FJ 2). Entre estas diligencias se encuentra la de examinar o acceder al contenido de esos instrumentos o efectos, así como a los documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que ello sea necesario de acuerdo con una estricta observancia de los requisitos dimanantes del principio de proporcionalidad (SSTC 70/2002, FJ 10, y 173/2011, FJ 2)."

La ausencia de normativa específica reguladora al respecto es destacable, porque, aunque es cierto que el monopolio jurisdiccional está previsto exclusivamente para cuando se afecta al derecho fundamental al secreto de las comunicaciones y para algunas manifestaciones del derecho a la intimidad, como la inviolabilidad del domicilio, también es cierto que toda injerencia en un derecho fundamental –con independencia de la exigencia de la previa autorización judicial o no– debe estar suficientemente prevista en el ordenamiento jurídico a fin de superar el triple requisito exigido por el artículo 8.2 CEDH. Estos tres requisitos necesarios para que una injerencia en el derecho a la vida privada pueda considerarse legítima son los siguientes: i) que la injerencia esté prevista en la ley, que se identifica con el derecho nacional en una perspectiva material –puede admitirse dentro de dicho concepto los criterios jurisprudenciales asentados; ii) que la injerencia obedezca a uno de los fines legítimos previstos en el artículo 8.2 CEDH: seguridad nacional, seguridad pública, bienestar económico del país, defensa del orden y prevención del delito, protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás; y iii) que la injerencia sea necesaria en una sociedad democrática, elemento este en el que se ubica el principio de proporcionalidad en sentido estricto.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

Esta circunstancia, además, no es nueva, sino que ya ha sido puesta de manifiesto por la doctrina hace algún tiempo (Nieva Fenoll, 2008, p. 5), incluso en relación con el patrullaje y las técnicas de investigación "tradicionales", señalándose el olvido casi crónico en que incurre el legislador a la hora de establecer una regulación específica sobre la actividad de investigación, vigilancia, seguimiento y averiguación de la policía y una suerte de asunción espontánea -a nuestro juicio, injustificada- por parte de los agentes policiales y judiciales de que, para mantener la eficacia de dichas actividades, es necesario que el detalle de las mismas permanezca en secreto. Este convencimiento, además, parece amparar no sólo el *modus operandi* en general, sino, incluso, las actividades concretas de investigación previa a la instrucción (patrullaje), en las que parece concluirse -a nuestro juicio, sin suficiente justificación- que es necesario mantener cierto sigilo sobre la actuación policial.

3.3. Manifestaciones del fenómeno

El contenido material del *ciberpatrullaje* puede identificarse con la llamada inteligencia sobre fuentes abiertas, u *open–source intelligence* (OSINT), que es una práctica consistente en recabar datos e información de fuentes disponibles al público con la finalidad de obtener información suficiente sobre una determinada circunstancia, escenario o decisión relacionada con la seguridad nacional, la aplicación del ordenamiento jurídico o, incluso, con la inteligencia de negocios. Su utilidad reside en que, mediante el tratamiento adecuado, permite extraer una funcionalidad no prevista de datos públicamente disponibles, aprovechando las sinergias que pasan desapercibidas al resto de ciudadanos.

La inteligencia sobre fuentes abiertas puede ofrecer resultados muy relevantes en la lucha contra la cibercriminalidad y la protección frente a injerencias extranjeras. Ahora bien, la potencialidad de dichas técnicas provoca que supongan también un grave riesgo para la privacidad de los ciudadanos, pues el acceso y tratamiento de tales datos pueden servir para multitud de fines difíciles de controlar, como trazar perfiles de la ciudadanía, construir sistemas de previsión de riesgo delictivo, etc.

No podemos, además, dejar de hacer referencia al empleo de técnicas de policía predictiva, búsquedas paramétricas en redes p2p, empleo de drones y acceso a imágenes públicas. Todas estas técnicas, además, se apoyan cada vez más en sistemas de inteligencia artificial y tratamiento automatizado de datos.

IV. Actividad autónoma durante el proceso penal

4.1. Facultades de investigación autónoma auténtica

Los poderes de investigación autónomos –en tanto que no precisan de autorización judicial– que han sido conferidos por el legislador a la Policía Judicial con ocasión de la reforma operada por la LO 13/2015 se encuentran recogidos en los ya mencionados artículos 588 *ter* k), 588 *ter* l) y 588 *ter* m) LECrim, y deben acordarse en el marco de un proceso penal debidamente incoado.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

La primera de las posibilidades de investigación autónoma consiste en identificar direcciones IP, prevista en el artículo 588 *ter* e. Como se puede apreciar, la propia redacción del artículo no se refiere en sentido expreso a la actividad de obtención de direcciones IP asociadas a una conexión cibernética, sino que, dando ello por sentado, regula la necesidad de que la Policía Judicial deba solicitar a la autoridad judicial que requiera a las entidades obligadas a colaborar los datos necesarios para identificar y localizar al terminal y su usuario (Barrio Andrés, 2018, p. 264).

El fundamento de esta previsión se encuentra en que la dirección IP, por sí sola, no identifica a persona alguna. Su operatividad se pone de manifiesto, únicamente, cuando se interrelaciona esa dirección IP con ciertos datos de identidad conservados por las operadoras de comunicaciones. Es decir, la dirección IP no identifica, pero permite identificar; por lo tanto, su obtención no resultaría extraña a las labores policiales que regula el art. 22.2 de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente conforme a la disposición transitoria de la Ley Orgánica 3/2018, de 5 de diciembre), que permite la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, pero la identificación final del usuario mediante el cruce de ese dato con los conservados por imposición de la Ley 25/2007, sí precisará de esa autorización judicial.

La segunda de dichas posibilidades consiste en identificar terminales mediante captación de códigos IMSI, IMEI o MAC, prevista en el artículo 588 *ter* l. La averiguación de esos códigos utilizando medios tecnológicos posibilita la identificación del número de teléfono que emplea el sujeto investigado e, incluso, su geolocalización en un punto geográfico relativamente preciso, desde el que esté efectuando la llamada (Delgado Martín, 2018, p. 452). La falta de exigencia de autorización judicial deriva del extendido conocimiento de que los dispositivos utilizados para averiguar estos identificadores no acceden al contenido de las comunicaciones. Sin embargo, resulta de gran importancia destacar que ocurre más bien lo contrario, pues los *IMSI catchers* pueden acceder al contenido de dichas comunicaciones, afectar a la cobertura del aparato, así como a los metadatos, claves de cifrados, datos de geolocalización e, incluso, escribir y acceder datos sobre la memoria del terminal móvil interceptado (Barrio Andrés, 2018, p. 265).

Por último, la policía judicial tiene la facultad también de identificar titulares, terminales o dispositivos de conectividad, prevista en el artículo 588 *ter* m LECrim. Se trata, en realidad, de un supuesto de cesión de datos concernientes a la titularidad o identificación de un dispositivo electrónico –desvinculados de los procesos de comunicación– a favor del Ministerio Fiscal o de la Policía, sin necesidad de autorización judicial, tal y como afirma la LO 13/2015 en su exposición de motivos (Calvo López, 2017, p. 25).

En el marco de esta diligencia de investigación se ha venido planteando cierta problemática entre la Policía Judicial y el Ministerio Fiscal, por una parte, y los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, de otro lado. Esta controversia tiene su origen en el artículo 3 LDCE, que los incluye entre los datos objeto de conservación. El problema surge cuando los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información,

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

al recibir las solicitudes de la Policía o del Ministerio Fiscal con apoyo en el artículo 588 *ter* m LECrim, se niegan a facilitarlos y aducen que, en atención a los artículos 3 y 6 LDCE, es necesaria autorización judicial para ello. Generalmente, se considera que la aparente contradicción entre el artículo 588 *ter* m LECrim y el artículo 6 LDCE debe resolverse, en este particular caso, a favor de la primera, por aplicación del criterio *lex posterior derogat anterior* (Barrio Andrés, 2018, p. 268).

4.2. Facultades de investigación autónoma en supuestos de urgencia

Como ya hemos tenido ocasión de exponer, la adopción de medidas de investigación tecnológica exige autorización judicial con carácter previo a su práctica, dado que con ellas se afectan generalmente los derechos fundamentales a la intimidad, propia imagen, inviolabilidad domiciliaria, secreto de comunicaciones y privacidad informática, entre otros.

Sin embargo, no es menos cierto que es posible que la policía adopte dichas medidas de manera anticipada, prescindiendo de autorización judicial habilitante, siempre que exista una situación de urgencia justificada (Velasco Núñez, 2010, p. 273). La cuestión es, claro está, determinar en qué consiste dicha urgencia.

4.3. Principios aplicables en todo caso

En los artículos 588 *bis* a) y siguientes LECrim se contiene el régimen jurídico común a las medidas de investigación tecnológica que, como sabemos, suponen una injerencia en los derechos fundamentales del artículo 18 CE. La propia ubicación sistemática del precepto evidencia que su contenido es de aplicación a todas las medidas de investigación digitales: interceptación de las comunicaciones telefónicas y telemáticas, interceptación de las comunicaciones telefónicas y telemáticas, captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, registro de dispositivos de almacenamiento masivo de información, y registros remotos sobre equipos informáticos, así como medidas de aseguramiento. Esto es necesariamente destacable porque -como hemos expuesto anteriormente- determinaría qué medidas, aun no precisando de autorización judicial, sí deben someterse a los principios previstos en dichos artículos.

Respecto del principio de especialidad, el apartado segundo del artículo 588 *bis* a) LECrim exige que la medida esté relacionada con la investigación de un delito concreto, sin que puedan autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o, incluso, despejar sospechas sin base objetiva. En ese sentido, lo que prohíbe el principio de especialidad es adoptar de manera prospectiva una medida de investigación de naturaleza tecnológica.

Por lo que se refiere al principio de idoneidad, el apartado tercero del artículo 588 *bis* a LECrim dispone que "servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad." En ese sentido, el Tribunal Supremo y el Tribunal Cons-

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

titucional han señalado que la medida es idónea cuando: i) parece adecuada a los fines de la instrucción (SSTS 85/2017, de 15 de febrero, 993/2016, de 12 de enero de 2017); ii) permite seguir avanzando en la instrucción (STS 982/2016, de 11 de enero de 2017); iii) y es susceptible de conseguir el objetivo propuesto (STC 207/1996, de 16 de diciembre).

En cuanto a los principios de excepcionalidad y necesidad, el apartado cuarto del artículo 588 *bis* a) dispone que "solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida." La idea detrás de esta regulación de supuestos alternativos ha sido la de prever escenarios excluyentes entre sí para que, en cualquiera de ellos, pueda entenderse justificado el cumplimiento de ambos principios.

En cualquier caso, una vez superados estos filtros, ha de analizarse la proporcionalidad en sentido estricto. El principio de proporcionalidad se prevé en el apartado quinto del artículo 588 *bis* a, al establecer que "las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

V. A modo de conclusión

Como podemos comprobar con los apartados anteriores, en la actualidad concurren varios factores en el ámbito de la prevención e investigación de la cibercriminalidad en el espacio:

Por un lado, la importancia del fenómeno de la cibercriminalidad en nuestra sociedad actual y en las agendas de los poderes reguladores es innegable, a la vista de su facilidad de comisión, su amplio ámbito material de actuación, y la relevancia de los intereses a que puede afectar y de las consecuencias económicas que puede tener.

Por otro lado, la búsqueda de una necesaria eficiencia y eficacia que defienda el sistema establecido provoca que se relajen garantías procesales y materiales consolidadas tras décadas de investigación científica y desarrollo social. La creciente complejidad del ámbito virtual provoca que los derechos fundamentales relativos a la intimidad, las garantías del proceso y, en particular, el instituto de la ilicitud de la prueba, representan trabas, lujos prescindibles, cuya relajación se considera conveniente a fin de alcanzar la mayor protección posible frente a la figura de la ciberdelincuencia.

Además, aunque las diligencias de investigación tecnológica, efectuadas en fase procesal, cuentan con previsión legal suficiente al respecto desde la entrada en vigor

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

de la Ley Orgánica 13/2015, de 5 de octubre, el ordenamiento jurídico español continúa sin contener previsión suficiente de las diligencias de averiguación y prevención que, con carácter preprocesal, realiza la policía en el ciberespacio (ciberpatrullaje).

Paralelamente, se aprecian tendencias conducentes a establecer la responsabilidad de los prestadores de servicios e intermediarios de internet por los contenidos de los propios usuarios. Esta atribución supondría, en consecuencia, imponerles la obligación de desplegar una diligencia activa, con facultades de revisión de los datos de los usuarios.

De igual modo, se traslada al usuario el acto de otorgar consentimiento a injerencias en su privacidad por el mero hecho de utilizar un servicio determinado. De esta forma, es la propia compañía prestadora de los servicios la que, además de disponer de los datos de conducta de sus usuarios, asume el esfuerzo de patrullar y analizar los mismos y quien traslada a la policía noticia de aquellas conductas o contenidos potencialmente ilícitos.

De esta manera, se puentea el régimen de garantías y exigencias legalmente establecido para proscribir las investigaciones que no vayan dirigidas a un sujeto específico por razones concretas, la actividad de patrullaje se traslada a los propios prestadores del servicio, y se construye un nuevo consentimiento tácito por parte del usuario.

Bibliografía

Armenta Deu, T. (2020). Prueba ilícita y regla de exclusión: Perspectiva subjetiva. *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, ISBN 978-84-945088-7-5, págs. 117-140*, 117-140.

Arrabal Platero, P. (2019). *La prueba tecnológica: Aportación, práctica y valoración*. Tirant lo Blanch.

Asencio Mellado, J. M. (2019). La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita. *Diario La Ley*, *9499*.

Asencio Mellado, J. M. (2021). La prueba ilícita y su triste destino. *La Administración de Justicia en España y en América, Vol. I*, 175-197.

Barrio Andrés, M. (2018). *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos* (2ª). Wolters Kluwers.

Beck, U. (2013). *La sociedad del riesgo: Hacia una nueva modernidad*. Grupo Planeta Spain.

Bonet Navarro, J. (2020). Apuntes sobre el concepto, obtención, introducción y fiabilidad de la prueba electrónica. *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, ISBN 978-84-945088-7-5, págs. 279-298*, 279-298.

Cabezudo Rodríguez, N. (2016). Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *I Jornada del Boletín del Ministerio de Justicia: Las reformas del proceso penal*, *2186*, 7-60.

Calvo López, D. (2017, febrero 16). Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: En especial la obtención de direcciones IP y numeraciones IMEI e IMSI (apartados K) a M) del art. 588 ter de la LECrim). *Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid*. Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid, Madrid.

Cybersecurity Market Size & Share Analysis—Industry Research Report—Growth Trends. (2023). https://www.mordorintelligence.com/industry-reports/cyber-security-market

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

Delgado Martín, J. (2018). *Investigación tecnológica y prueba digital en todas las jurisdicciones* (2ª edición actualizada). La Ley.

Etxeberria Guridi, J. F. (2011). La sentencia del TEDH «S. y Marper c. Reino Unido», de 4 de diciembre de 2008, sobre ficheros de ADN, y su repercusión en la normativa española. *Derecho y nuevas tecnologías, Vol. 1, 2011 (Primera parte. Nuevas tecnologías, sociedad y derechos fundamentales), ISBN 978-84-9830-276-9, págs. 393-406*, 393-406.

Fuentes Soriano, O. (2020). La prueba prohibida aportada por particulares: , A la luz de las nuevas tecnologías. *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, ISBN 978-84-945088-7-5, págs. 715-744*, 715-744.

González Hurtado, J. A. (2013). *Delincuencia informática: Daños informáticos del artículo 264 del Código penal y propuesta de reforma* [Http://purl.org/dc/dcmitype/Text]. Universidad Complutense de Madrid.

Guias Y Estudios | INCIBE-CERT | INCIBE. (2023). https://www.incibe.es/incibe-cert/publicaciones/guias-y-estudios

Jiménez Mejía, D. (2014). La crisis de la noción material de bien jurídico en el derecho penal del riesgo. *Nuevo Foro Penal*, *82*, 148-176.

La ciberdelincuencia, un gran negocio. (2022). https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAytDA3MzRVK0stKs-7Mz7M1MjAyMjAzNAYJZKZVuuQnh1QWpNqmJeYUpwIAuQrogzUAAAA=WKE

Lloveras Soler, J. M. (2020). Capitalismo de control. *Alternativas económicas*, *80*.

Lucena Cid, I. V. (2012). La protección de la intimidad en la era teconlógica: Hacia una reconceptualización. *Revista internacional de pensamiento político*, *7*, 117-144.

Martín Ríos, P. (2020). El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital. *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, ISBN 978-84-945088-7-5, págs. 1259-1270*, 1259-1270.

Martínez Santos, A. (2013). Terrorismo, proceso penal y derechos fundamentales. *Cuestiones constitucionales*, *29*, 459-466.

Müller and Bostrom AI Progress Poll. (2014, diciembre 29). AI Impacts. https://aiimpacts.org/muller-and-bostrom-ai-progress-poll/

Nieva Fenoll, J. (2008). La protección de derechos fundamentales en las diligencias policiales de investigación del proceso penal. *La ley penal: revista de derecho penal, procesal y penitenceiario*, *50*, 81-101.

Ortega Giménez, A., & González Martínez, J. A. (2009). Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial. *Diario La Ley*, *7188*, 1.

Ortiz Pradillo, J. C. (2013). El impacto de la tecnología en la investigación penal y en los derechos fundamentales. En *Problemas actuales de la justicia penal* (pp. 317-343). Colex.

Real Academia de Ingeniería. (2020). http://diccionario.raing.es/es/lema/arpanet

Rives Seva, A. P. (2022). *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo.*

Sanchís Crespo, C. (2012). La prueba en soporte electrónico. *Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio, 2012, ISBN 978-84-9903-947-3, págs. 707-734*, 707-734.

The Economic Impact of Cybercrime and Cyber Espionage. (2020). https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

The Public Oversight of Surveillance Technology (POST) Act: A Resource Page. (2021). Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page

Vegas Torres, J. (2015). Sobre el alcance del secreto de las comunicaciones. *Una filosofía del derecho en acción: homenaje al profesor Andrés Ollero, 2015, ISBN 978-84-7943-489-2, págs. 1609-1626*, 1609-1626.

Velasco Núñez, E. (2010). *La investigación de delitos cometidos a través de Internet y otras nuevas tecnologías: Cuestiones procesales* [Http://purl.org/dc/dcmitype/Text]. Universidade da Coruña.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

COMENTARIOS

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

La gestión de la ciencia, la tecnología y la innovación en los organismos públicos de investigación (OPIs) de España

THE MANAGEMENT OF SCIENCE, TECHNOLOGY AND INNOVATION IN PUBLIC RESEARCH ORGANIZATIONS (PROS) IN SPAIN

Iván Hernández Blanco
Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT)
Ivan.Hernandez@ciemat.es 0000-0003-0671-1797

Recibido: 16 de febrero de 2023 | Aceptado: 11 de junio de 2023

RESUMEN

En los últimos años el avance de la inversión en I+D+i ha crecido exponencialmente. Tras la crisis financiera de 2007-2008 y la crisis sanitaria originada por el virus SARS-CoV-2, la inversión en I+D+i en España ha alcanzado los 17.249 millones de euros en 2021, el 1,43% del PIB. Con motivo de este aumento es necesaria una forma eficaz de poder gestionar los recursos en materia de ciencia y tecnología. La financiación concedida por parte de la Unión Europea con los fondos Next Generation EU y concretamente del Mecanismo para la Recuperación y la Resiliencia (MRR) han potenciado aún más esta dotación económica para investigación en los Organismos Públicos de Investigación. Tras la reciente reforma de la Ley de la Ciencia en septiembre de 2022, se pone en marcha un camino para que en 2030 la financiación de los agentes públicos del Sistema Español de Ciencia, Tecnología e Innovación logre el 1,25 % del PIB, de conformidad con la Recomendación (UE) 2021/2122 del Consejo de 26 de noviembre de 2021 sobre un Pacto de Investigación e Innovación en Europa, de 26 de noviembre de 2021.

PALABRAS CLAVE

Ciencia
Investigación
Financiación
Gestión
Proyectos

ABSTRACT

In recent years, the advancement of investment in R+D+i has grown exponentially. After the financial crisis of 2007-2008 and the health crisis caused by the SARS-CoV-2 virus, investment in R&D in Spain has reached 17,249 million euros in 2021, 1.43% of GDP. Due to this increase, an effective way to manage resources in science and technology is necessary. The financing granted by the European Union with the Next Generation EU funds and specifically from the Mechanism for Recovery and Resilience (MRR) have further strengthened this financial allocation for research in Public Research Organizations.

KEYWORDS

Science
Research
Financing
Management
Projects

After the recent reform of the Science Law in September 2022, a path is set in motion so that in 2030 the financing of public agents of the Spanish System of Science, Technology and Innovation achieves 1.25% of GDP, of in accordance with Recommendation (EU) 2021/2122 of the Council of November 26, 2021 on a Research and Innovation Pact in Europe, of November 26, 2021.

I. Los organismos públicos de investigación de España

Para comenzar a iniciarnos en el camino de la gestión de la ciencia en España es necesario entender cómo surgieron los Organismos Públicos de Investigación en España (en adelante OPIs).

"Tras la guerra civil española, no había nada que se pareciese a lo que hoy se podría denominar una política científica y tecnológica clara" (Arana García, 2003, p. 18). Hasta que el 28 de noviembre de 1939 se crea el Consejo Superior de Investigaciones Científicas, heredero de la Junta para la Ampliación de Estudios e Investigaciones Científicas (JAE) y sustentado en el preámbulo de su ley "[...] frente a la pobreza y paralización pasadas, (España) siente la voluntad de renovar su gloriosa tradición científica". Y también con la finalidad de fomentar, orientar y coordinar la investigación científica nacional (art. 1, Ley de 24 de noviembre de 1939).

La mayoría de los OPIs que conocemos actualmente surgieron en la época del régimen franquista. El Instituto Nacional de Técnica Aeronáutica (INTA) en 1942 (Decreto de 7 de mayo de 1942), la Junta de Energía Nuclear (JEN) en 1951 (Decreto-ley de 22 de octubre de 1951) y el Instituto Nacional de Investigaciones Agrarias (INIA) en 1971 (Decreto-ley 17/1971, de 28 de octubre).

Tras la transición española, la aprobación de la Ley 13/1986, de 14 de abril, de Fomento y Coordinación General de la Investigación Científica y Técnica (en adelante LFCGICT)[1], supuso la regulación de forma homogénea a través de su artículo decimotercero como OPIs de seis grandes centros de investigación adscritos a diversos ministerios existentes en ese momento: El Consejo Superior de Investigaciones Científicas, la Junta de Energía Nuclear, que pasa a denominarse Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas, el Instituto Geológico y Minero de España, el Instituto Nacional de Técnica Aeroespacial y el Instituto Español de Oceanografía.

Asimismo, esta ley contempló la integración del Instituto Nacional de Investigaciones Agrarias, organismo autónomo adscrito al Ministerio de Agricultura, Pesca y Alimentación, también como OPI (Disposición Adicional Séptima LFCGICT).

Entre las funciones que se les encomendaba a estos organismos estaban:

- Gestionar y ejecutar los Programas Nacionales y Sectoriales que les fueran asignados en el Plan Nacional.
- Contribuir a la definición de los objetivos del Plan Nacional y colaborar en las tareas de evaluación y seguimiento de los mismos.

1. BOE núm. 93, de 18 de abril de 1986.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

— Asesorar en materia de investigación científica e innovación tecnológica a los Organismos dependientes de la Administración del Estado o de las Comunidades Autónomas que lo solicitaran (art. 14 LFCGICT).

Es el comienzo de los entes adscritos a la Administración General del Estado con potestad de formación investigadora, seguimiento del Plan Nacional de Investigación Científica y Desarrollo Tecnológico[2] y asesoramiento en materia de investigación científica y tecnológica.

Tras más de veinte años, en el año 2011 se aprueba la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación (en adelante LCTI), actualmente en vigor[3], potenciada por el avance tecnológico, la Unión Europea y el aumento de la comunidad científica en España, seis veces mayor que en 1986. Así, la premisa básica que se defiende en esta ley es la de consolidar un marco para el fomento de la investigación científica y técnica y sus instrumentos de coordinación general con un fin concreto: contribuir al desarrollo económico sostenible y al bienestar social mediante la generación, difusión y transferencia del conocimiento y la innovación (Preámbulo LCTI).

Algunos de los objetivos que pretende esta ley son:

— Fomentar la investigación científica. Promoviendo su inclusión y responsabilidad en todos sus ámbitos de conocimiento.
— Impulsar la ciencia como valor básico de la sociedad para la generación de conocimiento.
— Impulsar la ciencia abierta al servicio de la sociedad y promover el acceso abierto a los datos de investigación.
— Impulsar la transferencia de conocimiento, propiciando una eficiente colaboración público-privada que enriquezca y mejore el tejido productivo y empresarial para así crear beneficios.
— Fomentar la innovación en todos los sectores y en la sociedad.
— Promover la innovación pública.
— Contribuir a un desarrollo sostenible.
— Coordinar y potenciar el fortalecimiento de las políticas de ciencia, tecnología e innovación en la Administración General del Estado y entre las distintas Administraciones Públicas (art. 2 LCTI).
— Impulsar la cultura científica, tecnológica e innovadora a través de la educación, la formación y la divulgación en todos los sectores y en el conjunto de la sociedad.
— Promover la participación activa del sector privado y la sociedad civil en materia de investigación, desarrollo e innovación.

2. Para el fomento y la coordinación general de la investigación científica y técnica que el artículo 149,1.15, de la Constitución encomienda al Estado y, en cumplimiento de lo establecido en el artículo 44.2, de la misma, siendo los poderes públicos promotores de la ciencia y la investigación científica y técnica en beneficio del interés general (BOE núm. 311, de 29/12/1978).

3. BOE núm. 131, de 02/06/2011.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

— Promover la retención, atracción y retorno del talento científico e investigador.
— Aplicar la ciencia y la innovación como herramientas primordiales para la modernización de la economía española y para la corrección de la despoblación y de los desequilibrios territoriales.

En resumen, esta ley pretende un cambio sustancial de la investigación científica llevándola al siglo XXI, dotándola de aspectos esenciales como la inclusión, el desarrollo sostenible, dotar a la educación de una cultura científica que se acerque a la ciudadanía mediante la divulgación, y de alguna forma utilizar la ciencia como herramienta para evolucionar la sociedad española.

Por otra parte, la LCTI reconoce como Sistema Español de Ciencia, Tecnología e Innovación (en adelante SECTI), al conjunto de agentes, públicos y privados, que desarrollan funciones de financiación, de ejecución, o de coordinación, así como el conjunto de relaciones, estructuras, medidas y acciones que se implementan para promover, desarrollar y apoyar la política de investigación, el desarrollo y la innovación en todos los campos de la economía y de la sociedad. Presidido por los principios de calidad, coordinación, cooperación, eficacia, eficiencia, competencia, transparencia, internacionalización, apertura de la investigación científica, evaluación de resultados, igualdad de trato y oportunidades, inclusión y rendición de cuentas.

Además, se establecen como OPIs de la Administración General del Estado la Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC), el Instituto Nacional de Técnica Aeroespacial (INTA), el Instituto de Salud Carlos III (ISCIII), el Centro de Investigaciones Energéticas Medioambientales y Tecnológicas (CIEMAT), y el Instituto de Astrofísica de Canarias (IAC). Posteriormente, en el año 2021 se integraron en el CSIC como Centros Nacionales[4]: el Instituto Nacional de Investigación y Tecnología Agraria y Alimentaria (INIA), el Instituto Geológico y Minero de España (IGME) y el Instituto Español de Oceanografía (IEO) que, como ya recogimos anteriormente, habían sido reconocidos como OPIs con la aprobación de la Ley 13/1986, de 14 de abril.

Así, estos cinco centros de investigación pertenecientes a la Administración general del estado, proporcionan ejecución directa de actividades de investigación científica y técnica, actividades de prestación de servicios tecnológicos y otras actividades de carácter complementario, necesarias para el adecuado progreso científico y tecnológico de la sociedad. Siendo el Ministerio de Ciencia e Innovación coordinador de las actuaciones de estos organismos a través de su Secretaría General de Investigación.

De esta forma organizacional de los OPIs podemos sacar en claro el papel fundamental de la investigación pública en I+D+i. Importante labor y notable para la sociedad que deseamos construir en el futuro más próximo. Siendo el asunto, averiguar cuáles pueden ser las políticas públicas más convenientes para encontrar sentido a la I+D+i, pues, aunque el conocimiento científico es público, normalmente su implementación es casi siempre privada (Lora-Tamayo, 2019, p. 116).

4. Véase el Real Decreto 202/2021, de 30 de marzo (BOE núm. 77, de 31 de marzo de 2021).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

Después de más de once años, el reclamo del mundo científico (Cosce, 2021), y tras muchas vicisitudes, el 25 de agosto de 2022 el Congreso de los Diputados aprobó definitivamente la reforma de la Ley de la Ciencia, la Tecnología y la Innovación, entrando en vigor el día 7 de septiembre del mismo año mediante la Ley 17/2022, de 5 de septiembre (en adelante LMLCTI).

La reforma vinculada al Pacto de la Ciencia y la Innovación[5] está orientada principalmente a fortalecer las capacidades del SECTI para la mejora de su eficacia, coordinación, gobernanza y transferencia de conocimiento. Entre las medidas más importantes de esta reforma destacan[6]:

- La mejora de la carrera científica y técnica en el ámbito de la I+D+i con la modalidad de un tipo de contrato indefinido de actividades científico-técnicas para la contratación de personal investigador, técnico y de gestión (art. 23 bis LMLCTI).
- Estimular la atracción de talento a España y la movilidad del personal de investigación con facilidades para la contratación de personal extranjero y la posibilidad de la doble adscripción en nuestro país y fuera de él (arts. 2.q y 17.1 LMLCTI).
- Se redefine el contrato del investigador distinguido para atraer a personal científico de prestigio a España que gocen de una reputación internacional consolidada basada en la excelencia de sus contribuciones en el ámbito científico o técnico (art. 23 LMLCTI).
- Reducir las cargas administrativas del sector de I+D+i en materia de subvenciones públicas mediante la simplificación de procedimientos, fomentar el uso de medios electrónicos y dar prioridad al muestreo y demás actividades de comprobación económico-administrativa en la justificación de las ayudas públicas (Disposición adicional undécima LMLCTI).
- Se da por primera vez un paraguas jurídico a la igualdad de género y se establecen medidas para la igualdad efectiva en el SECTI, asegurando un abordaje dual, donde la perspectiva de género sea eje transversal de los instrumentos de planificación de los agentes públicos en ciencia, tecnología e innovación a la vez que se implementan acciones específicas (art. 4 bis y 4 ter LMLCTI).
- Se protege la financiación pública de I+D+i estable y creciente con el objetivo de que alcance el 1,25% del PIB en 2030, de conformidad con la Recomendación (UE) 2021/2122 del Consejo de 26 de noviembre de 2021 sobre el Pacto de Investigación e Innovación en Europa, de 26 de noviembre de 2021.

En definitiva, estas mejoras en el SECTI pretenden poner en marcha el progreso del personal de investigación, tan mermado en la época de la crisis económica española y

5. Véase: Pacto por la Ciencia y la Innovación del 3 de marzo de 2021. Recuperado el 01/02/2023 de https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/ciencia-e-innovacion/Documents/2021/040321-PactoCiencia.pdf

6. Recuperado el 01/02/2023 de https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/ciencia-e-innovacion/Paginas/2022/250822-aprobacion-ley-ciencia.aspx

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

de la que aún tenemos resquicios, debido a la fuga de cerebros, que causó que investigadores de prestigio acudiesen al extranjero a buscar financiación para sus investigaciones. Además, se procura acortar trámites burocráticos que hacen que el personal investigador se dedique demasiado a ellos, provocando en muchas ocasiones tedio. Y finalmente, se intenta que la inversión en I+D+i quede de alguna forma ligada a nuestro PIB para que no haya evasivas en financiación pública por parte del Gobierno de turno.

II. La agencia estatal de investigación

En la disposición adicional duodécima de la LCTI se autoriza legalmente al Gobierno, con plazo de un año, para la creación de Agencia Estatal de Investigación (en adelante AEI), orientada al fomento de la generación del conocimiento en todas las áreas del saber mediante el impulso de la investigación científica y técnica. La misma se encuentra adscrita al Ministerio de Ciencia e Innovación, está presidida por el titular de la Secretaría General de Investigación y el órgano ejecutivo es su director.

No fue hasta el año 2015 con el Real Decreto 1067/2015, de 27 de noviembre, por el que se crea la Agencia Estatal de Investigación y se aprueba su Estatuto[7], cuando finalmente se materializa un mandato retrasado durante más de cuatro años. Entró en funcionamiento como tal el día 20 de junio de 2016, siendo nombrada primera directora de la misma Marina Villegas Gracia (Resolución de 21 de junio de 2016). Igualmente, la AEI no contó con presupuesto propio hasta el año 2017 cuando recibió un total de 609 millones de euros por transferencias de los Presupuestos Generales del Estado (en adelante PGE) para el año 2017 (Ley 3/2017, de 27 de junio).

La AEI tiene como misión el fomento de la investigación científica y técnica en todas las áreas del saber mediante la asignación competitiva y eficiente de los recursos públicos, el seguimiento de las actuaciones financiadas y de su impacto, y el asesoramiento en la planificación de las acciones o iniciativas a través de las que se instrumentan las políticas de I+D+i de la Administración General del Estado (art. único, Real Decreto 1067/2015, de 27 de noviembre).

Además, el objetivo natural de la AEI es la financiación, evaluación, gestión y seguimiento de la actividad de investigación científica y técnica destinada a la generación, intercambio y explotación del conocimiento que fomente la Administración General del Estado por su sola iniciativa o en concurrencia con otras Administraciones nacionales o internacionales.

Son fines de la AEI, la promoción de la excelencia, el fomento de la colaboración entre los agentes del Sistema y el apoyo a la generación de conocimientos de alto impacto científico y técnico, económico y social, incluidos los orientados a la resolución de los grandes retos de la sociedad, y el seguimiento de las actividades financiadas (artículo 2, Estatuto de la Agencia Estatal de Investigación, en adelante EAEI).

Entre las funciones principales de la AEI destacan:

7. BOE núm. 285, de 28 de noviembre de 2015.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

— La gestión de los programas, instrumentos y actuaciones que se le adjudiquen en el marco de los Planes Estatales de Investigación Científica y Técnica y de Innovación.
— La organización y gestión de la evaluación científico-técnica previa y posterior de los programas que lleve a cabo.
— La verificación, seguimiento y evaluación posterior de las actividades financiadas por la AEI, así como el control de la justificación de las ayudas recibidas.
— El seguimiento de la gestión, financiación, justificación y resultados de actuaciones ejecutadas por la AEI, así como el asesoramiento sobre las mismas.
— La gestión de las actuaciones de I+D+i financiadas con fondos europeos y de las resultantes de la participación española en programas internacionales (art. 5 EAEI).

Para comprender la importancia del cometido de la AEI podemos observar detalladamente en la Tabla 1 la relación de convocatorias gestionadas en el año 2021, con la indicación del año de convocatoria, presupuesto, el estado actual de tramitación de la misma, la cuantía concedida (o en su caso propuesta) y el éxito en términos económicos.

Por tanto, podemos observar que, en el año 2021, la AEI contaba con un presupuesto de 1.090.917.482 € en ayudas a I+D+i y se concedieron un total de 504.053.808 €, menos de la mitad del presupuesto inicial previsto.

III. La financiación de los organismos públicos de investigación

Las capacidades científicas y tecnológicas de los OPIs, así como su tamaño y estructura son muy diversos. Su financiación depende fuertemente de las transferencias de fondos públicos que reciben a través del programa 46 de los PGE para el año 2023[8]. A estos fondos se les suman los recursos capturados externamente a través de convocatorias públicas competitivas del Plan Nacional, de las convocatorias del programa Horizonte Europea 2021-2027[9], de las convocatorias de las Comunidades Autónomas (CCAA), de los servicios ofrecidos a las administraciones públicas, de los contratos obtenidos con el sistema privado y tras la crisis sanitaria originada por el virus SARS-CoV-2 de los fondos Next Generation EU procedentes del Mecanismo para la Recuperación y la Resiliencia (MRR)[10].

8. BOE núm. 308, de 24/12/2022.
9. Recuperado el 26/01/2023 de https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
10. Recuperado el 26/01/2023 de https://ec.europa.eu/commission/presscorner/detail/es/ip_20_940

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

Tabla 1. Convocatorias gestionadas en el año 2021 por la AEI

CONVOCATORIAS GESTIONADAS EN 2021	Convocatoria	Estado	Presupuesto (€)	Concesión (€)
Predoctorales (PRE)	2021	TR	110.038.260	---
Personal Técnico de Apoyo (PTA)	2020	RC	7.020.000	6.810.000
Torres Quevedo (PTQ)	2020	RC	15.000.000	14.867.695
Doctorados Industriales (DIN)	2020	RC	4.000.000	3.940.353
Ramón y Cajal (RYC)	2020	RC	80.089.750	71.659.250
Juan de la Cierva-formación (FJC)	2020	RC	14.622.800	14.044.200
Juan de la Cierva-incorporación (IJC)	2020	RC	27.188.400	26.406.526
Proyectos de I+D+i (PID)	2021	PRP	452.000.000	---
Proyectos Europa Excelencia (ERC)	2021	RC	1.500.000	1.2825.526
Programación Conjunta Internacional (PCI)_I	2020_2	RC	5.598.026	5.447.493
Programación Conjunta Internacional (PCI)_II	2021_1	PR	13.140.834	12.936.791
Programación Conjunta Internacional (PCI)_III	2021_2	RC	14.719.412	14.397.350
Severo Ochoa / María de Maeztu (CEX)	2020	RC	40.000.000	40.000.000
Proyectos de I+D+i en líneas estratégicas, en colaboración público privada	2021	RC	86.000.000	60.718.625
Proyectos I+D+i "Pruebas de Concepto"	2021	RC	40.000.000	39.999.999
Equipamiento Científico-Técnico	2021	RC	180.000.000	180.000.000
TOTAL			**1.090.917.482**	**504.053.808**

Nota: RC: Resolución de concesión, PRP: propuesta de resolución provisional, TR: en tramitación sin llegar a PRP. Extraído del Informe General de Actividad de la Agencia Estatal de Investigación 2021 (p.10)[11]

11. Véase: Informe General de Actividad de la Agencia Estatal de Investigación 2021. Recuperado el 30/01/2023 de https://www.aei.gob.es/sites/default/files/page/field_file/2022-07/Informe%20General%20de%20Actividad%20AEI%202021.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

3.1. Programa 46 Investigación, Desarrollo, Innovación y Digitalización

El Programa 46 de los PGE para el año 2023 contempla casi 7.700[12] millones de euros en Investigación, Desarrollo, Innovación y Digitalización para el SECTI. Concretamente el programa *463B-Fomento y coordinación de la investigación científica y técnica* establece el fortalecimiento de la investigación básica para contribuir a la generación del conocimiento y, por otra parte, pretende crear un clima favorable para que las empresas se incorporen plenamente a la cultura de la innovación tecnológica con el fin de incrementar su competitividad[13].

Este programa asume como base fundamental la *Estrategia Española de Ciencia, Tecnología e Innovación 2021-2027 (EECTI)*, que tiene entre sus objetivos potenciar la capacidad de España para atraer, recuperar y retener talento. Para su consecución, se favorecerá, entre otros, el relevo generacional mediante el fomento de las vocaciones científicas, ofreciendo oportunidades a los jóvenes talentos[14] (Gráfico 1).

Extraído de Estructura de políticas de gasto y programas del Ministerio de Ciencia e Innovación del Proyecto de PGE 2023 (p.1)[15].

3.2. Plan Estatal de Investigación Científica, Técnica y de Innovación (PEICTI) 2021-2023

El Plan Estatal de Investigación Científica, Técnica y de Innovación (en adelante PEICTI), está integrado en la Estrategia Española de Ciencia, Tecnología e Innovación 2021-2027, y centra sus objetivos en el refuerzo de la I+D+i en los sectores más estratégicos tras la pandemia: salud, transición ecológica y digitalización, además de avanzar en el desarrollo y afianzamiento de la carrera científica. Entre sus objetivos destacan:

- Mejorar el modelo de gestión, estableciendo una financiación por objetivos.
- Fomentar el relevo generacional, impulsando la atracción de talento mediante el desarrollo de una carrera científica.

12. Véase el resumen orgánico por programas del presupuesto de gastos del Ministerio de Ciencia en Innovación en el Proyecto de PGE 2023. Capítulos 1 a 9. Recuperado el 02/02/2023 de https://www.sepg.pap.hacienda.gob.es/Presup/PGE2023Proyecto/MaestroDocumentos/PGE-ROM/doc/1/3/27/2/2/N_23_A_R_31_128_1_1_2_3.PDF

13. Véase la descripción de los programas del sector del Ministerio de Ciencia en Innovación en el Proyecto de PGE 2023. Programa 463B. Fomento y coordinación de la investigación científica y técnica. Recuperado el 03/02/2023 de https://www.sepg.pap.hacienda.gob.es/Presup/PGE2023Proyecto/MaestroDocumentos/PGE-ROM/doc/1/3/27/3/2/7/N_23_A_R_31_128_1_2_3_1463B_C_1.PDF

14. Aprobada por acuerdo del Consejo de Ministros el 8 de septiembre de 2020. Recuperado el 06/02/2023 de https://www.lamoncloa.gob.es/consejodeministros/referencias/documents/2020/refc20200908.pdf (p. 25) y de España, G. Ministerio de Ciencia e Innovación. (2020). *EECTI. Estrategia Española de Ciencia, Tecnología e Innovación: 2021-2027*. Recuperado el 12/02/2023 de https://www.ciencia.gob.es/InfoGeneralPortal/documento/e8183a4d-3164-4f30-ac5f-d75f1ad55059 (p.24).

15. Véase la estructura de políticas de gasto y programas del Ministerio de Ciencia e Innovación del Proyecto de PGE 2023. Recuperado el 03/02/2023 de https://www.sepg.pap.hacienda.gob.es/Presup/PGE2023Proyecto/MaestroDocumentos/PGE-ROM/doc/1/3/27/1/N_23_A_R_31_128_1_0_1.PDF

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

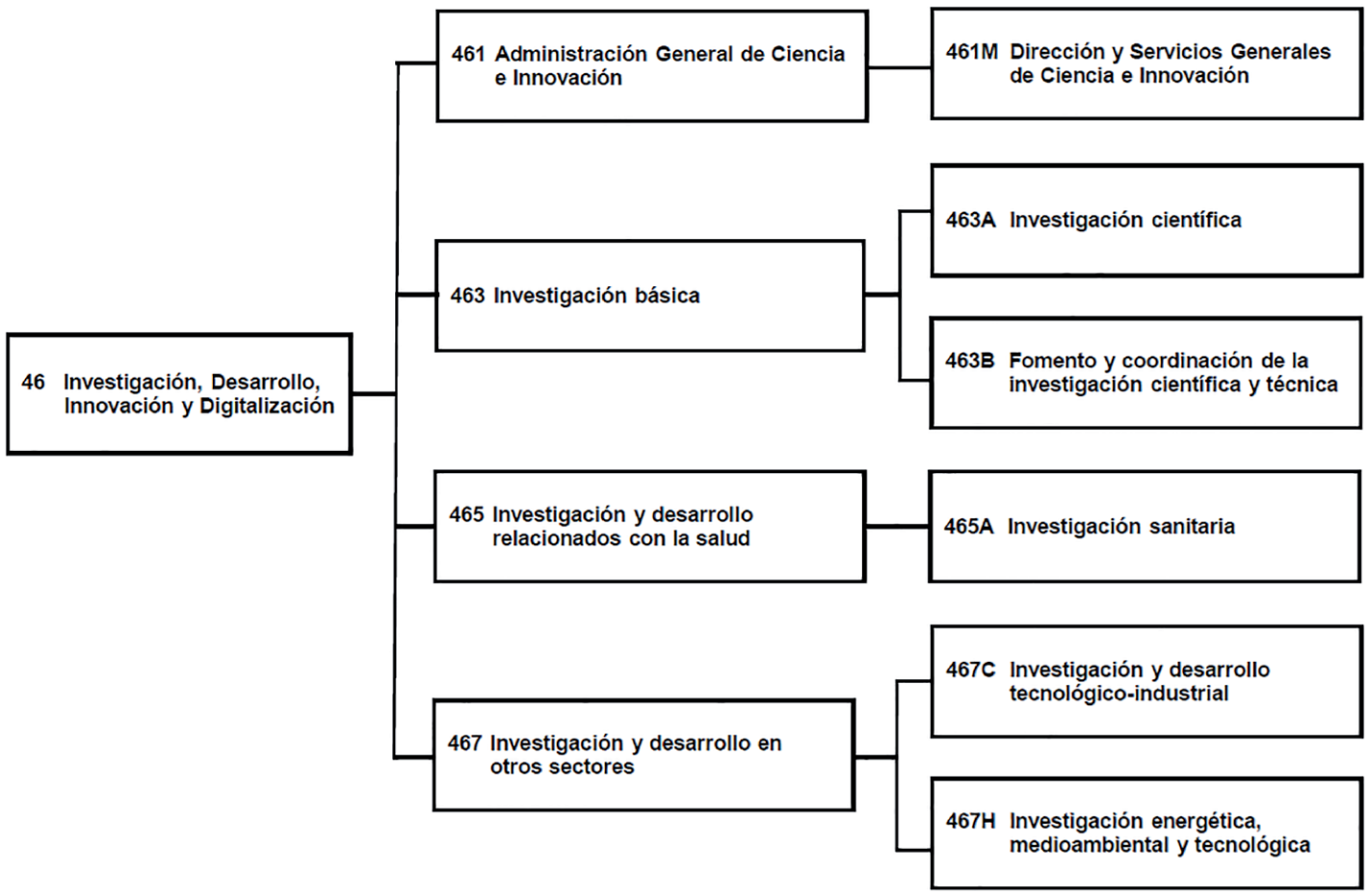
- Impulso de la investigación en líneas estratégicas (top-down).
- Particular foco en salud y medicina de vanguardia.
- Diseño conjunto entre el Gobierno y las Comunidades Autónomas de los denominados Planes Complementarios.
- Protagonismo en la construcción del Espacio Europeo de Investigación.
- Intensificar los incentivos a la transferencia de conocimiento, reforzando el vínculo entre investigación e innovación.

El PEICTI 2021-2023 instrumentaliza 4 Programas Estatales (ver Gráfico 2).

La financiación de los PEICTI ascendió a 10.835 millones de euros durante el periodo 2013-2016 y a 9.337 millones de euros durante el periodo 2017-2020. En cambio, el presupuesto ordinario para el PEICTI 2021-2023 que, además, cuenta con fondos europeos de la política de cohesión para el periodo 2021-2027, principalmente del Fondo Europeo de Desarrollo Regional (FEDER) y del Fondo Social Europeo Plus (FSE+), es de 4.295 millones de euros.

Cabe destacar que el PEICTI 2021-2023 se despliega en circunstancias extraordinarias, ya que su presupuesto ordinario se complementa con fondos extraordinarios por un valor total de más de 6.000 millones de euros, provenientes del Plan de Recuperación, Transformación y Resiliencia del Gobierno de España que utiliza fondos europeos Next Generation EU, de los que hablaremos más adelante[16].

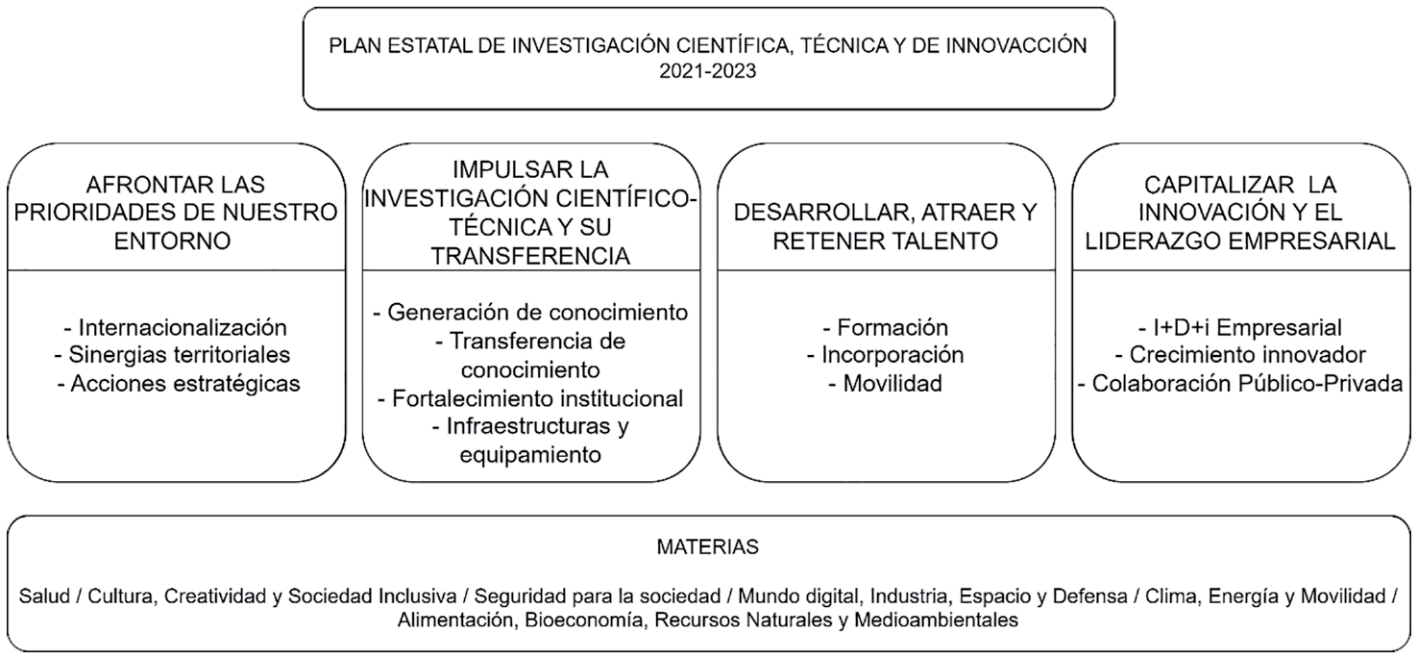
Gráfico 1. Estructura de políticas de gasto y programas del Ministerio de Ciencia Innovación 2023



16. Recuperado el 03/02/2023 de https://www.ciencia.gob.es/InfoGeneralPortal/documento/e1f-1deb1-7321-4dd9-b8ca-f97ece358d1c (pp. 66-68).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

Gráfico 2. Estructura del PEICTI 2021-2023 Extraído del Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2023 (Ministerio de Ciencia e Innovación, 2020a, p. 22)



3.3. Programa Marco: Horizonte Europa 2021-2027

El programa marco denominado Horizonte Europa, recoge el testigo del anterior Programa Horizonte 2020 (FECYT-MINECO, 2014) para seguir apoyando actividades de ciencia, tecnología e innovación en la Unión Europea desde 2021 hasta 2027. Como sus predecesores, el Programa Horizonte Europa financia actividades de alto valor añadido europeo dado que, en su mayor parte, se trata de proyectos de I+D+i ejecutados por consorcios que agrupan a participantes de múltiples países y que son concedidos en concurrencia competitiva sobre la base de evaluaciones inter pares con expertos internacionales independientes. El objetivo general del programa es alcanzar un impacto científico, tecnológico, económico y social de las inversiones de la UE en I+D+i, fortaleciendo de esta manera sus bases científicas y tecnológicas y fomentando la competitividad de todos los Estados Miembros (EEMM)[17].

Cuenta con un presupuesto de 95.517 millones de euros. Además, se ejecuta a través de otros dos programas con presupuesto propio:

— El Fondo Europeo de Defensa, que cuenta con 8.000 millones de euros para apoyar la investigación y el desarrollo en materia de defensa con el objetivo de fomentar la competitividad, la eficiencia y la capacidad de innovación de la base tecnológica e industrial europea en el sector de defensa.

17. Véase: Plan de Incentivación Horizonte Europa. Recuperado el 05/02/2023 de https://www.horizonteeuropa.es/sites/default/files/noticias/20201118_Plan%20Incentivacion%20Horizonte%20Europa_Clean_V14%20para%20SECGNAL_RR%20%28....pdf (p.3)

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

— El Programa de Investigación y Formación en fisión y fusión nuclear (EURATOM), con 1.380 millones de euros, que aborda las aplicaciones de la energía nuclear en Europa, incluyendo la seguridad física y tecnológica y la protección contra la radiación (Ministerio de Ciencia e Innovación, 2022b, p. 10).

3.4. Fondos Next Generation EU procedentes del Mecanismo para la Recuperación y la Resiliencia (MRR)

El Consejo Europeo aprobó el 21 de junio de 2020 la creación del programa NextGenerationEU, el mayor instrumento de estímulo económico jamás financiado por la Unión Europea, en respuesta a la crisis causada por el SARS-CoV-2[18].

En el marco de la iniciativa NextGenerationEU se crea un nuevo recurso financiero: el Mecanismos de Recuperación y Resiliencia (MRR), un nuevo Fondo de gestión directa en subvenciones y préstamos, en el que cada Estado miembro elabora su Plan de Recuperación para programarlos.

El Consejo de Ministros de España en su reunión del día 27 de abril de 2021, ratificó el Acuerdo por el que se aprueba el Plan de Recuperación, Transformación y Resiliencia (Resolución de 29 de abril de 2021)[19].

El Plan español se estructura en diez políticas, específicamente la sexta política "Pacto por la ciencia y la innovación y refuerzo del Sistema Nacional de Salud", las cuales se sintetizan en 30 Componentes. El Ministerio de Ciencia e Innovación es responsable del Componente 17 "Reforma institucional y fortalecimiento de las capacidades del sistema nacional de ciencia, tecnología e innovación" con una asignación de 3.380 millones de euros procedentes del Mecanismo de Recuperación y Resiliencia[20].

El objetivo es hacer frente, en el corto plazo, a la recuperación económica y social del país y, en el medio plazo, incrementar y acelerar la inversión en I+D+i de forma sostenible y en áreas estratégicas, haciendo del SECTI un instrumento clave para abordar los grandes desafíos actuales, como la transición ecológica y justa, la digitalización y el reto demográfico. El Plan tiene como fin fomentar la inversión pública y privada en I+D+i, con el fin de alcanzar en 2027 el 2,12% del PIB y acercarnos a los principales países de la Unión Europea.

Los principales retos abordados son:

1. La necesidad de reforzar la coordinación y la gobernanza del SECTI.
2. El desarrollo de una nueva carrera científica para retener y atraer el talento y mejorar la carrera investigadora.

18. Véase: Conclusiones del Consejo Europeo, 17 a 21 de julio de 2020 sobre el Plan de Recuperación y el marco financiero plurianual para 2021-2027. Recuperado el 06/02/2023 de https://www.consilium.europa.eu/media/45124/210720-euco-final-conclusions-es.pdf (p. 2).

19. BOE núm. 103, de 30 de abril de 2021.

20. Recuperado el 06/02/2023 de https://www.ciencia.gob.es/home/Estrategias-y-Planes/Plan-de-Recuperacion-Transformacion-y-Resiliencia-PRTR/NextGeneration-EU---El-Mecanismo-de-Recuperacion-y-Resiliencia-para-financiar-el-Plan;jsessionid=A6AA23CC209E78473F4F57D94C6031E9.2

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

3. La necesidad de mejorar la eficacia y eficiencia de las políticas de investigación e innovación y de fortalecer el SECTI.
4. Abordar la baja participación del sector privado y cerrar la brecha existente entre la inversión pública y la inversión privada en I+D+i.
5. La necesidad de identificar las áreas clave de la investigación y la innovación para la recuperación, transformación y resiliencia de España.

Para lograr hacer frente a estos retos, se planteó la reforma de la Ley de la Ciencia, la Tecnología y la Innovación, el desarrollo avanzado del Sistema de Información de Ciencia, Tecnología e Innovación, que facilite la toma de decisiones basadas en la evidencia, y la reorganización de los Organismos Públicos de Investigación.[21]

IV. La gestión de los proyectos de I+D+i en los OPIs

Para comprender mejor el alcance de la gestión de proyectos en materia de I+D+i debemos adentrarnos en la definición de proyecto científico.

La naturaleza científica de su objetivo a alcanzar, les dota de unas características de incertidumbre mayor que otros proyectos técnicos, en los que se detallan minuciosamente todos sus elementos. Además, están sometidos formalmente al régimen jurídico de la Ley General de Subvenciones Públicas[22], así como lo dispuesto en las convocatorias competitivas publicadas en el marco de planes de programas de ayudas a la investigación por sus entidades financiadoras (CSIC, 2021, pp. 8-9).

Una dificultad asociada a la gestión de proyectos deriva del obligado cumplimiento del régimen jurídico de las subvenciones públicas; régimen no del todo adecuado para aplicarlo a la investigación al estar pensado para el fomento de actividades económicas privadas y a proyectos que no son científicos y ocurren en periodos de tiempo relativamente cortos. Por el contrario, los proyectos científicos forman parte de un transcurso continuo, que es la línea de investigación, que se adapta a los requerimientos de distintas convocatorias de ayudas que les permiten obtener financiación en cada momento.

Con todo ello, podríamos categorizar a un proyecto, desde el ámbito de la gestión, como el un conjunto de actividades coordinadas y controladas con una fecha de inicio y otra de final, llevadas a cabo para lograr un objetivo, conforme con unos requisitos específicos que incluyen compromisos en plazo, costes y recursos (ISO 9000:2015).

De esta definición surge una imprecisa unión entre el ámbito de la gestión y el ámbito rigurosamente científico, ya que en la vida de un proyecto se mezclan, conviven e interfieren aspectos de pura gestión con cuestiones inequívocamente científicas. Así, un proyecto no es solo un "concepto científico" por la naturaleza de la actividad que se

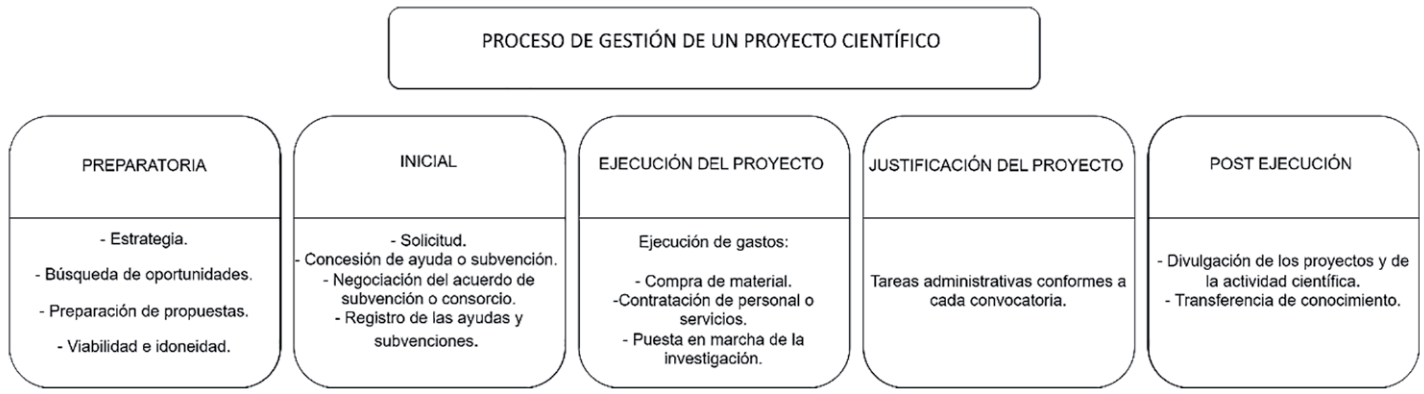
21. Véase: Plan de Recuperación, Transformación y Resiliencia. Recuperado el 06/02/2023 de https://www.ciencia.gob.es/InfoGeneralPortal/documento/d5f52341-5672-4424-99e1-0e3842c33fe7 (p. 160)
22. BOE núm. 276, de 18/11/2003.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

desarrolla, sino que es también un "concepto de gestión" en tanto que es un instrumento jurídico que integra una serie de actividades desplegadas por distintos actores junto con los procedimientos necesarios para llevarlas a cabo (CSIC, 2021, p. 9).

Por otra parte, todo proyecto se divide en distintas fases o etapas, habitualmente secuenciales, fases que determinan lo que se debe hacer en el marco del mismo, el denominado alcance del proyecto, y que permiten un control sobre la evolución del mismo y posibilitan su gestión. El conjunto de fases de un proyecto se denomina ciclo de vida del mismo. El ciclo de vida de un proyecto define el inicio y el final del mismo, así como su importancia y, por tanto, cómo se integra en el resto de operaciones del entorno en el que se desarrolla. Cada fase suele definirse en función de unos resultados previstos, relacionados con hitos, cuya consecución es un requisito o sostiene fases posteriores (López, 2004).

Gráfico 3. Ciclo de vida de un proyecto de I+D+i Elaborado a partir del Manual de Gestión de Proyectos y Actividad Científica en el CSIC (p. 35)



Vistas las etapas por las que pasan los proyectos científicos, se puede deducir la carga administrativa y burocrática que implican. Es por ello que en los últimos años ha surgido la figura del gestor de proyectos, encargado de las tareas de seguimiento, control, justificación, subsanación y finalización del mismo. Figura clave en proyectos con una fuerte financiación que conllevan una afanosa implicación justificativa. Proceso de trabajo que deriva en lograr una adecuada gestión y distribución de los fondos con los que cuenta la investigación.

Bibliografía

Acuerdo del Consejo de Ministros de 8 de septiembre de 2020 por el que se aprueba la Estrategia Española de Ciencia, Tecnología e Innovación 2021-2027 y se dispone su remisión a las Cortes Generales. Recuperado el 06/02/2023 de https://www.lamoncloa.gob.es/consejodeministros/referencias/documents/2020/refc20200908.pdf

Conclusiones del Consejo Europeo, 17 a 21 de julio de 2020 sobre el Plan de Recuperación y el marco financiero plurianual para 2021-2027. Recuperado el 06/02/2023 de https://www.consilium.europa.eu/media/45124/210720-euco-final-conclusions-es.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

Consejo Superior de Investigaciones Científicas (CSIC). (2021). *Manual de Gestión de Proyectos y Actividad Científica en el CSIC*. Recuperado el 10/02/2023 de https://delegacion.madrid.csic.es/wp-content/uploads/2021/09/CSIC-manual_proyectos_cientificos-maquetado.pdf

Cosce (2021). Informe Cosce de urgencia ante una inmediata propuesta de reforma de la Ley de la Ciencia y la Innovación (Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación). Informes Cosce. Madrid: Confederación de Sociedades Científicas de España. Recuperado el 01/02/2023 de https://aegh.org/wp-content/uploads/2021/04/Informe-COSCE-Reforma-Ley-Ciencia-abril-2021.pdf

De la Calidad, S. D. G. (2015). Fundamentos y vocabulario. *NC ISO*, *9000*. 3.4.2. Recuperado el 10/02/2023 de https://www.iso.org/obp/ui/es/#iso:std:iso:9000:ed-4:v1:es

Descripción de los programas del sector del Ministerio de Ciencia en Innovación en el Proyecto de PGE 2023. Programa 463B. Fomento y coordinación de la investigación científica y técnica. Recuperado el 03/02/2023 de https://www.sepg.pap.hacienda.gob.es/Presup/PGE2023Proyecto/MaestroDocumentos/PGE-ROM/doc/1/3/27/3/2/7/N_23_A_R_31_128_1_2_3_1463B_C_1.PDF

Estructura de políticas de gasto y programas del Ministerio de Ciencia e Innovación del Proyecto de PGE 2023. Recuperado el 03/02/2023 de https://www.sepg.pap.hacienda.gob.es/Presup/PGE2023Proyecto/MaestroDocumentos/PGE-ROM/doc/1/3/27/1/N_23_A_R_31_128_1_0_1.PDF

FECYT-MINECO, O. E. (2014). Guía del participante horizonte 2020. Recuperado el 12/02/2023 de https://www.horizonteeuropa.es/sites/default/files/inline-files/guia-del-participante-h2020.pdf

García, E. A. (2003). Organización administrativa de la ciencia y tecnología en España: el Ministerio de Ciencia y Tecnología y los organismos públicos de investigación. *Documentación administrativa*. Recuperado el 12/02/2023 de http://www.ugr.es/~sej03266/actividad/red_medicamentos/repositorio/revistas/Organizacion_administrativa_de_la_ciencia_y_tecnologia_en_Espana.pdf

Informe General de Actividad de la Agencia Estatal de Investigación 2021. Recuperado el 30/01/2023 de https://www.aei.gob.es/sites/default/files/page/field_file/2022-07/Informe%20General%20de%20Actividad%20AEI%202021.pdf

López, R. A. (2004). Gestión de Proyectos Europeos de I+ D. *Revista madri+ d*, (25)

Lora-Tamayo, E. (2019). La labor de los centros públicos de investigación. *Nueva revista de política, cultura y arte*, 171, 112-149. Recuperado el 12/02/2023 de https://reunir.unir.net/bitstream/handle/123456789/13950/La%20labor%20de%20los%20centros%20p%c3%bablicos%20de%20investigaci%c3%b3n%20EMILIO%20LORA-TAMAYO.pdf?sequence=1&isAllowed=y

Ministerio de Ciencia e Innovación. (2020a). *PEICTI. Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2023*. Recuperado el 03/02/2023 de https://www.ciencia.gob.es/InfoGeneralPortal/documento/e1f1deb1-7321-4dd9-b8ca-f97ece358d1c

Ministerio de Ciencia e Innovación. (2020b). *EECTI. Estrategia Española de Ciencia, Tecnología e Innovación: 2021-2027*. Recuperado el 12/02/2023 de https://www.ciencia.gob.es/InfoGeneralPortal/documento/e8183a4d-3164-4f30-ac5f-d75f1ad55059

Ministerio de Ciencia e Innovación. CDTI, E.P.E. y Fundación Española para la Ciencia y la Tecnología (FECYT). (2022). Guía del participante-Horizonte Europa. Recuperado el 05/02/2023 de https://www.horizonteeuropa.es/sites/default/files/noticias/Gu%C3%ADa%20del%20participante%20-%20Horizonte%20Europa%20web_0.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

Pacto por la Ciencia y la Innovación del 3 de marzo de 2021. Recuperado el 01/02/2023 de https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/ciencia-e-innovacion/Documents/2021/040321-PactoCiencia.pdf

Plan de Incentivación Horizonte Europa. Recuperado el 05/02/2023 de https://www.horizonteeuropa.es/sites/default/files/noticias/20201118_Plan%20Incentivacion%20Horizonte%20Europa_Clean_V14%20para%20SECGNAL_RR%20%28....pdf

Plan de Recuperación, Transformación y Resiliencia. Recuperado el 06/02/2023 de https://www.ciencia.gob.es/InfoGeneralPortal/documento/d5f52341-5672-4424-99e1-0e3842c33fe7

Resumen orgánico por programas del presupuesto de gastos del Ministerio de Ciencia en Innovación en el Proyecto de PGE 2023. Capítulos 1 a 9. Recuperado el 02/02/2023 de https://www.sepg.pap.hacienda.gob.es/Presup/PGE2023Proyecto/MaestroDocumentos/PGE-ROM/doc/1/3/27/2/2/N_23_A_R_31_128_1_1_2_3.PDF

Webgrafía

https://ec.europa.eu/commission/presscorner/detail/es/ip_20_940 (Recuperado el 26/01/2023).

https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en (Recuperado el 26/01/2023).

https://www.ciencia.gob.es/home/Estrategias-y-Planes/Plan-de-Recuperacion-Transformacion-y-Resiliencia-PRTR/NextGeneration-EU---El-Mecanismo-de-Recuperacion-y-Resiliencia-para-financiar-el-Plan;jsessionid=A6AA23CC209E78473F4F57D94C6031E9.2 (Recuperado el 06/02/2023).

https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/ciencia-e-innovacion/Paginas/2022/250822-aprobacion-ley-ciencia.aspx (Recuperado el 01/02/2023).

Legislación

Constitución Española. *Boletín Oficial del Estado núm. 311*, de 29 de diciembre de 1978, pp. 29313 a 29424. https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Decreto de 7 de mayo de 1942 sobre creación del Instituto Nacional de Técnica Aeronáutica. *Boletín Oficial del Estado núm. 141*, de 21 de mayo de 1942, pp. 3530 a 3531. https://www.boe.es/buscar/doc.php?id=BOE-A-1942-4587

Decreto-ley 17/1971, de 28 de octubre, por el que se modifica la Administración Institucional del Ministerio de Agricultura y se encomienda al Gobierno la reestructuración de dicho Departamento. *Boletín Oficial del Estado núm. 264*, de 4 de noviembre de 1971, pp. 17679 a 17681. https://www.boe.es/buscar/doc.php?id=BOE-A-1971-1391#:~:text=A%2D1971%2D1391-,Decreto%2Dley%2017%2F1971%2C%20de%2028%20de%20octubre%2C,a%2017681%20(3%20p%C3%A1gs.%20)

Decreto-ley de 22 de octubre de 1951 por el que se crea la Junta de Energía Nuclear. *Boletín Oficial del Estado núm. 297*, de 24 de octubre de 1951, pp. 4778 a 4779. https://www.boe.es/buscar/doc.php?id=BOE-A-1951-11120#:~:text=Decreto%2Dley%20de%2022%20de,a%204779%20(2%20p%C3%A1gs.%20)

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

Jefatura del Estado. - Ley creando el Consejo Superior de Investigaciones Científicas. *Boletín Oficial del Estado núm. 332*, de 28 de noviembre de 1939, pp. 6668 a 6671. https://www.boe.es/datos/pdfs/BOE//1939/332/A06668-06671.pdf

Ley 13/1986, de 14 de abril, de Fomento y Coordinación General de la Investigación Científica y Técnica. *Boletín Oficial del Estado núm. 93*, de 18 de abril de 1986, pp. 13767 a 13771. https://www.boe.es/buscar/doc.php?id=BOE-A-1986-9479

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. *Boletín Oficial del Estado núm. 131*, de 24 de diciembre de 2022, pp. 54387 a 54455. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-9617

Ley 17/2022, de 5 de septiembre, por la que se modifica la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación. *Boletín Oficial del Estado núm. 214*, e 6 de septiembre de 2022, pp. 123852 a 123922. https://www.boe.es/buscar/doc.php?id=BOE-A-2022-14581

Ley 3/2017, de 27 de junio, de Presupuestos Generales del Estado para el año 2017. *Boletín Oficial del Estado núm. 153*, de 28 de junio de 2017, pp. 53787 a 54396. https://www.boe.es/buscar/doc.php?id=BOE-A-2017-7387

Ley 31/2022, de 23 de diciembre, de Presupuestos Generales del Estado para el año 2023. *Boletín Oficial del Estado núm. 308*, de 24 de diciembre de 2022, pp. 180551 a 181414. https://www.boe.es/buscar/doc.php?id=BOE-A-2022-22128

Ley 38/2003, de 17 de noviembre, General de Subvenciones. *Boletín Oficial del Estado núm. 276*, de 18 de noviembre de 2003, pp 40505 a 40532. https://www.boe.es/buscar/doc.php?id=BOE-A-2003-20977

Real Decreto 1067/2015, de 27 de noviembre, por el que se crea la Agencia Estatal de Investigación y se aprueba su Estatuto. *Boletín Oficial del Estado núm. 285*, de 28 de noviembre de 2015, pp. 112457 a 112487. https://www.boe.es/buscar/doc.php?id=BOE-A-2015-12889

Real Decreto 202/2021, de 30 de marzo, por el que se reorganizan determinados organismos públicos de investigación de la Administración General del Estado y se modifica el Real Decreto 1730/2007, de 21 de diciembre, por el que se crea la Agencia Estatal Consejo Superior de Investigaciones Científicas y se aprueba su Estatuto, y el Real Decreto 404/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Ciencia e Innovación. *Boletín Oficial del Estado núm. 77*, de 31 de marzo de 2021, pp. 36471 a 36486. https://www.boe.es/buscar/doc.php?id=BOE-A-2021-5031

Recomendación (UE) 2021/2122 del Consejo de 26 de noviembre de 2021 sobre un Pacto de Investigación e Innovación en Europa. *Diario Oficial de la Unión Europea núm. 431*, de 2 de diciembre de 2021, pp. 1 a 9. https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-81674

Resolución de 21 de junio de 2016, de la Presidencia de la Agencia Estatal de Investigación, por la que se publica el Acuerdo del Consejo Rector, por el que se nombra Directora de la Agencia Estatal de Investigación a doña Marina Villegas Gracia. *Boletín Oficial del Estado núm. 152*, de 24 de junio de 2016, pp. 45723 a 45726. https://www.boe.es/buscar/doc.php?id=BOE-A-2016-6161

Resolución de 29 de abril de 2021, de la Subsecretaría, por la que se publica el Acuerdo del Consejo de Ministros de 27 de abril de 2021, por el que aprueba el Plan de Recuperación, Transformación y Resiliencia. *Boletín Oficial del Estado núm. 103*, de 30 de abril de 2021, pp. 51346 a 51349. https://www.boe.es/buscar/doc.php?id=BOE-A-2021-7053

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 99-115
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.07

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

Singapur un camino interrumpido hacia la regulación de las técnicas de reemplazo mitocondrial

SINGAPORE AN INTERRUPTED PATH TOWARDS THE REGULATION OF MITOCHONDRIAL REPLACEMENT TECHNIQUES

Marta Reguera Cabezas
Hospital Universitario Marqués de Valdecilla. Cantabria.
marta.reguera@scsalud.es 0000-0003-2252-7199

Recibido: 01 de mayo de 2023 | Aceptado: 11 de junio de 2023

RESUMEN

Las técnicas de reemplazo mitocondrial pueden reducir significativamente el riesgo de transmisión de enfermedades mitocondriales a la descendencia. Singapur estaba analizando la posibilidad de realizar cambios legislativos históricos que permitirían a las parejas afectadas por enfermedades mitocondriales hereditarias maternas la oportunidad de tener hijos genéticamente no afectados. Sin embargo, tras el informe del BAC, parece que la República de Singapur, no se convertirá en el tercer país a nivel internacional en autorizar el uso de las técnicas de reemplazo mitocondrial.

PALABRAS CLAVE

Enfermedades mitocondriales
Leyes
Técnicas de reproducción asistida
Reemplazo mitocondrial
Singapur

ABSTRACT

Mitochondrial replacement techniques can significantly reduce the risk of transmission of mitochondrial diseases to offspring. Singapore was exploring historic legislative changes that would allow couples affected by maternal inherited mitochondrial diseases the opportunity to have genetically unaffected children. However, following the BAC report, it appears that the Republic of Singapore willd not become the third country internationally to authorize the use of mitochondrial replacement techniques.

KEYWORDS

Mitochondrial diseases
Laws
Assisted reproduction techniques
Mitochondrial replacement
Singapore

I. Introducción

En este trabajo abordamos las incertidumbres científicas y ético-jurídicas planteadas por las terapias mitocondriales y los avances de Singapur en determinar la pertinencia de su autorización legislativa. Un camino prometedor para reducir la transmisión de enfermedades mitocondriales en las familias afectadas.

II. La prevención como argumento principal

Las mitocondrias son orgánulos celulares con material genético propio y de herencia materna exclusiva. Son responsables de la producción energética necesaria para la vida celular. Las enfermedades que afectan a estos orgánulos, denominadas enfermedades mitocondriales, son un grupo heterogéneo de trastornos multiorgánicos potencialmente mortales y de severidad variable (Davis et al., 2018). Se trata a su vez, de enfermedades de carácter hereditario que afectan principalmente, aunque no de forma exclusiva, a órganos y tejidos con un alto requerimiento energético, como son el cerebro o el músculo (Grady *et al.*, 2018). Son enfermedades para las que no se dispone en la actualidad de un tratamiento curativo eficaz (Pfeffer *et al.*, 2012)the heart, the liver, and kidneys, diabetes mellitus and sensorineural deafness. Current treatment is largely supportive and the disorders progress relentlessly causing significant morbidity and premature death. Vitamin supplements, pharmacological agents and exercise therapy have been used in isolated cases and small clinical trials, but the efficacy of these interventions is unclear. The first review was carried out in 2003, and identified six clinical trials. This major update was carried out to identify new studies and grade the original studies for potential bias in accordance with revised Cochrane Collaboration guidelines.\nOBJECTIVES: To determine whether there is objective evidence to support the use of current treatments for mitochondrial disease.\nSEARCH METHODS: We searched the Cochrane Neuromuscular Disease Group Specialized Register (4 July 2011.

Un grupo de estas enfermedades son aquellas que están causadas por mutaciones en el ADN mitocondrial (mtDNA). El contenido de mtDNA mutado es transmitido a la descendencia a través de los gametos femeninos (Wei & Chinnery, 2020)paving the way for two decades of discovery linking mtDNA variation with human disease. Severe pathogenic mutations cause sporadic and inherited rare disorders that often involve the nervous system. However, some mutations cause mild organ-specific phenotypes that have a reduced clinical penetrance, and polymorphic variation of mtDNA is associated with an altered risk of developing several late-onset common human diseases including Parkinson's disease. mtDNA mutations also accumulate during human life and are enriched in affected organs in a number of age-related diseases. Thus, mtDNA contributes to a wide range of human pathologies. For many decades, it has generally been accepted that mtDNA is inherited exclusively down the maternal line in humans. Although recent evidence has challenged this dogma, whole-genome sequencing has identified nuclear-encoded mitochondrial sequences (NUMTs, debido a la segregación aleatoria

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

de las mitocondrias (con y sin mutaciones). Este es un fenómeno conocido como heteroplasmia (Richardson *et al.*, 2015). Las secuencias de mtDNA no son exclusivas de un individuo, sino que son compartidas por el linaje familiar materno. Partiendo de esta premisa, en algunas familias existen varias generaciones de individuos afectados, a menudo con graves consecuencias, lo que lleva a algunas mujeres a buscar opciones para prevenir la transmisión de enfermedades a sus hijos (Yamada *et al.*, 2020).

En la actualidad las terapias de reemplazo mitocondrial, identificadas por su acrónimo en inglés MRT, se postulan como la única solución plausible a la transmisión de estas enfermedades. En concreto, la introducción del reemplazo mitocondrial en la práctica clínica podría evitar la trasmisión de la enfermedad y reducir la incidencia poblacional de la enfermedad mitocondrial en el futuro (Craven *et al.*, 2020). No obstante, estas terapias no están exentas de dilemas éticos. Dado que el mtDNA se hereda a través del gameto femenino es imprescindible la utilización de los ovocitos de una donante para la aplicación de la técnica. Ello implica la utilización de elementos celulares con material genético de tres personas (un ovocito de la mujer con mutaciones en su mtDNA, un ovocito donante con mtDNA sano y un espermatozoide) para crear el embrión. Teniendo esto presente se explica porqué ha sido bautizada coloquialmente como la "técnica de los tres padres genéticos"(Farnezi *et al.*, 2020).

Bajo el término MRT se engloban varias técnicas con diferentes abordajes técnicos y denominaciones: reemplazo mitocondrial, donación mitocondrial o donación citoplasmática. Todas ellas comparten como objetivo común la sustitución citoplasmática por el citoplasma del óvulo donado con la finalidad de reemplazar totalmente el contenido mitocondrial del ovocito alterado, de tal modo que se reduce al máximo la probabilidad de trasmisión del mtDNA mutado a la descendencia (Kirillova & Mazunin, 2022). Desde el discurso biomédico es usual encontrarnos técnicas denominadas con terminología variada. El motivo de esta variabilidad en las denominaciones de algunas técnicas biomédicas no esta del todo claro. No obstante, en muchas ocasiones los nombres elegidos no son de todo inocentes (Cristina, 2022).

En el caso concreto de las MRT, cualquiera de las variantes de la técnica conlleva inevitablemente la incorporación de un orgánulo celular donado con material genético propio. La modificación en el contenido genético que este proceso genera ha sido calificado por organismos internacionales como una modificación del genoma en la línea germinal y con ello de su heredabilidad. Un aspecto esencial es que la posición de las sociedades científicas no es unánime[1]. Tales objeciones son la causa de que estas modificaciones estén prohibidas por las legislaciones de numerosos países. En efecto,

1. Heritable Human Genome Editing", NASEM, 2020.
Disponible en: https://www.nap.edu/catalog/25665/heritable-human-genome-editing#toc
Human Genome Editing: Science, Ethics, and Governance, NASEM, 2017.
Disponibleen:https://www.nap.edu/catalog/24623/human-genome-editing-science-ethics-and-governance

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

Tailandia es el único país que no prohíbe explícitamente las modificaciones del genoma humano[2].

El origen del uso de las MRT en la prevención de la transmisión de mutaciones mitocondriales fue propuiesto en las investigaciones de Tachibana en 2013 probando la técnica en modelos animales no humanos (Tachibana *et al.*, 2013). Poco tiempo después se publicaría el primer nacimiento en el mundo de un niño sano derivado de la aplicación de MRT en una mujer portadora del Síndrome de Leigh, en 2016 en México. Sin embargo, no tardó en trascender, que el procedimiento MRT fue llevado a cabo por J. Zhang y su equipo en Estados Unidos (Zhang *et al.*, 2017; Zinkant, 2016), a pesar de las restricciones normativas del país[3]. El proceso se culminó con la transferencia de embriones al útero materno en México (Palacios-González & Medina-Arellano, 2017). De este modo, el procedimiento reavivó un complejo debate sobre la permisividad o no de las MRT, las investigaciones en estas técnicas y sus potenciales usos, las implicaciones ético-jurídicas, así como los movimientos trasfronterizos para de pacientes y profesionales para su aplicación en países con regulaciones más laxas (G. Cohen, 2018; I. G. Cohen *et al.*, 2020).

III. Contexto internacional legislativo de las MRT

La aplicación de dicha opción terapéutica en la actualidad depende principalmente del régimen jurídico relacionado con las MRT en cada país. De forma general, podemos encontrar países con una prohibición de las MRT directa o indirecta (a través de la prohibición de técnicas que modifiquen el genoma en la línea germinal). Por otro lado, en países que no tienen ninguna regulación al respecto, el uso de las MRT dependerá de la oferta de tratamientos de los centros de reproducción asistida.

En Europa, Reino Unido en 2015, tras años de extensas revisiones e investigaciones, reguló y permitió el uso de las técnicas MRT[4] bajo unos criterios específicos[5]. Habría que remontarnos a 2005 cuando la Human Fertilization and Embryology Authority (HFEA)[6] -organismo gubernamental competente en la regulación de cualquier

2. Singapur Podría Convertirse En El Segundo País En Legalizar La Terapia De Reemplazo Mitocondrial | Ciencia en detalle 2023 (sciencebiweekly.com)

3. Malarkey MA, "Letter to Dr. John Zhang", 2017, US Food Drug Adm., Silver Spring, MD. https://www.fda.gov/media/106739/download

4. Reino Unido, país no firmante del Convenio de Oviedo. La normativa por la cual se regula la donación mitocondrial y las condiciones de su aplicación fueron publicadas en 2015 por la Human Fertilization and Embryology, La solicitud de autorización se produce individualmente en cada caso con acreditación de la existencia del riesgo derivado de alguna anomalía en el DNA mitocondrial que se desencadena una enfermedad genética grave. Dicha autorización es emitida por la HFEA.

Disponible en: https://www.hfea.gov.uk/about-us/news-and-press-releases/2017-news-and-press-releases/hfea-statement-on-mitochondrial-donation

5. http://www.parliament.uk/business/publications/research/briefingpapers/SN06833/mitochondrial-donation

6. Human Fertilisation and Embryology Authority. Code of Practice Edition 9.0: 33. Mitochondrial donation. Follow-up arrangements.

Disponible en: www.hfea.gov.uk/code-of-practice/33

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

técnica relacionada con la embriología humana o la medicina reproductiva- autorizó a la Universidad de Newcastle a llevar a cabo las investigaciones precisas para demostrar la viabilidad de las MRT en embriones humanos, iniciando así el largo camino hacia su regulación. La HFEA analizó cuatro revisiones de expertos independientes sobre el estado de desarrollo de las MRT en materia de efectividad, seguridad, riegos y resultados obtenidos (de 2011 a 2016). En ellas, el principal objetivo era determinar si las MRT eran técnicas efectivas para prevenir la herencia de enfermedades mitocondriales[7]. La regulación de Reino Unido en materia de embriología e investigación biomédica, de forma general, es permisiva con el avance de la ciencia (Sheldon, 2015). Todavía más, en la normativa reguladora la Ley sobre Fecundación Humana y Embriología, de 1990 (HFEA, Human Fertilization and Embryology Act), modificada en 2008, de la intervención del genoma, la HFEA, ya existía una disposición, que podría permitir modificar el ADN de la línea germinal "*para evitar la transmisión de enfermedades mitocondriales graves*", contenido en la sección 3ZA (subsección 5) (Border & Barber, 2015). No obstante, para resolver cualquier duda o perspicacia, el gobierno de Reino Unido contó con el apoyo del Departamento de Salud (Bredenoord & Appleby, 2017), quién optó por argumentar que intervención por MRT no constituye una importante modificación del genoma humano en la línea germinal[8], al considerar el reemplazo un pequeño intercambio de los genes de un orgánulo celular por los mismos genes sin alteraciones, es decir, "sanos", sin alterar con ello los genes nucleares[9] (Richardson *et al.*, 2015).

El gobierno británico proyectó el reglamento de las MRT (propuesta de reforma de Ley) para junio de 2013[10], así como una consulta pública (Panel ciudadano) entre febrero y junio de 2014 (Sheldon, 2015). Junto con todo ello, el estudio de las implicaciones bioéticas de las MRT para la HFEA fue desarrollado por el Nuffield Council on Bioethics, el cual concluyó con un dictamen favorable[11].

7. Heritable Human Genome Editing, 2020. NASEM.
Disponible en: https://www.nap.edu/nap-cgi/skimchap.cgi?recid=25665&chap=19-34

8. Department of Health, UK. Mitochondrial Donation: Government Response to the Consultation on Draft Regulations to Permit the Use of New Treatment Techniques to Prevent the Transmission of a Serious Mitochondrial Disease from Mother to Child. 2014. pp15.
Disponible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/332881/Consultation_response.pdf.

9. Department of Health (UK), Mitochondrial Donation: Government response to the consultation on draft regulations to permit the use of new treatment techniques to prevent the transmission of serious mitochondrial disease from mother to child. 2014 Jul, pp. 18–19.
Disponible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/332881/Consultation_response.pdf.

10. Department of Health and Human Fertilisation and Embryology Authority. Innovative genetic treatment to prevent mitochondrial disease, 2013.
Disponible en: https://www.gov.uk/ government/news/innovative-genetic-treatment-to-prevent-mitochondrial-disease.

11. Nuffield Council on Bioethics. Novel techniques for the prevention of mitochondrial DNA disorders: an ethical Review. London: Nuffield Council on Bioethics, 2012, p. 88.
Disponible en: http://www.nuffieldbioethics.org/mitochondrial-dna-disorders.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

De acuerdo con la consulta pública y el informe del Nuffield Council on Bioethics, la HFEA[12] comunicó al Gobierno que: *"existe un apoyo general para permitir el reemplazo mitocondrial en el Reino Unido, siempre y cuando sea lo suficientemente seguro para ofrecerlo en un entorno de tratamiento y se haga dentro de un marco regulatorio"*[13,14,15]. *"El 3 de febrero de 2015, la Cámara de los Comunes del Reino Unido aprobó, por 382 votos a favor y 128 en contra, una modificación de la Ley de Embriología y Fecundación Humana de 2008, que permitirá la realización de la denominada Trasferencia Mitocondrial en seres humanos*" (De Miguel Beriain *et al.*, 2016).

La normativa contempla que los niños nacidos tras una MRT sean inscritos en un registro para su seguimiento a largo plazo y así tener la posibilidad de recabar información con potencial prospectivo sobre la seguridad y eficacia de las MRT[16]. Sin embargo, no obliga a tal registro, lo que puede suponer una pérdida de información muy valiosa. Además, a diferencia de otras técnicas de reproducción humana asistida (TRHA) en el Reino Unido, se limita el acceso a la información en lo que respecta a la identidad de las donantes de ovocitos[17] como fuente de mitocondrias sanas. Esta postura está basada en que el procedimiento MRT no utiliza el material genético nuclear del ovocito donado, tan solo su citoplasma.

Se acordó, además, que la aplicación clínica de las MRT y, en particular, de las variantes técnicas ST y PNT, habrían de estar supervisadas en todo momento por la HFEA y quedando sujetas a un doble control, por un lado, de los centros autorizados para su práctica, y por otro, de los casos individuales de los sujetos a los que se les aplica, teniendo en cuenta algunas restricciones: a) Limitación de la aplicación a los casos en que los padres desean tener un hijo genéticamente relacionado que no esté afectado por una enfermedad mitocondrial grave; b) Limitación de la aplicación en casos de mutaciones del mtDNA para las que no exista otra alternativa técnica; c) Licencia limitada de forma individual a cada solicitud, previo informe favorable de la HFEA; d) Revisión continua de la autorización de la licencia del centro solicitante; e) Proceso de consentimiento informado completo; f) Seguimiento a largo plazo de la descendencia; g) Prohibición de otros usos más allá de la indicación permitida.

12. HFEA Scientific review of the safety and efficacy of methods to avoid mitochondrial disease through assisted conception: 2016 update. 2016.
Disponible en: https://www.hfea.gov.uk/media/2611/fourth_scientific_review_mitochondria_2016.pdf.
13. HFEA, 2013, p. 4.
14. Department of Health, UK. Mitochondrial Donation: Government Response to the Consultation on Draft Regulations to Permit the Use of New Treatment Techniques to Prevent the Transmission of a Serious Mitochondrial Disease from Mother to Child, 2014, p15.
15. Ibidem.
16. Hum. Fertil. Embryol. Auth. 2016. Scientific review of the safety and efficacy of methods to avoid mitochondrial disease through assisted conception: 2016 update. Rep., Hum. Fertil.
https://www. hfea.gov.uk/media/2611/fourth_scientific_review_mitochondria_2016.pdf
17. Hum. Fertil. Embryol. Auth. 2014, ob. cit.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

Haciendo también una breve referencia a la legislación de Reino Unido, este gobierno analizó el coste del proceso por paciente, considerando viable su inclusión en el sistema de salud nacional[18] (Rhys-Evans, 2020).

El Reino Unido se convirtió así en el primer país mundial en autorizar y regular las MRT y controlar las licencias de aplicación. En la actualidad, el número de solicitudes enviadas y aceptadas a la HFEA para someterse a MRT no está a disposición del público. Recientemente, a la fecha de escritura de este trabajo, se ha publicado el primer nacimiento por esta técnica en Reino Unido[19].

Al otro lado del mundo, Australia es un país proactivo en investigación y autorización de procedimientos que involucran técnicas de reproducción asistida con fines clínicos y de investigación[20] a través del Comité de Acreditación de la Tecnología Reproductiva (Assisted Reproductive Technology Working Committee, National Health and Medical Research Council, NHMRC). En concreto, el Comité de Licencias de Investigación de Embriones, dependiente del NHMRC, es el encargado de evaluar y aprobar las solicitudes para desarrollar nuevos procedimientos guiados por expertos clínicos[21]. Ahora bien, de acuerdo con la Ley de Prohibición de la Clonación Humana para la Reproducción (2002), la legislación australiana prohíbe en concreto la alteración del genoma de las células humanas cuando esta sea heredable a través de la línea germinal, lo que supuso una barrera inicial para el uso de las MRT.

El Senado de Australia, siguiendo el ejemplo de Reino Unido autorizó en 2018 al National Health and Medical Research (NHMRC) para establecer un Comité de Trabajo de Expertos en Donación Mitocondrial para investigar una variedad de conocimientos y perspectivas sobre los aspectos legales, normativos, científicos y éticos relacionados con la idoneidad del uso clínico de las MRT. La investigación, tras varios años de duración, concluyó con el informe del Comité de Expertos Mitocondriales quienes respaldaron el "gran potencial de la donación mitocondrial para abordar los efectos debilitantes de heredar la enfermedad mitocondrial"(Dziadek & Sue, 2022; Newson *et al.*, 2019)[22].

De acuerdo con el procedimiento seguido, en marzo de 2022 el Parlamento australiano aprobó el proyecto de ley para permitir el uso de la donación mitocondrial para prevenir la transmisión de enfermedades mitocondriales graves (Noohi *et al.*, 2022).

18. Reglamento de Fertilización Humana y Embriología (Donación Mitocondrial) de 2015. Instrumentos estatutarios del Reino Unido de 2015 Nº 572. https://www.legislation.gov.uk/uksi/2015/572/contents/made(consultado en agosto de 2021).

19. Nace en Reino Unido el primer bebé con ADN de tres personas (abc.es)

20. Consejo Nacional de Salud e Investigación Médica. Directrices éticas sobre el uso de la tecnología de reproducción asistida en la práctica clínica y la investigación. Canberra: NHMRC, 2017. https://www.nhmrc.gov.au/art.

21. Consejo Nacional de Salud e Investigación Médica. Informe sobre la consulta pública del NHMRC sobre las cuestiones sociales y éticas planteadas por la donación mitocondrial (informe de la consulta). NHMRC 2020. https://www.nhmrc.gov.au/mitochondrial-donation-0#downlo.

22. Consejo Nacional de Salud e Investigación Médica. Directrices éticas sobre el uso de la tecnología de reproducción asistida en la práctica clínica y la investigación. Canberra: NHMRC, 2017. https://www.nhmrc.gov.au/art.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

Esta ley introduce la donación mitocondrial a través de un enfoque gradual distribuido en tres etapas: a) La *primera etapa* permite la investigación y la realización de ensayos clínicos con las MRT para su uso en reproducción humana. La finalidad de estos estudios es recopilar datos sobre la efectividad y seguridad del procedimiento antes de que se otorgue la aprobación para uso clínico; b) La segunda etapa contempla la monitorización y evaluación del ensayo mediante la introducción del sistema de licencias a centros especializados para llevar a cabo el reemplazo mitocondrial, con la incorporación de mujeres australianas portadoras de enfermedad mitocondrial; c) En la tercera etapa se llevará a cabo la aplicación del sistema de concesión de licencias para donaciones mitocondriales a centros especializados. Este sistema de licencias capacita tanto a los profesionales de la embriología de forma nominativa para cada técnica MRT, como a los centros. Además deben cursarse las solicitudes de tratamiento para pacientes de forma individualizada. En nuestra opinión, *a prioir,* parece ser un sistema más preciso y garantista que el régimen de autorizaciones de Reino Unido.

La reforma de la Ley de Donación Mitocondrial, es conocida como Ley de Maeve por *Maeve Hood*, una niña con Síndrome de Leigh, entró en vigor el 1 de octubre de 2022.

IV. Singapur camino de la regulación de las MRT

Singapur, el pequeño estado asiático, también inició el camino hacia un estudio sobre la regulación de las MRT. Posiblemente de forma coetánea a Australia, salvo que sus gobiernos han tomado distinta dirección en su decisión.

En 2005, el Comité Asesor de Bioética de Singapur (BAC)[23], había recomendado en su informe sobre Pruebas Genéticas y Genética Investigación que no se debe permitir en la actualidad la práctica clínica de técnicas que conlleven modificaciones genéticas en la línea germinal. A esta afirmación debemos añadir que las leyes en Singapur no permiten la modificación de la línea germinal humana en el entorno clínico.

Sin embargo, debido a los avances científicos y políticos acontecidos en el campo de MRT internacionalmente, en concreto la normativa de Reino Unido como primer país en legalizar la aplicación clínica de MRT en 2015, y basándose en la sentencia del Tribunal Supremo de Singapur de 2017 del caso BAC contra Thomas Medical[24], en el que se reconoció el interés de la relación genética entre progenitores y descendientes y ha sido origen de argumentaciones en defensa de las MRT (Schaefer & Labude, 2017). El Gobierno de Singapur estimó oportuno investigar la situación actual de las MRT y revisar sus recomendaciones sobre las modificaciones genéticas en la línea germinal,

23. El BAC, creado en diciembre de 2000, es un comité asesor independiente que estudia las áreas en evolución de la investigación biomédica humana y recomienda al gobierno de Singapur las políticas que considere oportunas.
Bioethics Advisor Committee, 2019.
https://www.bioethicssingapore.org/who-we-are/what-we-do

24. BAC vs. Thomson Medical Pte Ltd and Others, SGCA (2017). https://www.supremecourt.gov.sg/news/ case-summaries/acb-v-thomson-medical-pte-ltd-and-others

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

particularmente en el contexto de la prevención de la transmisión de enfermedades mitocondriales.

En 2014, el BAC formó el Grupo de Revisión de Tecnología de Reemplazo Genoma Mitocondrial compuesto por 13 expertos locales e internacionales con el propósito de revisar la posición sobre la modificación de la línea germinal, con un enfoque en MRT.

El grupo publicó el documento de consulta titulado "Ethical, Legal and Social Issues Arising from Mitochondrial Genome Replacement Technology", 2018. La primera parte del documento incluye un detallado desarrollo sobre las mitocondrias y sus patologías. Contiene además, información explicativa sobre los mecanismos de herencia y las mutaciones correspondientes para cada enfermedad, las limitaciones que presentan otras como el diagnóstico genético preimplantacional (DGP), el diagnóstico prenatal o las TRHA. A esta base biomédica añade un segundo capítulo en el cual incluye una descripción de cada de las técnicas, así como una argumentación acerca de las modificaciones de la línea germinal. El Comité parece prestar una especial atención a las modificaciones de la línea germinal con uso clínico[25], con la finalidad de que el gobierno favorezca esta legislación. Algunas otras consideraciones más importantes de dicho documento fueron[26].

- Proponer como objetivo el "proteger los derechos y el bienestar de las personas y permitir al mismo tiempo que las ciencias biomédicas se desarrollen y desarrollen todo su potencial en beneficio de la humanidad"[27].
- Definir la "modificación genética de la línea germinal" como "un tipo de tecnología genética que implica la alteración de la composición genética de una persona de forma permanente y que puede transmitirse a su descendencia"[28].
- Limitar el uso de MRT a la prevención de enfermedades mitocondriales graves. El documento recoge argumentos a favor y en contra de la aplicación clínica de las MRT y plantea cuestiones como los posibles beneficios, la autonomía reproductiva, la equidad y el bienestar de las generaciones futuras.

En particular, el documento reconoce la preocupación por la fina línea que supondría pasar de las MRT a la modificación genética de la línea germinal.

Teniendo esto presente y dado que Singapur es una sociedad multicultural y pluralista con una amplia gama de perspectivas religiosas, el BAC espera que los grupos religiosos continúen ser activo y contribuir a los debates sobre bioética en curso. Se llevaron a cabo las sesiones de diálogo con los miembros de la Junta de Revisión Institucional (IRB), médicos, investigadores, líderes religiosos abordando: ¿Cuáles son los posibles beneficios de MRT?; ¿Cuáles son los impactos psicológicos o sociales en los niños nacidos usando tales técnicas?. Problemas éticos, legales y sociales que surgen

25. Bioeth. Advis. Comm. 2005, ob. cit.
26. Bioeth. Advis. Comm. 2018, ob. cit.
27. Bioeth. Advis. Comm. 2018, ob. cit.
28. Ibidem, p.37.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

de la tecnología de reemplazo del genoma mitocondrial: un documento de consulta. Tecnología de reemplazo del genoma mitocondrial. ¿Es injusto impedir que las mujeres portadoras de mutaciones mitocondriales accedan a nuevos tecnología que les ofrece el potencial de tener hijos sanos relacionados genéticamente?. ¿Debería el bienestar de las generaciones futuras prevalecer sobre los deseos de las generaciones existentes? (es decir, los futuros padres), o ¿viceversa?. Ahora bien, suponiendo que todas las técnicas son igualmente seguras y efectivas, ¿existe alguna responsabilidad ética? distinciones que deben establecerse entre las diversas técnicas de reemplazo mitocondrial?

La consulta pública se llevó a cabo de abril a junio de 2018. De las opiniones del público y las organizaciones interesadas ayudarán al BAC a formular su recomendación sobre si la aplicación clínica de MRT debe o no permitirse en Singapur, se concluyó que la principal preocupación era la seguridad de la técnica. Además, los participantes de la consulta expresaron qué solo debe permitirse en Singapur si se demuestra que es seguro para unos fines concretos y delimitados. El BAC estuvo de acuerdo con estas las preocupaciones en torno a la seguridad de MRT.

Tras las reflexiones, del informe preliminar de 2021 pueden extraerse las siguientes conclusiones:

- El BAC reconoce que la sustitución de mitocondrias afectadas por donantes sanos mitocondrias tiene el potencial de prevenir la transmisión de trastornos mitocondriales en humanos.
- Si bien la introducción de cambios genéticos hereditarios conlleva riesgos imprevisibles, la evidencia científica preclínica sugiere que las MRT no son inseguras, pero se requieren más estudios con un seguimiento estrecho de unmayor numero de casos.
- El BAC opina que la MRT es una intervención preventiva, no una forma de terapia, adquiere un cariz diferente en la relación beneficio.
- Existen alternativas a las MRT, si bien estas opciones tienen limitaciones y pueden no ser consideradas óptimas por todos.
- Plantea varios problemas éticos, legales y sociales.
- Señala que el Reino Unido es un caso atípico en el escenario mundial en este sentido, ya que es el único país que ha desarrollado regulaciones controles y supervisión para permitir MRT[29].

El aspecto esencial del documento es la conclusión por la cual "La modificación genética de la línea germinal no debe permitirse en este momento. Es prematuro eximir a MRT de la prohibición de la clínica modificación genética de la línea germinal y recomienda que la práctica clínica y la investigación clínica relacionada con la MRT in vivo en sujetos humanos no deben ser permitido en este momento".

29. Tras nuestra investigación podemos afirmar, que ya no es el único tras la reciente aprobación de la Ley de Maeve en Australia.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

V. Conclusiones

La aplicación clínica de las MRT puede reducir significativamente el riesgo de transmisión de enfermedades mitocondriales heredadas de la madre, una situación que se vuelve vital para las familias portadoras de mutaciones mitocondrailes pues les porciona su única opción para tener hijos no afectados y genéticamente relacionados.

En Singapur se ha considerando la posibilidad de abordar un cambio legislativo, no obstante a la luz del informe del BAC, con un enfoque cauteloso, expone claras objeciones a la investigación y práctica clínica con MRT.

En definitiva, podemos concluir, que tras los pasos andados, Singapur no abordará la regulación permisiva de las MRT a corto plazo.

Ningún otro país, a parte de los mencionados en este trabajo, ha adoptado leyes específicamente sobre las MRT.

Agradecimientos

La autora aprovecha este espacio para agradecer los revisores/as anónimos de este artículo sus valiosas correcciones y sugerencias que han permitido mejorar este texto.

Algunos de los datos de ests trabajo pertenecen a una investigación de mayor alcance de la propia autora aún sin publicar.

Bibliografía

BAC. (2018). *Consultation Paper on Ethical, Legal and Social Issues Arising from Mitochondrial Genome Replacement Technology* (p. 49). Bioethics Advisory Committe. https://www.bioethics-singapore.org/publications/press-releases/bac-mgrt-press-release

Border, P., & Barber, S. (2015). *Mitochondrial donation. Standard Note: SN/ SC/6833.* (London: House of Commons Library). United Kingdom Parliament. https://commonslibrary.parliament.uk/research-briefings/sn06833/

Bredenoord, A. L., & Appleby, J. B. (2017). Mitochondrial Replacement Techniques: Remaining Ethical Challenges. *Cell Stem Cell*, *21*(3), 301-304. https://doi.org/10.1016/j.stem.2017.08.009

Cohen, G. (2018). Circumvention Medical Tourism and Cutting Edge Medicine: The Case of Mitochondrial Replacement Therapy. *Indiana Journal of Global Legal Studies*, *25*(1), 439-462. https://doi.org/10.2979/indjglolegstu.25.1.0439

Cohen, I. G., Adashi, E. Y., Gerke, S., Palacios-González, C., & Ravitsky, V. (2020). The Regulation of Mitochondrial Replacement Techniques Around the World. *Annual Review of Genomics and Human Genetics*, *21*(1), 565-586. https://doi.org/10.1146/annurev-genom-111119-101815

Craven, L., Murphy, J. L., & Turnbull, D. M. (2020). Mitochondrial donation—Hope for families with mitochondrial DNA disease. *Emerging Topics in Life Sciences*, *4*(2), 151-154. https://doi.org/10.1042/ETLS20190196

Cristina, M. (2022). ¿Alquiler o sustitución del embarazo? Sobre la importancia de los significantes en la construcción de sentido. *Revista de Bioética y Derecho*, *54*, 5-22. https://doi.org/10.1344/rbd2021.54.34891

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

Davis, R. L., Liang, C., & Sue, C. M. (2018). Mitochondrial diseases. *Handbook of Clinical Neurology*, *147*, 125-141. https://doi.org/10.1016/B978-0-444-63233-3.00010-5

De Miguel Beriain, I., Atienza Macías, E., & Armaza Armaza, E. J. (2016). Algunas consideraciones sobre la transferencia mitocondrial: ¿un nuevo problema para la bioética? *Acta bioethica*, *22*(2), 203-211. https://doi.org/10.4067/S1726-569X2016000200007

Dziadek, M. A., & Sue, C. M. (2022). Mitochondrial donation: Is Australia ready? *Medical Journal of Australia*, *216*(3), 118-121. https://doi.org/10.5694/mja2.51309

Farnezi, H. C. M., Goulart, A. C. X., Santos, A. D., Ramos, M. G., & Penna, M. L. F. (2020). Three-parent babies: Mitochondrial replacement therapies. *JBRA Assisted Reproduction*, *24*(2), 189-196. https://doi.org/10.5935/1518-0557.20190086

Grady, J. P., Pickett, S. J., Ng, Y. S., Alston, C. L., Blakely, E. L., Hardy, S. A., Feeney, C. L., Bright, A. A., Schaefer, A. M., Gorman, G. S., McNally, R. J., Taylor, R. W., Turnbull, D. M., & McFarland, R. (2018). MtDNA heteroplasmy level and copy number indicate disease burden in m.3243A>G mitochondrial disease. *EMBO Molecular Medicine*, *10*(6), e8262. https://doi.org/10.15252/emmm.201708262

Kirillova, A., & Mazunin, I. (2022). Operation «mitochondrial wipeout»—Clearing recipient mitochondria DNA during the cytoplasmic replacement therapy. *Journal of Assisted Reproduction and Genetics*, *39*(10), 2205-2207. https://doi.org/10.1007/s10815-022-02561-6

Newson, A. J., de Lacey, S., Dowling, D. K., Murray, S., Sue, C. M., Thorburn, D. R., Gillam, L., & Degeling, C. (2019). Public attitudes towards novel reproductive technologies: A citizens' jury on mitochondrial donation. *Human Reproduction (Oxford, England)*, *34*(4), 751-757. https://doi.org/10.1093/humrep/dez021

Noohi, F., Ravitsky, V., Knoppers, B. M., & Joly, Y. (2022). Mitochondrial Replacement Therapy: In Whose Interests? *The Journal of Law, Medicine & Ethics: A Journal of the American Society of Law, Medicine & Ethics*, *50*(3), 597-602. https://doi.org/10.1017/jme.2022.98

Palacios-González, C., & Medina-Arellano, M. de J. (2017). Mitochondrial replacement techniques and Mexico's rule of law: On the legality of the first maternal spindle transfer case. *Journal of Law and the Biosciences*, *4*(1), 50-69. https://doi.org/10.1093/jlb/lsw065

Pfeffer, G., Majamaa, K., Turnbull, D. M., Thorburn, D., & Chinnery, P. F. (2012). Treatment for mitochondrial disorders. *The Cochrane Database of Systematic Reviews*, *4*. https://doi.org/10.1002/14651858.CD004426.pub3

Richardson, J., Irving, L., Hyslop, L. A., Choudhary, M., Murdoch, A., Turnbull, D. M., & Herbert, M. (2015). Concise reviews: Assisted reproductive technologies to prevent transmission of mitochondrial DNA disease. *Stem Cells (Dayton, Ohio)*, *33*(3), 639-645. https://doi.org/10.1002/stem.1887

Schaefer, & Labude, M. K. (2017). Genetic affinity and the right to «three-parent IVF». *Journal of Assisted Reproduction and Genetics*, *34*(12), 1577-1580. https://doi.org/10.1007/s10815-017-1046-8

Sheldon, K. (2015). Crossing the Germline Barrier: The Three Genome Baby. *Ethics in Biology, Engineering and Medicine: An International Journal*, *6*(3-4), 237-261. https://doi.org/10.1615/EthicsBiologyEngMed.2016016331

Tachibana, M., Amato, P., Sparman, M., Woodward, J., Sanchis, D. M., Ma, H., Gutierrez, N. M., Tippner-Hedges, R., Kang, E., Lee, H.-S., Ramsey, C., Masterson, K., Battaglia, D., Lee, D., Wu, D., Jensen, J., Patton, P., Gokhale, S., Stouffer, R., & Mitalipov, S. (2013). Towards germline

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

gene therapy of inherited mitochondrial diseases. *Nature*, *493*(7434), 627-631. https://doi.org/10.1038/nature11647

Wei, W., & Chinnery, P. F. (2020). Inheritance of mitochondrial DNA in humans: Implications for rare and common diseases. *Journal of Internal Medicine*, *287*(6), 634-644. https://doi.org/10.1111/joim.13047

Yamada, M., Akashi, K., Ooka, R., Miyado, K., & Akutsu, H. (2020). Mitochondrial Genetic Drift after Nuclear Transfer in Oocytes. *International Journal of Molecular Sciences*, *21*(16), 5880. https://doi.org/10.3390/ijms21165880

Zhang, J., Liu, H., Luo, S., Lu, Z., Chávez-Badiola, A., Liu, Z., Yang, M., Merhi, Z., Silber, S. J., Munné, S., Konstantinidis, M., Wells, D., Tang, J. J., & Huang, T. (2017). Live birth derived from oocyte spindle transfer to prevent mitochondrial disease. *Reproductive Biomedicine Online*, *34*(4), 361-368. https://doi.org/10.1016/j.rbmo.2017.01.013

Zinkant, K. (2016). *Da traut sich niemand ran*. Süddeutsche.de. https://www.sueddeutsche.de/wissen/bioethik-da-traut-sich-niemand-ran-1.2850609

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 116-128
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.08

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

Análisis legal del uso de los robots en la medicina

LEGAL ANALYSIS OF THE USE OF ROBOTS IN MEDICINE

Marina Galvín Gordillo
Universidad de Sevilla
margalgor1alum@alum.us.es 0009-0005-8340-6931

Recibido: 06 de junio de 2023 | Aceptado: 13 de junio de 2023

RESUMEN

En este trabajo vamos a tratar de explicar cuáles son los efectos y las consecuencias del uso de los robots en la medicina y sus aspectos legales, asimismo, analizaremos los avances en la tecnología y la inteligencia artificial y sus aplicaciones en el campo de la medicina y la salud, que ha supuesto el avance en la calidad de vida y está ayudando a curar enfermedades y dando diagnósticos que hasta hace poco eran impensables.

PALABRAS CLAVE

Medicina
Robots
Inteligencia artificial
Salud
Calidad de vida

ABSTRACT

In this paper we are going to try to explain which are the effects and consequences of use of the robots in medicine, and its legal aspects, in other words, what would be its effects, the advances in technology and artificial intelligence and its applications in the field of medicine and the health, and that have improved the quality of life, curing diseases and performing diagnosis that until recently were not possible.

KEYWORDS

Medicine
Robots
Artificial intelligence
Health
Quality of life

I. Introducción

El hombre a lo largo del tiempo ha buscado su mejora en la calidad de vida y, para ello, ha puesto su inteligencia y su trabajo al servicio de la lucha contra las enfermedades, esto caracteriza de forma indefectible el pasado, el presente y el futuro de la humanidad; los avances sin precedentes que ha experimentado la Biomedicina (Revolución Biomédica) y la Biotecnología abren nuevos horizontes para el tratamiento de graves enfermedades e incluso incrementar la esperanza de vida, sin embargo, estos avances han suscitado el debate político, ético, científico, filosófico y jurídico sobre las implicaciones positivas y negativas de éstos, que han sido muy notables sobre todo en España donde se han ido produciendo una serie de reformas legales que han planteado cuestiones antagónicas, por ejemplo, la legalización de la investigación con células madre procedentes de embriones supernumerarios de los procesos de fecundación *in vitro*, la autorización del diagnóstico genético o la clonación terapéutica mediante la Ley de Investigación Biomédica (LIB) 14/2007[1], de 3 de julio.

No obstante, y a pesar de los aspectos positivos de la tecnología en la biomedicina, nunca debe darse prioridad al llamado "imperativo tecnológico" como alternativa desde el humanismo, definido por (González,2004) como la superación y alternativa al viejo imperativo ético, que se pregunta lo que es factible y lo que no, pero lo técnicamente factible y viable no tiene por qué ser moralmente legítimo y jurídicamente lícito, a diferencia de la ciencia pura académica o instrumental que sólo busca enriquecer con sus conocimientos siendo éticamente neutral, pero la unión entre la innovación tecnológica y la investigación científica dan como resultado la tecno ciencia que ha transformado el conocimiento científico para alcanzar otros fines que en ocasiones son silenciados, así como controlar la actividad de los científicos por la sociedad que marca las líneas democráticamente establecidas que no deben ser traspasadas, y que los propios científicos tienen que controlar por medio de la "ética de la responsabilidad" como consecuencia, entre otras, de los posibles peligros generados por los avances biotecnológicos, debiendo observarse en todo momento los principios de responsabilidad y de precaución. El principio de responsabilidad ha sido mencionado en la obra *Das Prinzip Verantwortung*, en la que se señala que la cautela es el primer mandato moral, y el pensamiento hipotético debe ser nuestra principal tarea (Jonas,1965). Interconectado con este principio encontramos el principio de precaución que se aplica ante las posibles incertidumbres científicas en conexión con los daños graves que pudiesen dar lugar la adopción de medidas para la prevención de los riesgos, arts 2 y 22, LIB, el carácter positivo o negativo de la tecno ciencia depende del destino que se le da (teoría de la neutralidad valorativa, Oliver.L, 2021) siendo por tanto imposible garantizar la total seguridad, pero la existencia de posibles riesgos imprevisibles no pueden provocar la parálisis de la investigación científica que ha logrado y está logrando importantes beneficios para la humanidad, por ejemplo la telemedicina como un avance en los diagnósticos y el tratamiento de

1. Ley de Investigación Biomédica (LIB) 14/2007, de 3 de julio, BOE n° 159, de 04 de julio de 2007, Ref: BOE-A-2007-12945, págs. 2826 a 2848

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

las enfermedades a distancia, esta técnica conforma una amplia acepción dada por la Organización Mundial de la Salud (OMS) donde la define como aportación de servicios de salud usando las nuevas tecnologías de la comunicación para un intercambio válido de información en el diagnóstico, la prevención de las enfermedades y por supuesto en cuanto a la investigación y evaluación continuada en los proveedores de la salud, todo ello, con el interés de mejorar la salud de los individuos y sus comunidades. En el aspecto ético cabe señalar uno de los documentos más importantes en esta materia como son las Directrices éticas para una inteligencia artificial (IA) fiable[2], estas directrices han sido redactadas por el Grupo de Expertos de Alto nivel sobre IA que fue constituido por la Comisión Europea en junio de 2018, en este documento respaldan el marco general para una IA fiable, aunque con un matiz porque no están necesariamente de acuerdo con todas y cada una de las afirmaciones que se realizan en estas Directrices, para ello es necesario que los sistemas de IA se centren en las personas y adopten el compromiso de utilizarlos al servicio de la humanidad y del bien común para mejorar el bienestar y la libertad de los seres humanos, por esta razón debe cumplir la ley puesto que ésta no avanza al mismo ritmo que la tecnología y, en ocasiones, puede ser inadecuada para abordar ciertas cuestiones, pero un código ético tampoco puede sustituir al razonamiento ético que debe ser sensible a detalles contextuales, generar esa confianza tiene mucho interés sobre todo en el Libro Blanco[3] sobre la IA, que es un enfoque europeo hacia la excelencia y la confianza en esta tecnología, ya que ha traído innumerables ventajas como la precisión en los diagnósticos o la mejor prevención de enfermedades, pero tiene su lado negativo ya que puede resultar nociva produciendo daños tanto materiales (salud y seguridad) como inmateriales (pérdida de privacidad, discriminación, etc).

En otras palabras, se trata de minimizar los riesgos enfocado principalmente en la protección de los Derechos Fundamentales. Para una IA fiable[4], el Libro Blanco propone tres componentes que deben ser acumulativos en sistemas de IA: a) lícita, que cumpla con la ley relacionada con la responsabilidad médica y que asegure una compensación justa cuando se produzca un efecto adverso, b) ética, que garantice el respeto a los principios y valores, y c) robusta, basada en la supervisión humana y gestión de la privacidad de los datos y la no discriminación; por consiguiente no podemos olvidar los principios y valores más importantes relacionados con la asistencia sanitaria y la IA.

La autonomía de la IA debe ser antropocéntrica, respetar en todo caso la autonomía y los derechos fundamentales de los pacientes, y debe rechazar la toma de decisiones basadas de forma exclusiva mediante procesos de automatización, ya que estas decisiones anularían o vaciarían las decisiones de los pacientes y también influirán en el juicio crítico del profesional, a la vez que plantean problemas a la hora de la determinación de la responsabilidad. La IA y la responsabilidad sanitaria consideran sujeto moral

2. Directrices éticas para una inteligencia artificial (IA) fiable, se puede consultar en la URL https://ec.europa.eu/digital-single-market/en/high-level-expert-group-aryificial-intelligence
3. Libro Blanco, COM (2020) 65 final, Bruselas, 19 de febrero de 2020, se puede consultar en la URL https://eur-lex.europa.eu
4. Directrices éticas para una inteligencia artificial (IA) fiable, *op.cit*., pág. 3

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

a los profesionales, descartando a los sistemas de IA, pudiendo ser responsables para su delimitación. Planteamos el requisito de la imprudencia, que se fundamenta en un elemento objetivo de cuidado cuya inobservancia puede producir un resultado perjudicial, pero no basta con la conducta inadecuada del mismo, como establece la ley de ordenación de las profesiones sanitarias que está basado en la unificación de la evidencia científica y en los medios disponibles.

La distancia como factor en el uso de las tecnologías de la información se ha visto incorporada por la eficiencia generada por la prestación del acto médico a distancia como elemento complementario a la visita presencial, son ejemplo de ello las apps de Salud, a través de las cuales el profesional puede disponer de datos, entre otros, sobre la temperatura, el nivel de glucosa, informaciones de salud, de los pacientes. La aplicación "M/Health", es la práctica de la medicina y la salud pública soportada por medio de teléfonos móviles y dispositivos inalámbricos, la reticencia en el uso de estas tecnologías está justificada por la inseguridad generada por el uso del tratamiento de la información, siendo necesario reducir el riesgo para generar confianza, debiéndose adaptar a las directrices de la normativa protectora de los datos de carácter personal (OMS, Informe de 2015, Global Observatory of eHealth, revisado en 2016) donde destacó que el uso de los dispositivos móviles el uso de los smartphones y otros dispositivos móviles para la práctica médica y la sanidad pública.

El Libro Verde[5] sobre sanidad móvil ponía de relieve que el rápido desarrollo de los servicios sanitarios móviles generaban inquietud sobre el adecuado tratamiento de los datos recogidos por medio de aplicaciones. Por ello, el Reglamento General de Protección de Datos 679/2018[6] señala, en su Considerando 6, que la globalización plantea retos en materia de protección de datos, y el Considerando 35 define el concepto de dato personal mediante una acepción más amplia que abarca todo lo relativo a la salud física y mental tanto en el presente como en el futuro, regulados en el artículo 4.15, RGPDE y en la Directiva 2011/24/UE, del Parlamento y del Consejo[7].

Con independencia de las directrices de carácter ético y moral en relación a la biotecnología, el Derecho en cuanto a conjunto de normas jurídicas que debe afrontar los problemas derivados de la investigación y las nuevas tecnologías aplicadas a la vida, se ocupa de las relaciones de alteridad, siendo heterónomo, y sus soluciones jurídicas no tienen por qué ser garantía de moralidad, la conexión entre la Bioética y Derecho está determinada en los derechos fundamentales que están recogidos en la Constitución y que son la base del Estado de Derecho, siendo además los principios rectores que reflejan la ética más esencial, los derechos fundamentales relacionados con la Bioética son el derecho a la vida, a la integridad física y la prohibición de tratos degradantes, artículos 10 y 15, CE; el primero recoge la dignidad humana como base del orden jurídico, que se caracteriza por ser una cualidad humana que tiene que ser interpretada atendiendo a

5. Libro Verde, sobre salud móvil en la U.E., COM (2014) 219 final, Bruselas, Comisión Europea 2014, se puede consultar en la URL https://eur-lex.europa.eu>summary
6. RGPDE 2016/679, de 27 de abril, DOUE nº 119, 04 de mayo de 2016, Ref: DOUE-L-2016-80807
7. Directiva 2011/24/UE, DOUE-L-2011/89723, págs. 45 a 65

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

las disposiciones constitucionales y los derechos fundamentales, por ello cabe destacar alguna Jurisprudencia al respecto (STC 120/1990 y ATC 149/1999), además podemos destacar la libertad y autonomía personal arts. 1 y 9, CE, la confidencialidad art 18 CE, la protección a la salud art. 43.1 y 2, CE. o el art. 25, de la Declaración Universal de los Derechos Humanos de la ONU[8], cabe destacar de estos instrumentos normativos su aplicación ya que conforman el corpus iuris internacional de acuerdo a la interpretación dada por la Corte Internacional de Derechos Humanos[9]. En ese sentido los principios generales que componen el objeto del Bioderecho se construye sobre la dignidad humana, construcción humanista del por ello corresponde a la bioética del Derecho un análisis basado en una crítica racional que pretenda justificar los principios y derechos que recogen los textos normativos dotando de legitimidad al Bioderecho exponiendo si una determinada práctica Bioética se ajusta o no a la dignidad humana, en este sentido la IA estudia las diversas maneras de la vida humana. La sociedad civil espera que la Bioética resuelva los problemas actuales.

II. Regulación jurídica de la biomedicina

La argumentación crítica expone que la IA afecta de forma estructural a la autonomía personal y a las relaciones de los individuos condicionando la decisión libre, y la autonomía relacional, donde la consideración del bien surge del reconocimiento intersubjetivo y proporciona las condiciones materiales necesarias para que la elección individual sea posible, reconociéndose las desigualdades estructurales que debe buscar la regulación jurídica adecuada que evite los desvíos algorítmicos que producen riesgos en la IA y afectan a la autonomía personal y relacional de los individuos neutralizados por el Derecho mediante estipulaciones normativas (Nedelsky. J, 2013).

El Derecho debe proporcionar criterios que sirvan para resolver conflictos específicos del mundo sanitario planteados en el ámbito de la IA, como por ejemplo la organización de grandes bases de datos clínicos (Big Data) ya que el sistema debe comprender el lenguaje natural y la modelación de las reglas jurídicas, por ello en los EE.UU la dimensión jurídica de la Bioética estuvo presente, sobre todo, a través de una serie de resoluciones judiciales que fueron desarrollando el marco jurídico de los avances biomédicos y las denominaciones empleadas para definir el ordenamiento jurídico que se ocupa de los aspectos normativos de sus adelantos, (Vila-Coro. M, 1995) alude al concepto Biojurídica, otros autores emplean el término Bioderecho o Derecho Biomédico

8. Declaración Universal de los Derechos Humanos de la ONU, fue adoptada por la Asamblea General de la Naciones Unidas en su Resolución 217 A (III), del 10 de diciembre de 1948, Paris (Francia), se puede consultar en la URL https://www.un.org>about-us>universal-decla:

9. La Corte Interamericana de Derechos Humanos fue creada en noviembre de 1969 en San José (Costa Rica) en la Conferencia Especializada en Derechos Humanos, estaba conformada por 25 naciones Americanas. Al día de hoy se han adoptado un sin número de instrumentos de carácter internacional, entre los cuales se encuentra la adopción de la Convención Americana sobre los Derechos Humanos, entre las funciones de esta última Convención están las siguientes: jurisdiccional, consultiva y de adopción de medidas provisionales, se puede consultar en la URL https://www.corteidh.or.cr

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

y se hace referencia a la Bioética y Derecho, considerándola una rama específica de la Bioética que se ocupa de los aspectos éticos y jurídicos de las actividades Biomédicas y cuyo objeto está constituido por la dimensión normativa que tienen repercusión jurídica (Méndez Baiges, 2010)

Cuando deba intervenir el Derecho, en relación a la regulación jurídica de la Biomedicina, el sociólogo alemán (Beck.U, 1986) señaló que el elemento que caracteriza a las sociedades tecnológicas es el riesgo y la hipertrofia legislativa, manifestada por medio de una ingente cantidad de normas para regular cualquier eventualidad, pero no debemos olvidar que el legislador debe ser prudente ya que el objeto de esta regulación se caracteriza por ser imprevisible e incierto y se hace necesario esperar para ver la dirección que toman en la sociedad estos acontecimientos.

Pero se debe apreciar que junto a las normas existe un Código Deontológico mediante el cual los profesionales deben regular su actividad, siendo por ello una regla vinculante de carácter interno que es la expresión de la ética de un colectivo concreto, por ejemplo, la Asociación Médica Mundial en 1964 llevó a cabo la Declaración de Helsinki[10] de principios éticos de la investigación médica en seres humanos, no cabe duda que éstas constituyen algo más que dictados de la moral y su carácter de instrumento de control social fuera del ordenamiento jurídico, debemos señalar que la prudencia no conlleva que el legislador renuncie a sus argumentos de la imprevisibilidad científica y que de algún modo abandone la resolución de los conflictos sociales que plantea la Biomedicina a la praxis judicial, sin embargo en la Doctrina se encuentra la primacía de la vía judicial frente a la legislativa, ya que el recurso a las sentencias de los tribunales, muy habitual en el Common Law, puede ser de utilidad para la resolución de supuestos no expresamente previstos en el ordenamiento jurídico.

III. El Big Data como factor determinante en la IA

En otro estado de cosas, los factores determinantes que han impulsado la IA son el Big Data y el desarrollo tecnológico-computacional que permite que los datos sean objeto de tratamiento por medio de complejos modelos algorítmicos, destacando el *machine learning* (aprendizaje de la máquina), donde la IA tiene por objeto que los sistemas informáticos desarrollen procesos lógicos que simule a la mente humana.

Desde el punto de vista jurídico, se basa en:

10. La Asociación Médica Mundial en 1964 llevó a cabo la Declaración de Helsinki, esta Declaración fue adoptada por la XVIII Asamblea Médica Mundial (AMM), Helsinki (Finlandia), junio 1964, que fue enmendado, 1°) por la XIX AMM, Tokio (Japón), octubre 1975, 2°) XXXV AMM, Venecia (Italia), octubre 1983, 3°) por la XXXXI AMM, Hongkong, septiembre 1989, 4°) por la XXXXVIII Asamblea General (AG), Somerset West, Sudáfrica, octubre 1996, 5°) por la LII AG, Edimburgo (Escocia), octubre 2000. Nota de clarificación, agregada por la AG de la AMM, Washington 2002.Nota de clarificación, agregada por la AG de la AMM, Tokio (Japón) 2004. 6°) LIX AG, Seúl (Corea), octubre 2008 y 7°) LXIV AG, Fortaleza (Brasil), octubre 2013, se puede consultar en la URL https://www.wma.net

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

1. El riesgo de identificar o re identificar los datos anónimos como pertenecientes a una persona determinada a través del Big Data o la llamada "minería de datos".
2. La toma de decisiones fundamentadas en procesos de automatización o perfiles obtenidos de los pacientes vaciando de contenido la autonomía del paciente.
3. La automatización en la toma de decisiones basadas exclusivamente en propuestas algorítmicas del sistema de IA que pueden anular la independencia decisional del profesional, siendo aceptada por éste sin fundamento.
4. El riesgo de clasificar a los pacientes atendiendo a los perfiles personales obtenidos de ellos, tomando decisiones discriminatorias o arbitrarias basadas sólo en esos perfiles
5. La capacidad sobre los elementos esenciales y sobre el proceso por el que un sistema de IA ha llegado a la conclusión indicando su propuesta, pero no aporta información significativa, esto comporta el riesgo que el profesional de la salud no pueda validar o descartar de forma razonable la propuesta del sistema al pretender adoptar su propia decisión, discutiéndose su propia responsabilidad si se acredita la existencia de algún error en el sistema o en el propio profesional
6. El aumento de otras prácticas discriminatorias o estigmatizadoras las cuales están prohibidas por la comunidad internacional o la legislación interna.

El Big Data comporta además una alteración cuantitativa del procesamiento de enormes cantidades de datos, sino también un cambio cuantitativo que aporta información que aparentemente no está implícita en los datos (exploración directa del paciente por parte del médico), todo ello precisa de un marco normativo que lo podemos encontrar en el Reglamento General de Protección de Datos de Europa (RGPDE), 2016/679, de 27 de abril[11] sin embargo la Ley no puede prever la naturaleza de estos datos y en función de ella establecer un régimen jurídico, en definitiva el Big Data presenta una importante novedad y un desafío, debiendo dirigirnos para ello al RGPD para comprobar si ese marco es suficiente para su regulación, estos interrogantes se plantean en el Derecho interno, en ese sentido la Ley Orgánica de Protección de Datos de carácter personal (LOPD) 3/2018[12], de 05 de diciembre desarrolla el Reglamento General de Protección de datos (RGPD) 2016/679[13], del 27 de abril, recoge criterios adaptados a las exigencias jurídicas derivadas de la aparición del Big Data, pero en relación a los datos relacionados con la salud su contenido no está dirigido al tratamiento de datos en el marco asistencial, sino en el de la investigación biomédica. El desarrollo de la tecnología está irrumpiendo en la asistencia sanitaria de muchas maneras, la más importante es la digitalización de las historias clínicas (HCE), que permiten recopilar por métodos digitales y de forma sistematizada la información de salud del paciente, tratamiento, diagnósticos, que acumula una gran cantidad de datos.

11. Reglamento Europeo de Protección de datos, 679/2016, DOUE núm 119 de 4 de mayo de 2016 págs 1 a 88, Referencia DOUE-L-2016-80807
12. LOPD 3/2018, BOE n° 294, 06 de diciembre 2018, Ref: BOE-A-2018-16673
13. RGPDE 2016/679, de 04 de mayo 2016, op. cit., pág. 5

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

Los datos masivos se caracterizan por la gran variedad en el tipo de datos y fuentes utilizadas en el ámbito sanitario, podemos distinguir: a) Texto no estructurado (notas médicas), b) Datos generados de forma continua (monitores, ponibles, etc.), c) Datos estructurados, que son notas de programación neutrolingüísticas (PLN) y d) Datos oscuros cómo correos electrónicos. Estos datos se pueden obtener en un formato estructurado, no estructurado o semiestructurado y se adquieren de fuentes primarias como los sistemas de apoyo de decisión clínica o secundarias como farmacias y laboratorios, pero lo más complejo de los datos masivos es que en su mayoría son cualitativos no estructurados o incongruentes, esto dificulta el proceso y análisis de imágenes u otras formas de procesamiento, los tipos de datos utilizados más frecuentemente son las publicaciones de investigación, entre otros.

El Aprendizaje automático es una sub discilplina de la IA que consiste en resolver el análisis de datos mediante la búsqueda de patrones entre ellos, los patrones brindan la oportunidad de comprender situaciones de salud complejas o predecir los resultados de salud futuros, ésta puede clasificarse en tres tipos: a) supervisado b) no supervisado y c) aprendizaje semi supervisado. El *deep learning* (aprendizaje profundo) utiliza diversas áreas de conocimiento como la ciencia de datos y la optimización. El aprendizaje profundo que se utiliza para el tratamiento de datos complejos, son especialmente adecuados para tratar datos no estructurados y secuenciales.

IV. El derecho de información al paciente

En este análisis legal tenemos que dirigirnos hacia el Derecho a la información y explicación al paciente, la literatura jurídica ha abierto un debate sobre la existencia de estos derechos, su explicación en el RGPDE y su alcance cuando se elaboran perfiles o se toman decisiones automatizadas que pueden afectar a la capacidad de las personas para acceder a determinados servicios o bienes se debate si los pacientes tienen derecho a recibir explicaciones sobre el sistema decisional de un sistema de IA, en cualquier caso el derecho a la información está garantizado en la legislación interna previa que son matizadas por el RGPDE (art. 22, apartados 1 y 4).

En todo caso el derecho a la información asistencial respecto a la IA debe ser objeto de un análisis más profundo en el plano jurídico, tanto que garantice que los facultativos cumplan con sus deberes en relación a los derechos de los pacientes y proveer las decisiones más adecuadas respecto a su salud, pero debemos asumir que en la práctica clínica y asistencial está plagada de sesgos humanos que son similares a los sesgos automatizados, por ejemplo el sesgo humano en una historia clínica o el sesgo en el modelo algorítmico, cuyos resultados no son válidos; algunos autores señalan que detrás de alguna de las propuestas y regulaciones de la IA, que busca hacer más transparentes las herramientas algorítmicas, hay una suposición implícita, que impone un nivel más alto de transparencia de lo que normalmente se le impondría a los responsables de toma de decisiones humanas, sin embargo será difícil encontrar un sistema de IA que decida directamente sin la intervención humana, en el caso de Decision Support

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

Systems la decisión final seguirá recayendo en el facultativo aunque la automatización obligará a redefinir los papeles en la relación médico-paciente. Aún será un poco más complicado que la disponibilidad de las TIC avanzadas puedan llegar a tomar decisiones completamente automatizadas.

Otro importante problema jurídico está referido a la elaboración de perfiles para clasificar a los pacientes en relación a características similares en base a determinados patrones, dando mayor importancia a las decisiones automatizadas que a las del médico sin darle la oportunidad de individualizar. Concretando: cualquier decisión que se apoye en un sistema basado en el procesamiento automatizado de algoritmos debe ser revisado por un ser humano cualificado, que considere las propuestas y de asegurar la opción por un tratamiento alternativo.

Atendiendo a la normativa europea las decisiones asistenciales no pueden basarse en los perfiles que se obtienen de los pacientes ya que, esta prohibición es inteligible con la esencia individualizadora que está abriendo el camino hacia la Medicina Personalizada de Precisión, esta perspectiva metodológica es la más adecuada para prevenir la asunción de conclusiones equivocadas en las que puede recaer un sistema computacional, de las cuales el paciente puede verse afectado no sólo en su capacidad de decisión sino también en sus expectativas.

Un problema importante es la falta de transparencia de los procesos decisorios algorítmicos basados en los sistemas de IA, es decir lo que se conoce como opacidad o caja negra (Black Boxes), por eso la transparencia ha ido ganando terreno en los procesos automatizados que ha llegado a manifestarse como un derecho prestacional, o sea, se entiende que toda información y comunicación relacionada con el tratamiento de los datos personales sea accesible y entendible, esto es decisivo ya que, la falta de interpretabilidad de los sistemas de IA es una de las limitaciones más importantes a implementar en la práctica médica, siendo necesario el aumento de la transparencia en la automatización. Los riesgos de la automatización de los datos pueden dar lugar a sesgos que pueden derivar en decisiones arbitrales o discriminatorias y en definitiva a la opacidad de la Inteligencia Artificial.

En este contexto, en Europa el RGPDE[14] concede el derecho a la explicación en el Considerando 71, algunos académicos dudan de la existencia jurídica y la viabilidad de este derecho ya que el Considerando 71 y el derecho a la explicación no son jurídicamente vinculantes ni tampoco exigidos por el art 22.3, RGPD y, por tanto, no hay obligación de abrir las cajas negras de las aplicaciones de IA en el ámbito de la salud. Sin embargo, los artículos 14.2 g, 13.2 f y 15.1 h, del RGPD, permiten al menos a los interesados obtener información significativa sobre la cuestión, así como de la importancia y consecuencias previstas de los sistemas automatizados de adopción de decisiones.

Cómo complemento del RGPD encontramos el Reglamento (UE) 2018/1807[15] donde en su artículo 9 establece que es directamente aplicable desde el 28 de mayo de 2019,

14. RGPD, op. cit., pág. 5
15. Reglamento (UE) 2018/1807, DOUE n° 303, 26 de noviembre, 2018, Ref: DOUE-L-2018-81888 , págs. 59 a 68

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

además recoge un marco de libre circulación de datos no personales en la UE estableciendo en su art 1 la disponibilidad de los datos para las autoridades competentes o los requisitos de localización de datos, el Reglamento se aplica al conjunto de datos no personales y el RGPD se aplica a los datos personales como no personales estando ambos indisolublemente unidos .

V. Responsabilidad del uso de la IA en la asistencia sanitaria

En cuanto al uso en la intervención sanitaria asistencial de robots y sistemas inteligentes autónomos o no, se pueden producir lesiones o muertes de los pacientes como consecuencia de las decisiones tomadas por ellos, y esto lleva a preguntarnos ¿si un sistema de IA puede ser imputado como sujeto activo de delito y ser directamente responsables?, en este caso hacemos referencia a la asistencia sanitaria, cuando se plantea el resultado dañoso o lesivo para el paciente, se puede imputar jurídicamente a los profesionales que intervienen como apoyo del sistema robotizados o sistemas inteligentes en el diagnóstico o en el tratamiento de las enfermedades, no debemos olvidar que que el sistema de IA puede dar conclusiones erróneas al procesar gran cantidad de datos, la Doctrina del riesgo en esta materia sería del todo aplicable en estos casos, y siendo conscientes que el Derecho Penal debe ofrecer una función preventiva en relación con las tecnologías, en un futuro mediante una fuerte intervención administrativa reforzada por normas que articulen el funcionamiento permitido de los sistemas de IA. En cuanto a los delitos imprudentes el *Compliance* consistiría no sólo en la existencia de procedimientos organizativos y de gestión del riesgo que previniera el desarrollo de una negligente planificación, sino también, basada en estructuras o procedimientos en cuanto a la prevención de la toma de decisiones rutinarias derivadas de las conclusiones del sistema de IA, una segunda posibilidad sería el examen minucioso del sistema por técnicos independientes valorando la adecuación de esos sistemas para el servicio que debe prestar, teniendo en cuenta el grado de error predecible y la posibilidad de bloquear su uso en caso de emergencia, cuya valoración positiva daría lugar a la utilización pública o privada del sistema de IA, mediante la configuración de estándares practicables en situaciones predecibles acotando el riesgo permitido (típicas o conocidas) .

Sin embargo, esta idea tiene características de difícil subsunción normativa, retornando de nuevo a los criterios normativos de la imprudencia, por ejemplo el principio de confianza la persona que participa en una actividad actuará en la confianza en conjunción con otro elemento normativo que se mueve en la esfera de la acción diligente no en la imputación objetiva del resultado, por ello lo que preocupa es que un sistema de IA dañe a una persona (paciente), ya que, el sistema no parece capaz de valorar y de conocer el contenido del deber de cuidado para lo que sólo son aptos los seres humanos al menos al día de hoy. En resumen el principio de confianza decaería para el médico cuando apreciara el indicio de un error, como presupuesto objetivo, neutral y aún todavía no normativo. Para que el sujeto humano pueda valorar el indicio de ese error ha de evaluar las propuestas decisionales del sistema de IA, ya que, de lo contrario los

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

indicios serían inapreciables y podría motivar al sistema a tomar sus propias decisiones frente aquél.

Un estudio de la Universidad de Stanford[16], en relación a los cuidados paliativos, entrenaron una Red neuronal profunda de datos basada en los días de hospitalización, el diagnóstico, edad del paciente, con el fin de medir la mortalidad de cada paciente entre 3 a 12 meses, este sistema de IA ahorraría al equipo de cuidados paliativos la carga de las revisiones de los pacientes "Algoritmo de la muerte".

Los sistemas de IA, que fueron estudiados en el precedente estudio se encuentran en su gran mayoría en fases experimentales, sin embargo existen excepciones muy avanzadas, por ello, esto nos lleva a preguntarnos ¿Cuáles son los cauces jurídicos apropiados que éstos sistemas de IA deberían seguir para ser validados conforme a los elevados estándares de seguridad y calidad?, de hecho para contestar esta pregunta debemos tener en cuenta a la FDA, este documento señala la necesidad de una regulación basada en la categorización del riesgo, es decir, los sistemas de IA se categorizarían dentro de las cuatro categorías del riesgo (mayor a menor), quedando el profesional para decidir si acepta o rectifica sus propuestas. En el ámbito europeo existen documentos de organismos como la Comisión europea, el Consejo Económico y Social Europeo así como de un grupo de expertos creados en el seno de estas instituciones que han desarrollado directrices, recomendaciones y principios básicos que deben guiar la implementación de las políticas en esta materia incluido su reflejo en una futura regulación o adaptación normativa, con especial mención a su enfoque ético, estas medidas están destinadas especialmente a la robótica, como la Resolución dictada por el Parlamento Europeo de 16 de febrero de 2017 con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, así como un Código Deontológico que está dirigido a los comités de ética de la investigación, en esta línea la Comisión Europea ha asumido un papel bastante activo ya que presentó en abril de 2018 un paquete de medidas basado en una Comunicación centrada en la inteligencia artificial para Europa, con tres pilares siendo uno de ellos la necesidad de un marco ético y jurídico adecuado para este objetivo se creó un grupo de expertos *High Level Expert Group on Artificial Intelligence* (IA HLEG)[17] que ha publicado las directrices éticas *Ethics Guidelines For Trustworthy* AI, de 8 de abril de 2019, el desarrollo de esta tecnología conlleva el acceso a una gran cantidad de datos y por ello indicamos el Reglamento UE 2018/1807 del Parlamento y del Consejo, de 14 de noviembre de 2018[18], sobre circulación de datos no personales, Esta política del uso de los datos se extiende al ámbito sanitario con la finalidad de obtener una asistencia sanitaria más enfocada a la promoción de la salud, la prevención y centrada en el paciente. El artículo 5.2, del RGPD, recoge la llamada Responsabilidad Proactiva en la

16. Este estudio podemos encontrarlo en la URL www.med.stanford.edu/paliative-care

17. High Level Expert Group on Artificial Intelligence (IA ,HLEG), DOUE C 252/239, Ref: DOUE 2018/C 252/25

18. Reglamento (UE) 2018/1807 del Parlamento y del Consejo de 14 de abril de 2018, relativo al marco para la libre circulación de datos no personales en la UE, DOUE: núm 303 de 28 de noviembre de 2018, págs 59 a 68, Referencia DOUE-L-2018-81888.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

que el responsable del tratamiento de los datos deberá cumplir con lo preceptuado en su apartado 1 integridad y confidencialidad, y la adopción de medidas técnicas y organizativas, la responsabilidad está implícitamente regulada en el Dictamen 3/2010 sobre el principio de responsabilidad[19]

Para continuar con las implicaciones legales de la Inteligencia artificial debemos mencionar algunas publicaciones al respecto por ejemplo el Consejo de Europa en la Recomendación CM/Rec (2020) del Comité de Ministros de los Estados Miembros sobre los impacto de los sistemas algorítmicos en los Derechos Humanos de 8 de abril de 2020, la UNESCO sigue a la UE en su Anteproyecto de Recomendación sobre la Ética de la IA al igual que los principios Éticos de la OCDE en materia de inteligencia artificial adoptado en mayo de 2019.

A nivel Doctrinal la IA está definida como la ciencia y la ingeniería de crear máquinas inteligentes especialmente programadas por computación inteligente, y por esta razón la regulación normativa de la IA, desde un punto de vista antropocéntrico, debe estar exenta de dificultades; el avance de la tecnología nanotecnología nos hace pensar que la ciencia avanza mucho más rápido que el Derecho, y por ese motivo encontramos respuestas imperfectas. La relación entre el Derecho sanitario y la IA ha supuesto numerosos problemas, sin embargo, existe un punto positivo ya que esta tecnología debe ser entendida como un instrumento o herramienta de apoyo al trabajo del jurista.

El marco regulatorio debe convertirse en un incentivo para facilitar la financiación incluyendo el respeto a los derechos fundamentales, como son la intimidad, la dignidad enfocados en la protección de datos, por ello la UE no debe rebajar la protección que se le ofrece a los ciudadanos en materia de privacidad. El Derecho debe considerar el grado de ponderación de los principios utilizados para el otorgamiento de los derechos, y podemos afirmar que según vaya avanzando y cambiando la sociedad y la IA surgirán nuevos derechos susceptibles de protección.

En el análisis que nos ocupa la autonomía, la privacidad, la rendición de cuentas y la responsabilidad deben ser matizadas para hacer frente al desafío de la IA y por otro debemos plantearnos la regulación jurídica en lo referente a la responsabilidad profesional para toda nueva innovación que está sujeta a los dictados de la Ley, en este sentido no existe una definición consolidada de la IA, pero sin embargo, se está de acuerdo que trata de emular la inteligencia humana en sistemas informáticos y en la sanidad se utilice para el campo del diagnóstico o bio marcadores de ciertas enfermedades. Se ha diferenciado entre Inteligencia superior e inteligencia general o humana y especial, la inteligencia superior (IA), que sin ninguna duda es una hipótesis hoy día, es una inteligencia muy superior a la humana. La inteligencia general o humana que constituye el prototipo típico de la IA y, por último, la inteligencia especial que utiliza grandes volúmenes de datos de forma superior a la humana, pero en el que el elemento decisorio es la persona humana, por ejemplo en EEUU la compañía Mountain Blue ha presentado un modelo de aprendizaje profundo para detectar el cáncer de mama y cuenta además

19. Dictamen 3/2010, sobre el principio de responsabilidad, 00062/10/ES, GT 173, adoptado el 13 de julio de 2010.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

con algoritmos para detectar enfermedades como ataques cardíacos, o derrames cerebrales que además cuenta con un asistente por voz que anima a los usuarios a preguntar sobre sus afecciones médicas.

VI. La robótica inclusiva

La robótica inclusiva es aquella que se ha desarrollado especialmente en el ámbito de la sanidad y los cuidados, en este sentido las funciones que pueden desempeñar los robots son muy variadas cirugía, farmacia, rehabilitación, robots hospitalarios y se han señalado tres grandes campos de aplicación de la robótica en este campo, que están enumeradas en la resolución con recomendaciones sobre normas de derecho civil sobre robótica, como son el quirúrgico, la rehabilitación y asistencial de cuidados, el robot que se encuentra más generalizado es el quirúrgico que dota al cirujano de una mayor precisión con muchas ventajas para el paciente como los tiempos de operación, o recuperación por ejemplo: el robot Da Vinci, éstos robots pueden almacenar el historial de la intervención realizada, las constantes vitales relacionadas con la intervención quirúrgica realizada, entre los robots asistenciales, o de rehabilitación de funciones corporales dañadas o exoesqueletos, o las prótesis biónicas que preocupan en especial a la Resolución del 16 de febrero de 2017[20] ya que pueden modificar la concepción del cuerpo humano sano.

La prevención de enfermedades debería tener un papel importante en la asistencia sanitaria este extremo sólo se podrá conseguir si la sociedad accede a una tecnología que pueda ofrecer una información precisa sobre el estado de salud y bienestar los dispositivos inteligentes o "ponibles" son sólo una de las diversas herramientas utilizadas por las personas para controlar sus constantes vitales pudiendo incluso el paciente ser supervisado por un profesional sanitario para que el paciente aplique los cambios necesarios antes que se produzca una enfermedad que ponga en riesgo su vida, además los pacientes clínicos también se beneficiarán de esta tecnología ya que, los profesionales sanitarios podrán atender a los pacientes teniendo acceso inmediato a los síntomas o a cualquier prueba de imagen y a los tratamientos que facilita la toma de decisiones y se beneficien de intervenciones que de otra manera hubiera sido casi imposible de aplicar, en resumen la IA aplicada a la medicina es la denominada IA estrecha que sólo puede realizar un conjunto de tareas relacionadas y entrenarse para ellas desde el análisis de imágenes médicas hasta el aprendizaje del habla humana, por ello las operaciones realizadas con la IA estrecha son realmente eficientes y competentes y en ocasiones supera a los seres humanos.

VII. La medicina de precisión

La medicina de precisión posibilita la adaptación de las intervenciones sanitarias a individuos o grupos de pacientes atendiendo al perfil de su enfermedad, la información

20. Resolución 2015/2102 (INL) DOUE C 252/201, Ref: DOUE 2018 C 252/22

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

sobre el diagnóstico, el objetivo de este tipo de medicina es utilizar la biología individual en lugar, de la biología poblacional en todas las fases del recorrido de un paciente por la asistencia sanitaria esto implica la recopilación de datos como la información genética y su ventaja más notable es la reducción en los costes de la asistencia sanitaria, la disminución de la respuesta adversa a los medicamentos, entre otras.

Existen muchos tipos de medicina de precisión y las podemos dividir en tres clases:

- Algoritmos complejos para el tratamiento de una gran cantidad de datos basado en el aprendizaje automático que realiza predicciones al pronóstico.
- Aplicaciones a la salud digital que procesan y registran datos añadidos por los pacientes a través de los dispositivos "ponibles"
- Pruebas basadas en la información genética de un grupo de población se utiliza por algoritmos de aprendizaje automático para encontrar respuestas al tratamiento de un paciente individual por ejemplo la administración de un tratamiento personalizado.

En resumen, el aprendizaje profundo tiene numerosas posibilidades, como por ejemplo la predicción en las propiedades de los fármacos, la generación ex novo de nuevas estructuras químicas mediante redes neuronales como la ingeniería proteica, las visualizaciones médicas, para diagnóstico y cirugía o el reconocimiento de las imágenes médicas.

VIII. Robots asistenciales

Se utilizan para dar soporte a las limitaciones físicas en ancianos y personas disfuncionales que les ayuda asistiéndolas en las actividades diarias y actuando como sus ojos y manos y pueden ayudar en las tareas cotidianas.

El robot asistencial RIBA que ayuda a los pacientes a levantar y mover cosas pesadas además se le puede dar instrucciones con sensores táctiles.

Otro robot asistencial es MARIO que aborda los problemas de aislamiento y demencia en los ancianos, estas aplicaciones utilizan herramientas potenciadas por la IA para procesar los datos recogidos por los robots con el fin de realizar tareas de reconocimiento facial o la identificación de objetos y procesos de diagnóstico, otra variante de estos robots son los llamados ayudantes cognitivos, que se utilizan como proceso de estimulación cognitiva en métodos de rehabilitación después de lesiones cerebrales por un accidente cerebrovascular o traumatismos, es el caso de VITRAEL se trata de una plataforma de estimulación cognitiva que sirve para evaluar entrenar o estimular habilidades cognitivas que se han deteriorado en el paciente esta aplicación funciona a través de la comunicación, la configuración y los juegos, mejorando significativamente las habilidades cognitivas del paciente como la atención o la planificación.

Una de las aplicaciones de los robots asistenciales y los robots de compañía para la estimulación social y emocional reduciendo la depresión o el estrés conectando emo-

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

cionalmente con el paciente por ejemplo la mascota robótica PARO o bebé foca robótico qué ayuda a detectar el tacto y los objetos visuales. Otro robot compañero es *Buddy* de *Blue Frog Robotics* que mediante sus sensores detecta caídas en las personas mayores, en conjunto los estudios relacionados con la investigación de la estimulación cognitiva demuestran una disminución de la velocidad del deterioro cognitivo y la progresión de la demencia.

IX. La inteligencia artificial y los seguros de salud

Los principales retos a los cuales se enfrenta el sector de los seguros de salud son la evaluación del riesgo, la estimación de primas, el fraude, la medicina preventiva, la competencia y la asistencia al cliente, además de los desafíos que supone el coste de la atención médica, el aumento de las expectativas de los consumidores en cuanto a la calidad de los servicios y los gastos generales producidos por la legislación que están aumentando en la mayoría de los países.

La IA es cada vez más utilizada por los proveedores de seguros de salud a través del *Big Data* es decir, por el tratamiento de una gran cantidad de datos para identificar el fraude, controlar los precios e identificar los riesgos, según el informe Gartner los tres principales usos de la IA en la industria de los seguros son: a) El análisis del fraude, b) Los chatbot y c) La optimización de los procesos.

Se estima que las aseguradoras pueden ahorrar hasta 7.000 millones de dólares en 18 meses con el uso de la IA, haciendo más eficientes las tareas administrativas y reduciendo el malgasto, hay varias maneras por la cuales la IA puede ser usada para reducir los costes mediante aplicaciones que se pueden agrupar en cinco categorías: 1) Mejorar la experiencia del cliente, 2) Reducir el fraude, 3) Mejorar la eficiencia de las oficinas, 4) Reducir los riesgos y optimizar las cuotas y 5) Crear nuevas oportunidades de negocio.

La industria de los seguros de salud con la aplicación y el uso de la IA puede beneficiarse de forma muy significativa.

X. Desafíos legales y éticos de la asistencia sanitaria y la IA

En este epígrafe vamos a analizar brevemente que es la IA y daremos una visión general de las tendencias relativas a la ética y al derecho de ésta en la atención sanitaria en EEUU y en Europa, en base a cuatro puntos principales, relacionados con el aspecto ético: a) El consentimiento informado para su uso, b) La seguridad y transparencia, c) La equidad y el sesgo algorítmico d) Privacidad de los datos.

En relación al aspecto legal diferenciamos cinco desafíos legales tanto en EE UU como en Europa que son: la seguridad y eficacia, la responsabilidad, la protección de datos y la privacidad, la ciberseguridad y la Ley de Propiedad intelectual. Para hacer realidad el enorme potencial de la IA, las partes interesadas en la esfera de la IA incluidos los fabricantes, los médicos, los pacientes y los especialistas en ética y legisladores deben participar en el debate ético y jurídico sobre la forma en que la IA se aplica en la práctica.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

Comenzamos con el primer inciso el breve análisis de lo que se entiende por inteligencia artificial desde la óptica de la selección de algunos subtipos, como el aprendizaje automático, como subconjunto de la IA sobre todo en el ámbito de su aplicación en la salud que permite a los sistemas computacional aprender de los datos. Este AA emplea las redes neuronales artificiales con múltiples capas para identificar patrones en un conjunto de datos muy grande estos algoritmos se encuentran más cerca de las cajas negras siendo los resultados muy difíciles de interpretar por los clínicos.

La atención sanitaria en los EEUU y la IA durante la presidencia de Barack Obama, los informes del gobierno de los EEUU sobre la IA destacaron sus aplicaciones para el bienestar público y sus aspectos de equidad, seguridad y gobernanta, además de mejorar la equidad la transparencia y la responsabilidad por diseño, así como crear una IA ética, sin embargo, desde la presidencia de Donald Trump la estrategia de la IA ha cambiado hacia un enfoque más orientado al libre mercado.

La American Industry Summit, en mayo de 2018[21], una de sus principales conclusiones fue que la administración Trump que tiene por objeto eliminar las barreras regulatorias para la investigación de IA. En enero de 2020 la Casa Blanca publicó un borrador de orientación para la regulación de la IA con 10 principios que los organismos deben tener en cuenta a la hora de formular planteamientos de las aplicaciones de la IA: Confianza pública en la IA, Participación pública, Integridad científica y la calidad de la información, Evaluación y gestión de los riesgos, Beneficios y costes, Flexibilidad, Equidad y no discriminación, Divulgación y transparencia, Seguridad y protección y Coordinación entre organismos.

En otro orden de cosas EE.UU encabezó, los esfuerzos históricos en el desarrollo de los principios de la IA innovadora y digna de confianza dirigida al respeto de los valores democráticos y de los derechos humanos.

En junio de 2019, el G-20 también publicó los principios de la IA extraídos de los principios de la OCDE para la IA[22], en relación a la Directiva 2019/1024 del Parlamento Europeo y del Consejo, desde enero de 2017 se han presentado numerosos proyectos de ley relacionados con la IA en EEUU por ejemplo SELF DRIVE Act H.R.3388, FUTURE of Artificial Intelligence Act 2017, H.R. 4625 y S.2217 y AI JOBS Act 2019, H.R. 827, además el Estado de California ha publicado en agosto de 2018 la legislación ACR 215 que respetaba los 23 principios de la IA de Asilomar(son una extensión de las leyes de Asimov con el fin de establecer las bases del desarrollo de las futuras plataformas de IA).

Por otro lado, el IDx-DR es el primer sistema de diagnóstico de IA autorizado por la FDA que proporciona una decisión autónoma de selección sin necesidad de que un ser humano interprete la 8imagen o los resultados que ésta basado en la IA para detectar un nivel más alto de retinopatía diabética en pacientes adultos entre los 22 años y más.

21. La American Industry Summit borrador de orientación para la regulación de la IA publicado por la Casa Blanca (Office of Science and Technology Policy, de 18/05/2018), se puede consultar en la URL https://amvirtual.vfairs.com

22. Los principios de la IA extraídos de los principios de la OCDE para la IA, los podemos encontrar en la URL https://www.oecd.org/digital/state/of/implementation/of/the/oecd/ai/principles/1cd40c44/en.Htm.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

En el caso de Europa, la Comisión Europea aprobó su estrategia de IA para Europa en Abril de 2018[23] esta tiene por objeto garantizar un marco ético y jurídico adecuado mediante la creación de la Alianza Europea para la IA y la elaboración de directrices éticas, además señala la Comisión la necesidad de reforzar la inversión tanto pública como privada en IA.

Um grupo de expertos de alto nivel sobre la IA o High Level Expert Group on AI, de la Comisión Europea designado en junio de 2018 y también es grupo directivo de la Alianza Europea para la IA publicó las directrices éticas en abril de 2019 que promueven la IA confiable y contienen siete requisitos, agencia y supervisión humanas, robustez y seguridad técnicas, privacidad y gobernanza de datos, transparencia,diversidad, y no discriminación y justicia, bienestar ambiental y social y responsabilidad, además publicó un documento sobre la definición de IA.

En febrero de 2020 la Comisión Europea publicó el Libro Blanco sobre la IA que contiene el enfoque europeo sobre la excelencia y la confianza, y también publicó una Comunicación sobre la Estrategia Europea para los datos y un Informe sobre las consecuencias en materia de responsabilidad y seguridad de la IA, internet de las cosas y la robótica.

En Europa existen diversos proyectos de aplicaciones dirigidas a la salud por ejemplo Ada, que evalúa los síntomas de un individuo y le da orientación, Google Health, Ultromics que se dedica a reducir los diagnósticos erróneos y prevenir la aparición temprana de enfermedades cardiovasculares.

Entre los desafíos éticos surgidos en el apartado anterior entre los más importantes encontramos en la práctica clínica y la asistencia sanitaria, el consentimiento informado derecho a la información del paciente, este es uno de los retos más directos en la integración de la IA en la práctica clínica. Otro de los desafíos es la seguridad y transparencia, es el caso de IBM Watson for Oncology que utiliza algoritmos de IA para evaluar la información de los registros médicos de los pacientes y ayudar a explotar opciones de tratamiento.

El tratamiento de los datos debe ser fiable y válido ya que cuanto mejor sean los datos de entrenamiento mejor será el rendimiento de la IA, en relación a la seguridad debe garantizarse cierto nivel de transparencia en este sentido las auditorías externas pueden ser una posible solución.

En cuanto al sesgo algorítmico y la equidad, la IA tiene la capacidad de mejorar la asistencia sanitaria y de democratizar esta asistencia, pero conlleva un riesgo de sesgo y por tanto de discriminación y de diagnósticos erróneos, algunos de estos sesgos pueden resolverse debido a la mayor disponibilidad de datos, sin embargo, el mayor número de algoritmos son complejos y no transparentes.

Otro desafío ético es la privacidad de los datos es imperativo proteger a los pacientes contra los usos ajenos médico/paciente que puedan afectarles negativamente, como las repercusiones en las cuotas de seguros de salud o las relaciones personales, por ello es necesario contar con una sólida legislación antidiscriminatoria similares a los regímenes en materia de privacidad genética.

23. Comunicación 2018, de la Comisión Europea, centrada en la IA COM (2018) 795 final, del 07 de diciembre de 2018, se puede consultar en la URL https://eur-lex.europa.eu>TXT

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

XI. Responsabilidad en las nuevas tecnologías en Estados Unidos y Europa

En materia de responsabilidad las nuevas tecnologías basadas en la inteligencia artificial plantean problemas para los actuales reglamentos de responsabilidad.

En Estados Unidos, pensemos el siguiente supuesto: un software de ADC basado en la IA da una recomendación que acaba con un diagnóstico incorrecto resultando lesivo para el paciente, el clínico será directamente responsable de la negligencia médica, ya que los clínicos deben actuar con el adecuado deber de cuidado, aunque la decisión se haya adoptado de buena fe en un algoritmo AA de caja negra, ya que el software de AA está bajo el control de un profesional de la salud que toma la decisión final, en el imaginario de todos se puede concluir que para eludir la responsabilidad por negligencia médica, los médicos utilizarían la IA como instrumento de confirmación por temor a la responsabilidad, en este sentido se podría mantener el antiguo régimen de responsabilidad que intenta cumplir dos funciones del derecho civil, por un lado la disuasión y por otro la indemnización de las víctimas. Se ha propuesto un modelo de responsabilidad del producto que sea exigible a los diseñadores de la IA, es decir la constitución de una responsabilidad objetiva del fabricante por los defectos, pero los Tribunales han tenido dudas en la práctica a la hora de aplicar las teorías de la responsabilidad por productos.

En la cuestión de la indemnización en Estados Unidos existe la compensación por vacunas donde los fabricantes de vacunas pagan un fondo para posteriormente responder por los riesgos de la vacunas, en el caso de las responsabilidad de los hospitales se les podría demandar en atención a las teorías de la negligencia empresarial y responsabilidad indirecta cuando se contrata una IA, y también acompañar a la protección de la responsabilidad con un plan de aprobación previa que examine a los fabricantes y profesionales de la salud de ciertas formas de responsabilidad.

En la actualidad no existe un marco reglamentario armonizado en la UE para la responsabilidad por la IA y la Robótica como los robots de asistencia y médicos, sin embargo Europa ha abordado la cuestión de la responsabilidad con la publicación de una Resolución del Parlamento Europeo titulada Normas de Derecho civil sobre robótica de 16 de febrero de 2017 [2015/2103 (INL)], en esta resolución se cuestiona si es suficiente el marco jurídico actual o es necesario adoptar nuevas normas en el marco de los actos y omisiones de los robots, la Directiva (85/374/CEE) sobre responsabilidad por productos defectuosos no abarca los avances en materia de robótica adecuadamente, por ello se solicita en esta resolución un una propuesta de instrumento legislativo sobre cuestiones jurídicas relacionadas con el uso de la robótica y la IA en los próximos 10 a 15 años combinado con directrices éticas, se recomienda por un lado una responsabilidad objetiva o bien un enfoque de gestión de riesgos que no se centra en la persona que causó el daño además de un plan de seguro obligatorio y un fondo de indemnización adicional para garantizar el pago de las posibles indemnizaciones recogido en el Anexo de la resolución

En 2018 la Comisión Europea adoptó la Estrategia de IA en un documento de trabajo de los servicios de la Comisión sobre la responsabilidad por las tecnologías digitales

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

emergentes[24] proporcionando al menos una protección básica a las víctimas, además como establece el Formación de Nuevas Tecnologías establecido por la Comisión Europea público otro informe sobre la responsabilidad de la IA y otras tecnologías emergentes que afirmó que aunque los regímenes de responsabilidad están regulados por los Estados miembros, la responsabilidad objetiva por productos defectuosos esta regulado en la Directiva 85/374/CEE[25], finalmente la Comisión Europea publicó en 2020[26] un informe sobre la repercusión en materia de seguridad y de responsabilidad de la IA y robótica, siendo necesario aducir cambios y actualizaciones de los marcos de responsabilidad para abordar adecuadamente los avances tecnológicos.

XII. Proteccion de datos en el uso de la ia en Estados Unidos y Europa

En Estados Unidos, la ley HIPAA[27] en materia de protección de datos tiene importantes lagunas en el entorno de la salud ya que sólo abarca la información específica sobre la salud generada por las entidades cubiertas o sus asociados comerciales, la HIPAA no se aplica a la información no relacionada con la salud además la definición de entidades cubiertas limita su ámbito de aplicación ya que incluye a los servicios de seguros y proveedores de servicios de la salud entre otros, en virtud de la HIPAA la información puede compartirse por razones de de investigación o comerciales ofreciendo dos razones por un lado la determinación por parte de alguien de un conocimiento y experiencia adecuados a los métodos estadísticos y por otro la supresión de los identificadores por ejemplo nombres, números de la Seguridad Social o identificadores biométricos sin conocimiento real de entidad cubierta, ésta no podría proteger adecuadamente a los pacientes debido a la posibilidad de la triangulación de los datos.

Por todo lo expuesto, la Ley HIPAA no es adecuada para la protección de la privacidad de la salud de los pacientes, en resumen esta ley federal debería facilitar tanto las innovaciones incluidas las aplicaciones de IA, en el ámbito de la salud como la protección de la privacidad de la salud de la personas, podemos destacar el Estado de California ha adoptado recientemente el 1 de enero de 2020 la *California Consumer Privacy Act*

24. En relación a las tecnologías emergentes tenemos la Directiva 2015/2366 UE, que da origen a la Comunicación de la Comisión Europea, COM (2018) 109 final, 08/03/2018, DOUE núm 337 de 23 de diciembre de 2015 páginas 35 a 127, Referencia DOUE-L-2015-82575, se puede consultar URL: https://www.boe.es>buscar>doc

25. Directiva 85/374/CEE, DOUE L 210 de 07/08/1985, págs 29 a 33, Ref: DOUE-L-1985-80678

26. La Comisión Europea en un documento de sesión de 05.10.2020, realiza una recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de IA [2020/2014 (INL)], se puede consultar en la URL: https://eur-lex.europa.eu>TXT

27. Health Insurance Portability and Accountability Act (HIPAA), 1996, Ley federal que obliga a la creación de unas normas nacionales par ala protección de información sensible sobre la salud de los pacientes y está cubierta por la llamada norma de la privacidad que contiene estándares para derechos individuales que entiendan y controlen como se usa estas información sobre la salud, se puede consultar en la URL: https://aspe.hhs.gov>reports>heal...

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

de 2018, esta CCPA es un intento de llenar las lagunas jurídicas y mejorar la protección de las personas.

En Europa tenemos el RGPD 2016/679, de 28 de mayo de 2018, que tiene por objeto proteger el Derecho de las personas físicas a la protección de los datos personales, art. 1.2, de aplicación en el marco de las actividades de los organismos en Europa como en terceros países, art 2.3.1. En el contexto de la asistencia sanitaria la definición de datos relativos a la salud se regula en el artículo 4.15, del RGPD, los datos personales relativos a la salud física o mental de una persona incluida la prestación de servicios sanitarios que revelen información sobre su estado de salud el RGPD de la UE tiene un alcance más amplio que la ley HIPAA en Estados Unidos, por decisión automatizada se entiende aquella que se toma sin intervención humana únicamente por medios automatizados (Reglamento 2016/679). Atendiendo al art 22.1, del RGPD, los interesados tendrán derecho a no ser objeto de una decisión basada únicamente en le tratamiento automatizado incluida la elaboración de perfiles que produzcan efectos jurídicos que les afecten de forma significativa, el art 22.2 recoge algunas excepciones salvo que las decisiones se basen en datos genéticos y biomédicos art 22.4, ambos artículos del RGPD.

XIII. Ciberseguridad

Este es otro de los desafíos importantes a la hora de plantear el uso de la IA en la atención sanitaria, gran parte de las infraestructuras de IdC (infraestructura digital crítica) son vulnerables a las amenazas, los objetivos en el ámbito de la salud pueden ser variados desde herramientas de diagnóstico dispositivos ponibles, píldoras inteligentes inalámbricas hasta dispositivos médicos, pudiendo tener acceso a información sensible sobre la salud de los pacientes o amenazar su salud con diagnósticos erróneos, la necesidad de la ciberseguridad quedó demostrada en el ataque del tipo *Ransomware Wanna Cry*, que dio lugar a la aprobación de la ley sobre ciberseguridad el Reglamento (UE) 2019/881[28], sus objetivos son lograr un alto nivel de confianza en la UE y lograr el buen funcionamiento del mercado interior, art 1.1. También hay avances en esta metería en EEUU con una ley sobre ciberseguridad la *Cibersecurty and Infrastructure Security Act* de 2018 (H.R. 3359)[29], que aumenta la capacidad nacional de los Estados Unidos para defenderse contra los ciberataques. En suma, este objetivo no será fácil ya que será necesario equilibrar los diferentes intereses de todas las partes involucradas.

28. Reglamento relativo a la ciberseguridad, DOUE 151, de 07/06/2019, Ref: DOUE-L-2019-80998

29. Cibersecurty and Infrastructure Security Act de 2018 (H.R. 3359), fue firmada por el presidente Donald Trump el 16/11/2018 mediante la cual se creó una agencia de seguridad de infraestructura y siverseguridad, bajo el departamento de Seguridad Nacional (Resolución AB, 375), se puede consultar en la URL: https://www.congress.gov>house-bill

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

XIV. Conclusiones

A lo largo del presente trabajo hemos planteado un recorrido lógico-científico-estructural del uso de los robots en medicina y sus repercusiones jurídicas, éticas, sociales y económicas a nivel europeo, nacional e internacional, así como los efectos del uso de la IA en la medicina y se han trabajado las consecuencias desde la óptica de la teoría del riesgo y el régimen de responsabilidad, en un intento por llenar las lagunas legales existentes en esta materia tan controvertida y difícil de regular, además hemos tratado las repercusiones de la ciberseguridad como elemento esencial en las infraestructuras digitales clínicas, siendo por lo tanto un objetivo difícil de alcanzar incluso en un futuro próximo.

Igualmente se puede afirmar las consecuencias significativas de las posibilidades terapéuticas y de tratamiento que pueden ofrecer las nuevas tecnologías no sólo a nivel científico-ético, sino también en la calidad de vida de los pacientes, sin embargo cabe señalar, como se ha indicado, la dificultad en su regulación jurídica y control por parte de las Autoridades para evitar sesgos de discriminación en la elaboración de perfiles de los pacientes así como errores en la manipulación de estas tecnologías por parte de los profesionales de la medicina. Y, como última visión, cabe señalar que a pesar de todo el uso responsable de los robots y la IA en la medicina no sólo es un gran avance para la ciencia sino también para toda la humanidad. En el contexto normativo se debe destacar la normativa de la UE, donde en su Reglamento 679/2016,[30] sobre protección de datos de carácter personal establece la imperiosa necesidad de respetar y proteger los derechos a la intimidad, y por supuesto la protección de los datos clínicos de los pacientes ante posibles invasiones por parte de los sesgos y los fallos de la IA, se hace mención al Libro Blanco[31] para una IA fiable que pretende aportar las directrices éticas como enfoque europeo de la fiabilidad y la confianza en la IA ante el rápido desarrollo de ésta, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades, sin embargo esta IA conlleva una serie de riesgos potenciales que deben ser controlados y regulados la discriminación de género, la vulneración de nuestras vidas por la acumulación masiva de datos (Big Data) en el tratamiento de la información de los pacientes, el adecuado tratamiento los datos por las aplicaciones médicas, o la construcción del Bioderecho sobre la base de la dignidad humana como reflejo de la construcción humanista, son algunos de los problemas que se han planteado a lo largo de este trabajo. Como reflejo de la argumentación critica la IA afecta de forma estructural a la autonomía de las personas y a las relaciones entre los individuos produciendo riesgos en esa autonomía relacional neutralizada por medio de estipulaciones normativas.

El uso de los robots sanitarios en el campo de la cirugía ha traído numerosos avances en la medicina pero también conlleva riesgos ya que, ante un defecto de la máquina se podría cometer una negligencia o un delito como consecuencia de ese mal funcionamiento eso nos lleva al régimen de la responsabilidad ya que en el sector sanitario la

30. Reglamento 679/2016 del Palamento y del consejo de 27 de abril de 2016, Op Cit pág 25
31. Libro Blanco Op. Cit. Pág 21

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

implementación de esta tecnología plantea quien debe ser responsable cuando se utiliza este tipo de los robots en la medicina se produce un daño, el fabricante, el programador, o los profesionales sanitarios que manipulan la máquina inteligente dar respuesta a esta pregunta no es tarea fácil, ya que no siempre se encuentra la fuente originadora de ese daño dificultando la delimitación del sujeto que debe soportar la reparación cabe preguntarse y de hecho lo hacemos a lo largo de este artículo si resultaría factible la aplicación de las reglas de la responsabilidad civil, el derecho de consumo, o la responsabilidad por productos defectuosos cuestionándose si sería necesario aprobar una legislación específica en las áreas afectadas por los robots, en este sentido si el daño se produce por defecto en este caso el robot se consideraría un producto sanitario o por la prestación de un servicio sanitario podemos acudir al régimen de responsabilidad establecido en le derecho de consumo regulado en el RD-L 1/2007 de 16 de noviembre(-TRLGDCU)[32] y en caso de negligencia del médico o del hospital acudiremos al régimen de responsabilidad regulado en el Código civil, en Europa encontramos la resolución del Parlamento Europeo 16 de febrero de 2017, destinada a la Comisión sobre normas de Derecho civil sobre Robótica, teniendo en cuenta que en el actual marco normativo vigente no se puede hacer responsable de la acción u omisión al robot de forma directa sino que habrá que atribuir tal responsabilidad al agente humano concreto. Se plantea por ello las deficiencias del marco jurídico vigente en el ámbito de la responsabilidad contractual , en la protección de datos de carácter personal o en la ciberseguridad, ya que la existencia de máquinas concebidas para elegir y tomar decisiones hace inaplicable las normas tradicionales poniendo de relieve la necesidad de adoptar nuevas normas eficientes y actualizadas acordes con los avances tecnológicos y las innovaciones recientes en esta materia, planteándose cuestiones muy controvertidas que cuenta con opiniones a favor pero con detractores, en todo caso el planteamiento está sobre la mesa y tendremos que observar su evolución.

Bibliografía

BECK. U, Risikolgesellshaft Buch, editorial Suhrkamp verlag, 1986.

BOHR A. y MEMARZADEH K. *Inteligencia Artificial en el ámbito de la salud*, Editorial Elservier, Barcelona, 2022, páginas 1- 339.

CÁRCAR BENITO, E.J., "La inteligencia artificial, aplicación jurídica y regulación en los servicios de salud", Revista *Derecho y Salud*, vol 29, nº Extra 1, 2019, págs. 265-277.

EUROPEAN COMMISSION, ETHICS GUIDELINES FOR TRUSTWORTHY (Grupo de expertos de alto nivel en IA), "Ethics guidelines for Trustworthy artificial intelligence", Revista *Ethics and Law,* nº IV, 2019.

32. Real decreto- Ley 1/2007 de 16 de noviembre (TRLGDCU), BOE núm 287 de 30 de noviembre de 2007, Referencia BOE-A-2007-20553, Texto Refundido de la la Ley General de defensa de los Consumidores y Usuarios.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

GARCÍA SAN JOSÉ, D., "Implicaciones Jurídicas y Bioéticas de la Inteligencia Artificial especial consideración del Marco Normativo Internacional", *Cuadernos de Derecho Transnacional*, nº 1, vol 13, 2021, págs 255-276.

GONZÁLEZ RODRÍGUEZ-ARNAIZ, G., *"*Un imperativo tecnológico, una alternativa hacia el humanismo*",* Revista *Cuadernos de Bioética*, nº 1, 2004, págs. 1-22

HANS J.*, Das Prinzip Verantwortung,* Editorial A. M . Suhrkamp, Frankfurt, 1985, págs. 1-426

ROMEO CASABONA, CM. y MORATINOS LAZCOZ, G., "Inteligencia artificial aplicada a la salud ¿Qué marco jurídico?", Revista *de Derecho y Genoma Humano: genética, biotecnología y medicina avanzada*, nº 52, 2020, págs. 139-167.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 129-151
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.09

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

Deontología profesional, la seguridad del paciente y principios esenciales. Conceptos clave para la regulación de la telemedicina, la Inteligencia Artificial y la robótica en el ámbito sanitario[1]

PROFESSIONAL DEONTOLOGY, PATIENT SAFETY AND ESSENTIAL PRINCIPLES. KEY CONCEPTS FOR THE REGULATION OF TELEMEDICINE, ARTIFICIAL INTELLIGENCE AND ROBOTICS IN THE HEALTH FIELD

Manuel Pérez Sarabia
Universidad de Sevilla. Consejo Andaluz de Colegios de Médicos
mperezsarabia@cacm.es 0000-0001-5901-5643

Recibido: 16 de junio de 2023 | Aceptado: 23 de junio de 2023

RESUMEN

En el debate abierto sobre regulación de la telemedicina, la IA y la robótica en el ámbito sanitario, y como estrategia de gobernanza europea prevista en el Libro Blanco sobre inteligencia artificial, así como para garantizar el establecimiento de un marco ético y jurídico apropiado, basado en los valores de la Unión Europea y en consonancia con la carta de Derechos Fundamentales, observamos que la situación de disrupción tecnológica no debe ir unida a una disrupción reguladora, puesto que la normativa vigente da respuesta a muchos aspectos esenciales. Por esta razón, propongo la deontología profesional, la seguridad del paciente y los principios de trasparencia, veracidad y competencia profesional, como conceptos y principios clave para superar con éxito los retos tecnológicos sanitarios a los que nos enfrentamos, y para que las autoridades públicas puedan garantizar que el desarrollo y uso de tecnologías está en consonancia con los derechos humanos.

PALABRAS CLAVE

Inteligencia artificial
Robótica
Deontología
Profesional
Seguridad del paciente
Competencia
Protección de la salud
Sanitario
Medicina

1. El presente artículo se ha realizado en el marco del Proyecto de Investigación: Biomedicina, Inteligencia Artificial, Robótica y Derecho: los Retos del Jurista en la Era Digital. Plan Estatal 2017-2020 Retos - Proyectos I+D+i Referencia: PID2019-108155RB-I00.

ABSTRACT

In the open debate on the regulation of telemedicine, AI and robotics in the health field, and as a European governance strategy envisaged in the White Paper on artificial intelligence, as well as to guarantee the establishment of an appropriate ethical and legal framework, based on In the values of the European Union and in line with the Charter of Fundamental Rights, we observe that the situation of technological disruption should not be linked to regulatory disruption, since current regulations respond to many essential aspects. For this reason, I propose professional deontology, patient safety and the principles of transparency, truthfulness and professional competence as key concepts and principles to successfully overcome the health technology challenges we face, and for public authorities to guarantee that the development and use of technologies is in line with human rights.

KEYWORDS

Artificial intelligence
Robotics
Deontology
Professional
Patient safety
Competition
Health protection
Healthcare
Medicine

1. Introducción

La sociedad actual vive un momento de desarrollo tecnológico disruptivo, la llamada 4ª revolución industrial, que afecta de pleno al ámbito sanitario.

Este desarrollo tecnológico, expansivo y galopante, genera la sensación generalizada de que, para regular este fenómeno, de incesante evolución, hay que renovar el sistema jurídico por completo. Una inquietud generalizada de que los sistemas jurídicos y la regulación vigentes ya no sirven, promoviéndose la creación de nuevos marcos regulatorios específicos.

A modo de ejemplo, la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión Europea sobre normas de Derecho Civil sobre Robótica (Parlamento Europeo, febrero 2017), vino a proponer, que al actual sistema de personalidad jurídica que distingue entre persona física y personas jurídicas, como sujetos de obligaciones y derechos, sería plausible que se incorporara una tercer tipo de personalidad jurídica, la personalidad jurídica electrónica de los robots como nuevos sujetos de derechos y obligaciones, plateado un escenario normativo tan disruptivo como el propio sistema tecnológico. Aunque este debate parece haber sido superado por la doctrina mayoritaria y por las iniciativas reguladoras de la propia Unión Europea, no deja de ser un planteamiento que cuenta con apoyos que incluso postulan crear una nueva rama jurídica (Valente, 2019, págs. 1-30), el derecho de los robots (Belloso Martín, 2018, págs. 21-81).

En respuesta a lo anterior, el Profesor SEOANE nos invita a no dejarnos deslumbrar por el desarrollo tecnológico, pues muchos problemas ya existían y nos son de la IA; por su parte la Profesora WISNER cita a parte de la doctrina que considera que no es necesario regular más, porque ya existe una regulación de derechos humanos en los distintos países; o la Profesora SEPULVEDA nos invita a romper con el concepto disrupción, pues implica una ruptura con el sistema anterior y significaría un retroceso; también reflexionaba el Profesor DE ASIS, sobre la incógnita de nuevos derechos para problemas nuevos

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

o viejos derechos para problemas nuevos, o sobre las soluciones malas para problemas simples (DE ASÍS ROIG, SEOANE, WISNER GLUSKO, SEPULVEDA GÓMEZ, 2021).

Me complacen las anteriores citas, aproximadas a las realizadas en sus conferencias, porque mi propuesta base es coincidente con las mismas, en cuanto considero que la disrupción tecnológica no tiene que ir pareja a una disrupción normativa.

Por todo ello, ante la pregunta ¿nos hace falta una regulación especifica para la telemedicina, la IA y la robótica? La primera respuesta es que en todo caso esa regulación especifica deberá observar la normativa de los estados y específicamente la normativa profesional y sanitaria, como primera conclusión anticipada, y en concreto, en este trabajo perfilamos dos claves o conceptos normativos que consideramos esenciales, la deontología profesional y la seguridad del paciente, que junto con los principios esenciales de trasparencia, veracidad y competencia profesional, deberán ser punto de partida para cualquier puesta en funcionamiento o regulación de sistemas tecnológicos que tratamos.

Como punto de partida debemos comprender que la técnica y el desarrollo tecnológico no son nada nuevo en la historia de la humanidad.

II. La técnica

La técnica y la tecnología no son nada nuevo, si bien su velocidad de desarrollo se ha multiplicado y la aparición de una nueva capacidad de autoaprendizaje en los desarrollos tecnológicos sobre inteligencia artificial, resulta desconcertante, aunque seguro que en cada etapa de la historia fueron igualmente desconcertantes los procesos capaces alterar los sistemas de desarrollo humano.

Ya lo dijo Ortega y Gasset, "*sin la técnica el hombre no existiría ni habría existido nunca*" (Ortega y Gasset, 2000, p.13) , al inicio del libro meditaciones de la técnica que surge en la inauguración de la Universidad de verano de Santander en el año 1933.

También , hace pocos días tuve la fortuna de escuchar al Profesor Fernando Llano en una magistral ponencia sobre el marco regulador de la medicina genética y la dignidad humana (Llano Alonso, 2021), donde hacía un breve recorrido por las distintas revoluciones industriales, describiéndonos, para ilustrar su ponencia, aquella famosa película de Chaplin en la que el director y actor era absorbido cómicamente por una maquinaria, que evidenciaba como el hombre podía ser absorbido por la tecnología.

En aquel instante, mi mente, además entender que podíamos ser absorbidos por el deslumbramiento que produce el desarrollo tecnológico hasta extremos cómicos o dramáticos, sintió como también podríamos ser absorbidos por un afán regulatorio que nos hiciera retroceder y olvidar los hitos logrados, por lo que retrocedí a miles de años atrás, cuando el primer ser humano descubrió el fuego, y pensé en aquella situación como tragicómica también, en cuanto la cantidad de veces que nuestros antepasados se quemarían y dañarían hasta lograr perfeccionar la técnica y tecnología del momento, entendiendo la técnica como el conjunto de habilidades adquiridas, por la práctica, y la tecnología, como aplicación instrumental de esas habilidades.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

Con esta reflexión, quiero llegar a una segunda conclusión adelantada: Los instrumentos y herramientas que han revolucionado, transformado y evolucionado el desarrollo del hombre, siempre han partido desde puntos de partida muy anteriores, no *ex novo,* puesto que han sido la adaptación de los elementos e instrumentos para el hombre, y no la adaptación del hombre a estos instrumentos.

Llego aquí, partiendo del pensamiento de ORTEGA, cuando afirma acertado como siempre, que, *"la técnica es lo contrario a la adaptación del sujeto al medio, puesto que es la adaptación del medio al sujeto"* (Diéguez Lucena, 2013, págs.73-97).

Pero en los momentos que vivimos, en ocasiones, parece que se propone una adaptación, al contrario, la del hombre a la tecnología, en lugar de la adaptación de la tecnología al hombre; y esto sí que constituiría un cambio de paradigma en la historia de la humanidad, o al menos en la historia contemporánea de occidente, desde la proclamación de los Derechos Humanos. Me refiero a una situación futurible, en la que los seres humanos, por ejemplo, nos tendríamos que adaptar obligadamente a recibir asistencia médica por un robot o sistema de IA autónomos, a distancia o presencial, el lugar de recibirla de un ser humano como nosotros, pues como señala el Profesor SEOANE, estamos perfilados; avocados a ser objetos de decisiones automatizadas, lo que quiebra nuestra seguridad jurídica (De Asís Roig, Seoane, 2021). El origen del problema no es la tecnología, sino el uso que hagamos de ella, o el uso que la regulación permita que se haga con ella.

Por ello, debemos resituarnos y ver que, si bien el desarrollo tecnológico al que nos enfrentamos, o disfrutamos, se caracteriza por desarrollar unas capacidades tecnológicas asimilables o incluso superiores a las naturales humanas, la técnica y la tecnología siempre ha existido desde que existe el hombre, y en la actualidad para su regulación debemos partir del ordenamiento vigente, sin necesidad de romper con él, pues especialmente en Europa y en España en concreto, es un ordenamiento garantista de los Derechos Humanos y más en el ámbito de la protección de la salud, la integridad y la vida, existiendo soluciones normativas idóneas para la mayoría de los problemas que se pueden plantear, existiendo ya garantías para un uso respetuoso con los derechos humanos, debiendo constituirse una regulación reducida, conducida a los aspectos más controvertidos de estas nuevas tecnologías:

- La opacidad y necesidad de transparencia de los algoritmos que constituyen estos sistemas.
- Las garantías de seguridad en su uso, como instrumentos o herramientas de especial peligrosidad. Una peligrosidad intrínseca, debido a su complejidad y capacidad de resolución que pueda afectar a bienes e intereses jurídicos protegidos.

En sentido con lo anterior, es conveniente visualizar las previsiones reguladoras de la Unión Europea y a continuación la regulación particular en España en el ámbito sanitario, para poder comprobar que efectivamente existe una regulación normalizada que debe de asumirse para no romper con el sistema de garantías y derechos del que

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

disfrutamos actualmente, y que posteriormente se debe complementar con la regulación o exigencias necesarias para garantizar el respeto a los derechos humanos en los aspectos controvertidos señalados.

III. Previsiones reguladoras en la UE

La extensión de este trabajo no nos permite ser demasiado exhaustivos en la descripción de la regulación y previsiones para el derecho a la protección de la salud y el desarrollo de las nuevas tecnologías, pero sí daré unas pinceladas sobre aspectos de gran relevancia.

En el ámbito de la inteligencia artificial y sus desarrollos debemos partir del derecho a la protección de datos, pues el punto de partida de todos estos sistemas parte del llamado *Big Data*, del uso masivo de datos correlacionados entre sí por esos desarrollos tecnológicos.

Esta es la razón, por la que para cualquier análisis de la materia estudiada debemos tener como muy relevante punto de referencia el Reglamento Europeo de Protección de Datos (Reglamento (UE), 2016) que establece en su artículo 9 los datos de salud como una categoría especial de datos, con un sistema de protección alta y reforzado, lo que hay que tomar en consideración de base, pues como señala PALMA ORTIGOSA (Palma, 2019) o TRONCOSO REIGADA (Troncoso Reigada, 2010, págs. 74 y 75), entre otros autores, la aplicación del derecho fundamental a la protección de datos tiene una repercusión en unos términos más amplios que la intimidad, sino también instrumental para el resto de los derechos fundamentales, y en nuestro caso como garantía para el derecho fundamental a la protección de la salud, la integridad y la vida, en cuanto al derecho, por ejemplo, de la prohibición de la toma de decisiones automatizadas sin revisión humana, o evidentemente, la exigencia normativa de especial protección de los datos de salud que hemos señalado anteriormente.

Por su parte, el Libro en Blanco sobre la inteligencia artificial (Comisión Europea, 2020), publicado por la Comisión Europea, hace referencia a la necesidad de supervisión humana, en relación con el artículo 22 del Reglamento Europeo de Protección de Datos, cuando exista una aplicación de inteligencia artificial con riesgo elevado de socavar la autonomía humana o provoque otros efectos adversos, lo que desde luego interpretamos cómo directamente aplicable a los derechos relacionados con la protección de la salud la integridad y la vida, pues qué característica más profunda de la autonomía humana que los derechos relacionados con la salud. Así mismo, la referencia que hace este artículo del 22 del mencionado Reglamento, a los efectos adversos, no podemos dejar de reflejarla y relacionarla con el capítulo que más adelante desarrollamos en referencia a la seguridad del paciente, sustentada sustancialmente sobre los llamados eventos adversos, que son incidentes sanitarios con daños para el paciente.

En relación con lo anterior, el libro en blanco destaca que tanto desarrolladores como implementadores de inteligencia artificial están sometidos a la legislación europea, al igual que cualquier otro ámbito de desarrollo tecnológico, industrial o comercial, se-

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

ñalando derechos fundamentales como la protección de consumidores, o la seguridad de productos y responsabilidad civil, lo que es una referencia congruente con la realidad que planteamos, en cuanto a la preexistencia un marco regulador idóneo en la actualidad.

Prosigue el Libro Blanco, indicando que debido a las características específicas de estas nuevas tecnologías, concretamente su opacidad, habrá que modificar las normativas, en la búsqueda de soluciones factibles, describiendo los principales riesgos relacionados con aspectos principalmente económicos y sobre privacidad e intimidad, sin reparar expresamente en los riesgos para el derecho a la protección de la salud y la integridad de las personas, lo cual consideramos que lo sobreentiende como evidente en su posterior referencia a la exigencia que tiene la IA de respetar los derechos y valores fundamentales. Aunque sí afirma, que el objetivo de una IA fiable, ética y antropocéntrica solo puede alcanzarse garantizando una participación adecuada de las personas con relación a las aplicaciones de IA de riesgo elevado, lo cual se trata de referencias de cierta ambigüedad, pero sobre las que no cabe otra interpretación respecto a los derechos tratados, que la señalada instrumentalidad del derecho a la protección de datos (Palma, 2019) (Troncoso Reigada, 2010, págs. 74 y 75) en relación con la restante normativa señalada en este trabajo, viniendo a determinar que en el ámbito de la salud, la adecuada participación profesional sanitaria constituye el núcleo de reserva de humanidad, participación indispensable por parte de médicos y otros sanitarios, como veremos en el capítulo sobre deontología profesional.

Por su parte, la Comunicación de IA para Europa (Comisión Europea, 2018) establece el derecho de las personas a saber si se están comunicando con una máquina o con otro ser humano, así como la necesidad de que la persona pueda ponerse en contacto con un ser humano, y garantizar que estos siempre puedan verificar o corregir las decisiones.

Asimismo, la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión para normas de Derecho civil sobre robótica (Parlamento Europeo, 2017), incide en la necesidad de integrar salvaguardas, control y verificación de las personas en los procesos de toma de decisiones automatizadas y basadas en algoritmos, incidiendo en el riesgo de deshumanización, subrayando la necesidad de no invadir el ámbito de decisión del médico, y la importancia de que no se disminuya ni perjudique la relación entre médico y paciente, lo que hay ponerlo en relación con la iniciativa del Consejo General de Colegios Oficiales de Médicos de España, que ha solicitado a la UNESCO, junto con otras organizaciones médicas internacionales, que declare la Relación Médico Paciente como Patrimonio Cultural Inmaterial de la Humanidad (Foro Profesión Médica en España, 2017).

Por su parte, el Parlamento Europeo en la incitativa legislativa aprobada el 21 de octubre de 2020[2], indica que la IA tiene que ser antropocéntrica y antropogénica, cumplir condiciones de seguridad, transparencia, rendición de cuentas, salvaguardas contra el

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

2. https://www.europarl.europa.eu/news/es/press-room/20201016IPR89544/el-parlamento-muestra-el-camino-para-la-normativa-sobre-inteligencia-artificial

sesgo y discriminación, contemplar el derecho de reparación, la responsabilidad social y medioambiental, el respeto de la intimidad y protección de datos.

En continuidad con la anterior iniciativa, el pasado 21 de abril de 2021, se presentó por la Comisión Europea la 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[3], que hace referencia a los resultados positivos y ventajas competitivas que la inteligencia artificial puede tener en sectores de gran impacto como la salud, la cual sitúa en el ámbito de un alto riesgo junto con la seguridad y los derechos fundamentales de las personas, estableciendo determinadas exigencias sobre gestión de riesgos y vigilancia humana, así cómo trazabilidad y transparencia garantizadas, priorizando la salud junto la seguridad y la protección de consumidores, así como también prevé otros derechos como el derecho a la libertad de empresa, exigiendo igualmente que estos sistemas tengan una evaluación de conformidad *ex ante*.

Por su parte, la Consideración 27 de la anterior Propuesta de Reglamento, merece la pena reflexionarla, en cuanto establece que la calificación de alto riesgo debe limitarse a aquellos sistemas de inteligencia artificial que tengan consecuencias perjudiciales importantes para la salud. La redacción literal del precepto introduce dos condiciones que pueden inducir al equivoco, en cuanto restringe la calificación de alto riesgo para cuando haya consecuencias perjudiciales e importantes. Estos conceptos jurídicos indeterminados, perjudiciales e importantes, manifiestan, salvo error de interpretación por el exponente, una clara intención de desarrollar una interpretación laxa, solo limitada por riesgos extremos, lo cual podría ser contradictorio con el marco garantista de derechos y valores de la propia Unión Europea.

En sentido muy parejo, la regulación específica sobre robótica, en concreto la Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre política industrial global europea en materia de inteligencia artificial y robótica (Parlamento Europeo, 2019), vuelve a reivindicar la necesidad de convertir a Europa en un continente emergente gracias al desarrollo de las nuevas tecnologías, incidiendo en el ámbito de la salud y los sistemas sanitarios.

Como crítica, principalmente a la Propuesta Reglamento de inteligencia artificial, significar que la Comisión Europea ha desarrollado un texto repetitivo y excesivamente amplio, que desvela cierta ambigüedad rehuyendo de la practicidad, posiblemente de manera consciente, redundando en aspectos como la compensación de daños, en lugar de reducir y sistematizar la regulación los aspectos verdaderamente controvertidos y no regulados por el momento, como son la transparencia, la trazabilidad, la exigencia de controles de calidad y seguridad por la autoridad pública, o la definición clara de la IA como instrumento. Es claro, desde mi punto de vista, que los órganos de Gobierno

3. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión. COM /2021/ 206 final. Bruselas, 21.4.2021. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

de la Unión Europea quieren lanzar un liderazgo mundial sobre inteligencia artificial y para ello reducir al máximo sus límites, viéndose también obligados a equilibrar con los Derechos Humanos y fundamentales, saliendo perdedora la transparencia y claridad normativa, por tanto, la seguridad jurídica, en esta búsqueda de equilibrio. De hecho, la Consideración 45 abre claramente el tráfico de datos de salud como fórmula potenciadora del desarrollo de sistemas de inteligencia artificial, lo que es principal prueba y señal del fin último de la propuesta reguladora.

Merecen mención, por su actualidad e influencia internacional, las Recomendaciones sobre ética de la inteligencia artificial publicadas por la UNESCO (Unesco, 2022), donde entre numerosos aspectos de interés se pone de relieve la importancia de las relaciones de los pacientes con su familia y con el personal sanitario (Recomendación 121), en línea con la importancia de potenciar la relación médico paciente como elemento clave para la dignidad humana, como bastión de humanidad (Foro Profesión Médica en España, 2017, p. 39).

Por su parte, la Organización Mundial de la Salud (OMS), en su Estrategia mundial sobre salud digital 2020-2025[4], promueve una salud digital ética, segura, fiable, equitativa Y trasparente, entre otras cuestiones.

Todas estas cuestiones vienen a ratificarnos que el marco normativo que se prevé, independientemente del fin último, no puede obviar principios y derechos básicos como la transparencia algorítmica o la reserva de humanidad. Por este motivo, cuestiones, como la propuesta de conferir personalidad a un robot, se han ido diluyendo, pues sería deshumanizar la humanidad, insolidario entre los hombres iguales, y arriesgar los Derechos Humanos, confiriéndole poderes humanos a las maquinas.

Por todo ello, partiendo de la base de que la normativa que se desarrolle debe respetar siempre los ordenamientos y derechos vigentes que vamos señalando, sí debemos anunciar como ya hemos venido insinuando, que la normativa en esta materia debe de centrarse en cuestiones como la opacidad, la transparencia, la explicabilidad, la fundamentación, y la responsabilidad sobre estas herramientas e instrumentos, que debe conllevar un sistema de matriculación o licencia con sus correspondientes revisiones periódicas o inspecciones técnicas, ajustadas a la ficha técnica del producto, también sistemas de certificación de calidad y seguridad, así como el correspondiente seguro de responsabilidad.

El concepto de riesgo es una idea clave para la Unión Europea a la hora de elaborar medidas y normas, riesgos centrados, como hemos expuesto, en cuestiones como la opacidad y la transparencia en las decisiones automatizadas, donde es necesario regular una exigencia de argumentación y fundamentación junto con la reserva de humanidad

Nos preguntamos, qué si bien para un médico es imperativo legal proporcionar información transparente al paciente, o para un juez es obligado motivar sus resoluciones, por qué para un tecnólogo no es una exigencia la transparencia en sus códigos fuentes y de los sistemas de elaboración de algoritmos. Quizás esta exigencia sí sea necesaria

4. Estrategia mundial sobre salud digital 2020-2025. https://apps.who.int/iris/bitstream/handle/10665/344251/9789240027572-spa.pdf?sequence=1&isAllowed=y

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

regularla expresamente, como ya se ha regulado los derechos de información médica o la obligación de motivación judicial, en aras de proteger los derechos e intereses públicos en juego, que no son baladíes.

IV. Regulación desde la perspectiva del ámbito sanitario

Como hemos señalado en la introducción, ni existe la necesidad de un sistema jurídico diferenciado, ni debemos romper en ningún caso con el sistema jurídico que tenemos, tanto en cuanto a la industria y desarrollo tecnológico, como respecto a los sistemas sanitarios en su sentido más amplio. Tenemos un modelo sanitario seguro, con garantías de atención universal, igualdad, seguridad y calidad.

Ley 14/1986 General de Sanidad, de 25 de abril[5], recoge necesidades como el respeto a la personalidad, la dignidad humana y la intimidad, el derecho de los pacientes a que se les asigne un médico y a elegirlo. Un médico persona física, desde luego, cuyo nombre se le dará a conocer al paciente, como parte de sus derechos fundamentales, como puede ser el derecho fundamental a un Juez predeterminado por Ley.

Ley 44/2003 de Ordenación de la Profesiones Sanitarias[6], establece que los profesionales sanitarios actuaran con autonomía técnica y científica, con la limitación de la Ley y la deontológica, debiendo quedar identificados los profesionales y garantizándose la continuidad asistencial.

Ley 41/2002 Reguladora Autonomía del Paciente[7], recoge derechos que han sido constituidos como fundamentales por el Tribunal Constitucional, como el derecho a la información del paciente, el consentimiento informado, u otros derechos que podríamos llamar complementarios a los anteriores, como el derecho a un historial clínico o la figura del médico responsable. Respecto a esta norma, quiero poner de relieve la trascendencia que tiene en relación por la aplicación de sistemas tecnológicos al ámbito de la salud, en cuanto a la garantía que supone el derecho a la información para el debido ejercicio de la autonomía de la voluntad en el momento de decidir sobre nuestra propia salud y/o un tratamiento médico. En este sentido el Tribunal Europeo de Derechos Humanos, en sentencia de 29 de abril de 2002, dictaminó que *"la imposición de un tratamiento sin el consentimiento del paciente supondría un ataque a la integridad física"* (Fernández Coronado, 2014, p.164). Esta doctrina, en línea con la seguida por el Tribunal Constitucional (Sentencia Tribunal Constitucional, 37/2011), en la que se reconoce el derecho a un consentimiento debidamente informado, como parte integrante del derecho fundamental a la integridad física, ex artículo 15 CE, adquiere una especial

5. Ley 14/1986 General de Sanidad, de 25 de abril https://www.boe.es/buscar/act.php?id=-BOE-A-1986-10499

6. Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias. https://www.boe.es/buscar/pdf/2003/BOE-A-2003-21340-consolidado.pdf

7. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

relevancia en cuanto al derecho de los pacientes de ser informados transparentemente de todas las cuestiones que afecten a su salud, incluso los medios tecnológicos utilizados, más aún cuando se trata de sistemas tan complejos como la inteligencia artificial o la robótica, aumentando aún más la complejidad si estos medios u otros se llevan a cabo desde la distancia.

La normativa enunciada es solo una muestra relevante, a la que habría que unir, además del resto de normativa estatal, la normativa autonómica especifica, y por supuesto normativa específica de protección de datos, como ya hemos señalado, y por supuesto normativa europea de aplicación directa, como pueden ser las directivas de cualificaciones porfesionales, de productos sanitarios o de medicina transfronteriza.

Pero sí me gustaría detenerme en la regulación profesional, concretamente en los informes emitidos por la Asociación Médica Mundial y el Comité Permanente de Médicos Europeos, destacando entre ellos el emitido en la 69 Asamblea Mundial (Rekiavik-2018), que reivindicaba que la telemedicina es un acto médico como otro cualquiera; debiendo respetarse las exigencias propias de cada acto y de la normativa del país del paciente (Asociación Médica Mundial, 2018). También la Comisión Central de Deontología y Derecho Médico del Consejo General de Colegios Oficiales de Médicos en un documento titulado "E-consulta. La Telemedicina en el acto médico", el 10 de junio 2020 (Comisión Central de Deontología Médica, 2020), señalaba entre otros aspectos que *"la asistencia médica ofrecida mediante las nuevas tecnologías o sistemas de comunicación se concibe como un verdadero acto médico que completa la atención presencial del médico.";* Asimismo, "*en determinadas circunstancias, como la actual pandemia de COVID-19, la e-consulta puede sustituir y otras veces completar el acto médico presencial porque este no sea posible, aconsejable o porque la ponderación del beneficio/riesgo para el paciente así lo sugiera. En cualquier caso, en situación de normalidad, la opción de usar la e consulta deberá ser consensuada con el paciente.*"

La razón de destacar, estas declaraciones de la profesión médica, es dejar muestra palpable de que nuestra sociedad, debido a la situación extrema producida por la pandemia de COVID-19, ha avanzado y se ha adaptado a pasos agigantados en la aplicación tecnológica, se ha regulado y adaptado también normativamente, aunque haya sido por la vía de la autorregulación de las profesiones garantes de Derechos Humanos, como es la medicina, sin renunciar a las bases y principios esenciales que garantizan los intereses que protegen, pudiendo resultar ejemplarizante para el desarrollo regulador que se prevé, que como venimos diciendo debe de partir de las bases y principios que actualmente son garantía para los ciudadanos, y en el ámbito sanitario, para los pacientes.

Entre las cuestiones esenciales para las garantías de los pacientes que tenemos reguladas, y que en su caso la regulación futura deberá garantizar con mayor énfasis, se encuentran cuestiones cómo la transparencia, en la que ya hemos insistido, con exigencias como la identificación recíproca de personas físicas intervinientes, para evitar actos de intrusismo, suplantación de identidad, garantizando de esta manera la relación médico paciente, previa comprobación de la habilitación profesional; también el derecho a la intimidad, el derecho a la información y autonomía del paciente, o el seguro de responsabilidad civil, entre otros.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

Por estos motivos, proponemos como punto de partida, que para cualquier proyección legislativa en la UE sobre el ámbito sanitario, se debe partir desde la regulación existente sobre deontología profesional, sobre los criterios de la seguridad del paciente y sobre los principios esenciales de trasparencia, veracidad y de competencia profesional; como claves para la regulación del desarrollo tecnológico en este ámbito, que se enfoque desde las garantías que sirven en el momento actual para que la humanidad se pueda beneficiar de las ventajas que brinda la IA, la robótica, y la medicina a distancia, como pueden ser la accesibilidad, la mejor adherencia a tratamientos, mejor intercomunicación profesional médico-médico, médico-farmacéutico, farmacéutico y médico paciente, o el control de riesgos con los farmacológicos, entre otras muchas aplicaciones.

V. Deontología profesional, seguridad del paciente y principios esenciales

Consideramos que en el debate abierto sobre regulación de la telemedicina, la IA y la robótica en el ámbito sanitario, y como estrategia de gobernanza europea prevista en el Libro Blanco sobre inteligencia artificial, así como para garantizar el establecimiento de un marco ético y jurídico apropiado, basado en los valores de la Unión Europea y en consonancia con la carta de Derechos Fundamentales de la propia Unión, de la manera establecida en la Comunicación de la Comisión al Parlamento Europeo sobre inteligencia artificial (Comisión Europea, 2018), es fundamental partir de estos conceptos claves para superar con éxito los retos tecnológicos sanitarios a los que nos enfrentamos, y para que las autoridades públicas puedan garantizar que el desarrollo y uso de tecnologías de inteligencia artificial está en consonancia con los derechos y valores enunciados.

5.1. La deontología profesional médica

La deontología profesional sanitaria se constituye como el deber y obligación ética y conductual, a la que se encuentran sujetos los profesionales sanitarios, suponiendo una relación de sujeción especial**,** a diferencia de la sujeción general de los restos de los ciudadanos respecto a las administraciones, esta sujeción especial es definida por García de Enterría y Fernández (García de Enterría, 2001, p.107) como una relación en la que existe una dependencia mayor por parte de los sujetos vinculados.

La ordenación profesional, cuya regulación y vigilancia compete a las corporaciones de derecho público, es la principal garantía para la protección de los intereses públicos, que en el ámbito sanitario son los derechos a la protección de la salud, a la integridad y la vida, que justifican el por qué de esta relación de especial sujeción, de esta especial dependencia deontológica de los sanitarios. El motivo de esta garantía es que la independencia profesional, amparada por el carácter público e independiente también de las corporaciones de derecho público, aseguran que los profesionales sanitarios puedan anteponer los derechos fundamentales e interese públicos que les competen, los derechos a la protección la salud, la integridad y la vida de los pacientes, por encima de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

los vaivenes propios de los intereses políticos, ideológicos, económicos, o de cualquier otra índole que puedan existir.

En el ámbito de la telemedicina, la inteligencia artificial y la robótica, estas garantías adquieren una especial relevancia, en cuanto a que al enfoque de esa función de autorregulación no es solo directa, respecto a lo que es el acto médico en concreto, sino que adquiere una función pública institucional, velando, al igual que ya lo hace para que no haya intrusismo profesional, porque las realidades tecnológicas sean instrumentos al servicio de los derechos de los pacientes, en lugar de medios autónomos, con funciones finalistas, ajenos a las garantías de nuestro sistema jurídico, donde es esencial la sujeción deontológica de los profesionales.

La ley 2/1974 sobre Colegios Profesionales[8], Con sus correspondientes modificaciones, entre ellas las más importantes introducidas mediante la conocida como ley ómnibus, la Ley 25/2009, de 22 de diciembre, para la adaptación a la Ley 17/2009 sobre el libre acceso de actividades y servicios, en relación con el bloque de la constitucionalidad, en cuanto competencias profesionales, y con el artículo 36 de la Constitución española, establece como fin esencial de las corporaciones de derecho público:

- La ordenación del ejercicio de las profesiones.
- La defensa de los intereses profesionales de los colegiados y la protección de los intereses de consumidores y usuarios de los servicios de los colegiados, en nuestro caso de los servicios médicos, o de otros profesionales sanitarios.

La razón de ser de los colegios profesionales, como corporaciones de derecho público, se justifica en la defensa del interés público que es la protección de la salud de los pacientes, confiriéndoles la Ley de Consumidores y Usuarios[9] la defensa de los usuarios de servicios prestados por médicos colegiados, por autoexclusión prevista en su artículo 93, así como la garantía de calidad de los servicios profesionales, estando entre sus deberes el control deontológico y la vigilancia frente al intrusismo profesional; y así lo ha venido estableciendo la reciente jurisprudencia, entre otras, la Sentencia del Tribunal Supremo 1216/2018, de 16 de julio[10], y en Sentencia del Tribunal Constitucional 3/2013, de 17 de enero[11].

Por su parte, la referida doctrina, consolidada, del Tribunal Constitucional, en numerosas sentencias, entre ellas la 3/2013, de 17 de enero, que ratificaba la obligatoriedad de la colegiación en Andalucía, fundamentaba:

8. Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales. https://www.boe.es/buscar/act.php?id=BOE-A-1974-289

9. Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555

10. Sentencia del Tribunal Supremo 2791/2018, de 16 de julio de 2018. http://www.poderjudicial.es/search/AN/openCDocument/47c54a4d73e1a1965a444dd3e915a50c327144d5ce39e908

11. Sentencia del Tribunal Constitucional 3/2013, de 17 de enero 2013. http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/23233

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

- Que la institución colegial está basada en encomienda de funciones públicas.
- Que esas funciones son los fines de ordenación del ejercicio de la profesión, reiterando la protección de los intereses de consumidores y usuarios.
- Todo ello sobre el sustento de la deontología y ética profesional, así como el control de las desviaciones en la práctica.
- Actuado con competencias propias, que son de manera exclusiva de los colegios profesionales, sustentada en el control de la buena práctica médica y de los requisitos habilitantes para el ejercicio profesional.
- Destaca la importancia de la función pública de ordenación deontológica y la reglamentación general de cualquiera de las formas de ejercicio profesional.
- Todo ello de manera indubitada, cuando se trata de materias de especial interés público y general que afecten de manera grave y directa a derechos fundamentales e intereses públicos especialmente protegidos, como son los derechos a la protección de la salud, la integridad física y la vida de las personas.

Asimismo, el TC establece una condición impuesta, una exigencia constitucional, que la colegiación tiene que demostrar ser un instrumento eficiente de control del ejercicio profesional para la mejor defensa de los destinatarios de los servicios. Se tiene que llevar a cabo, por tanto, una verdadera protección de los intereses generales y una actuación adecuada para la consecución de fines públicos y tutela del interés público protegido, la protección de la salud en relación con el derecho fundamental a la integridad y la vida.

No solo el Tribunal Constitucional se ha pronunciado sobre esta materia, sino que también nuestro Tribunal Supremo en reciente Sentencia 1216/2018, de 16 de julio[12], que conecta nuevamente con las garantías de colegiación obligatoria y los derechos de los pacientes, fundamentando su necesidad para las siguientes acciones:

- La evitación del intrusismo y de actos ilegales.
- Garantía de la colegiación para los derechos de los pacientes.
- Ser una herramienta eficaz para la calidad de la prestación médica y la responsabilidad profesional.

En este caso, el TS determina la legalidad de la colegiación de oficio, como una potestad administrativa de los colegios para que puedan garantizar la atención de calidad de los pacientes, validando una reglamentación mediante la que el colegio profesional podría colegiar, incluso contra su propia voluntad, a aquellos profesionales que cumpliendo con los requisitos de titulación se encontraran ejerciendo la profesión sin cumplir con el requisito habilitante de la colegiación, con el objeto de que los colegios pudieran controlar un ejercicio profesional conforme a derecho, en aras de garantizar los intereses públicos protegidos.

12. STS, *ídem*.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

Asimismo, el Tribunal Supremo, en Sentencia de 11 de noviembre de 1992, e igualmente el Tribunal Constitucional en Sentencia de 8 de marzo de 1996, ya venían avalando la tutela del interés público de los colegios profesionales, disponiendo que: *"dicha potestad disciplinaria debe entenderse de modo amplio, de manera que suponga un robustecimiento de los poderes públicos del Colegio profesional"*.

Por su parte, a nivel internacional, las organizaciones médicas internacionales como la **Asociación Médica Mundial** nacida como respuesta a los crímenes de la 2ª Guerra Mundial (Asociación Médica Mundial, 2021), o la Unión de Médicos Especialistas Europeos, determinan una unidad supranacional de principios y valores para los derechos de los pacientes.

La deontología profesional va en línea con el espíritu de la regulación internacional más actual, en el sentido reivindicado por gran parte de la doctrina y los documentos que hemos venido analizando, que viene poniendo de manifiesto que inteligencia artificial y la robótica evidencian una especial necesidad asumir los valores de la ética y de la deontología profesional, más en el ámbito sanitario donde nuestro ordenamiento y la jurisprudencia establecen la garantía de la deontología para los derechos a la protección de la salud, la integridad y la vida de los pacientes.

5.2. Seguridad del paciente

La segunda clave, la seguridad del paciente, es recogida por la Estrategia Mundial sobre Salud Digital 2020-2025[13], como una dimensión más de la salud digital, junto a la promoción de la salud, la ética, la interoperabilidad, entre otros aspectos.

Asimismo, la Propuesta de Reglamento de IA, en su Consideración 28[14], recoge que los sistemas de inteligencia artificial pueden tener efectos adversos para la salud, especificando que en el sector sanitario los riesgos para la salud y la vida son especialmente elevados, por lo que los sistemas de diagnóstico y de apoyo a las decisiones humanas, cuya sofisticación es cada vez mayor, dice el texto que deben de ser fiables y precisos. Aunque el texto identifique "efectos" en lugar de "eventos", sí podemos decir o interpretar que existe una remisión práctica a la seguridad del paciente.

En este contexto, de desarrollo tecnológico, entra en escena la seguridad del paciente, que es un concepto jurídico y al tiempo un concepto sanitario, que se está desarrollando doctrinalmente, principalmente en el segundo ámbito, el sanitario, y en el que se trata de establecer sistemas de prevención de los llamados eventos adversos, que son incidentes sanitarios con daños para los pacientes.

La seguridad del paciente, como hemos indicado, podemos considerarla como un concepto con un doble sentido de análisis, el **sentido puramente sanitario** y **el sentido como concepto jurídico**, estando ambos íntimamente relacionados, pero con perspectivas de desarrollo teórico y práctico diferenciada y única al tiempo.

13. Estrategia Mundial sobre la Salud, *loc. cit.*
14. Propuesta de Reglamento de IA, *op. cit.*

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

En origen y principal área de desarrollo surge como objetivo de las ciencias de la salud, pero contiene un eminente sentido jurídico, pues tanto su desarrollo como implementación conllevan diversos aspectos con repercusión legal, tanto en el ámbito de la ordenación administrativa**,** en cuanto prevé una regulación sanitaria orientada a la prevención de daños, como en el ámbito de la seguridad jurídica, y también en el ámbito de las responsabilidades, tanto profesionales como patrimoniales.

En un sentido puramente sanitario se constituye como un objetivo o estrategia sanitaria, orientado a conocer los riesgos de eventos adversos con el fin de implantar medidas de prevención para evitarlos.

En un sentido o en otro, la seguridad del paciente es un elemento de garantías y seguridad sanitaria y jurídica para los pacientes, pero también para los profesionales.

El Ministerio de Sanidad ha publicado informe con recomendaciones para el análisis de incidentes de seguridad del paciente con daños (Ministerio de Sanidad, 2021), donde nos señala el marco de creciente de complejidad sanitaria con elevado uso de tecnología. También menciona la obligación deontológica de informar al paciente, que antes hemos remarcado como parte intrínseca del derecho a la protección de la salud y la integridad, según doctrina del TC[15].

Por su parte, la ley 16/2003 de Cohesión y Calidad del Sistema Nacional de Salud[16], establece en su art. 59 el registro de acontecimiento adversos, que recogerá información sobre practicas que sean potenciales problemas para la seguridad del paciente.

Llegados a este punto, podemos considerar los derechos de información al paciente como parte del contenido esencial de los derechos a la protección de la salud y del derecho a la integridad y como exigencia deontológica necesaria para la seguridad del paciente. Información en el sentido más amplio, en todo lo que pueda afectar a los derechos del paciente y donde desde luego está la información sobre el uso de las tecnologías. Incluso, podríamos llevar este derecho al ámbito de la salud pública, y el derecho a ser informados con veracidad por los agentes responsables en cada caso, de todo aquello que pueda afectar a su derecho a la protección de la salud, como se ha puesto de manifiesto en las últimas crisis sanitarias vividas, como la pandemia del covid 19, la llamada fiebre del nilo, la listeriosis, o la viruela del mono.

Es reseñable significar que países como Dinamarca o Italia ya han promulgado leyes especificas sobre seguridad del paciente (Ministerio de sanidad, 2021, p.37), lo que unido al desarrollo estratégico que existe en las diferentes Comunidades Autónomas (Ministerio de Sanidad, 2021, págs. 30-51), nos lleva observar que cualquier desarrollo tecnológico en este ámbito sanitario tiene que prever las premisas y garantías establecidas por las estrategias de seguridad del paciente, así como también definir e introducir los riegos de estos desarrollos tecnológicos en las estrategias de seguridad del paciente.

15. Sentencia del Tribunal Constitucional 37/2011, *loc. cit*.
16. Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. https://www.boe.es/buscar/act.php?id=BOE-A-2003-10715

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

5.3. Principios esenciales: trasparencia, veracidad y de competencia profesional

En relación con las claves reguladoras motivadas anteriormente, desde las que se debe de partir para regular y aplicar en todo caso los nuevos instrumentos tecnológicos, considero que existen tres principios fundamentales para enfocar normativamente de manera correcta los retos a los que nos enfrentamos, estos son los principios de transparencia, de veracidad y de competencia profesional.

5.3.1. Principio de trasparencia

El principio de transparencia, en relación con la deontología y la seguridad del paciente, parte de principios irrenunciables cómo son la perfecta identificación del profesional, la adecuada elaboración de un historial clínico, o la adecuada información al paciente y consentimiento informado para que pueda decidir en ejercicio de su autonomía de la voluntad.

Todas estas cuestiones son directamente aplicables a la práctica medica con instrumentos tecnológicos, por lo que cualquier instrumento cuya resolución pueda tener una repercusión en los derechos a la protección de la salud, la integridad o la vida debe partir de una información veraz, completa y trasparente, tanto en el plano estrictamente sanitario, como en el plano tecnológico, para que la decisión sea debidamente informada y con todas las garantías.

En este punto, debemos referir el cada vez más nombrado termino posverdad, que se considera un neologismo, más utilizado desde que los partidarios de la salida del Reino Unido de la Comunidad Europea se valieran de mensajes que distorsionaban la realidad, para influir en las votaciones del referéndum, donde finamente se acordó la salida del Reino Unido.

Los axiomas, aquellas realidades tan evidentes que no requieren ser demostradas, están desapareciendo. Las verdades o certidumbres evidentes para todos están siendo absorbidas por intereses ideológicos y económicos, o incluso por el despotismo de la incultura. Intereses ilegítimos, que no se corresponden con la evidencia razonada y razonable, **la evidencia científica,** ni tan siquiera el interés por lo esencial, que es el ser humano.

Este relativismo en los conceptos, como hemos señalado, es fruto del **fenómeno llamado posverdad,** que consiste en una manipulación de hechos objetivos, instrumentada por estos intereses ilegítimos, en la medida que manipulan la realidad, generando una pseudorealidad paralela, que sustituye a la realidad objetiva, que encuentra sus canales de influencia en diversos medios como pueden ser las redes sociales, de comunicación, o incluso en los propios órganos de gobierno de las administraciones, y por supuesto en sistemas de inteligencia de organismos públicos o privados.

La posverdad no es un fenómeno nuevo, si bien es cierto que es un término cada vez más utilizado en los últimos tiempos, pues constituye un verdadero problema de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

actualidad debido a los canales tecnológicos expansivos de trasmisión de información, hablamos de una **manipulación deliberada de la realidad, que** se puede implantar en los diferentes ámbitos de la sociedad.

Por ello, la importancia del principio de trasparencia, ante estos retos tecnológicos que sobrepasan nuestro conocimiento, la regulación debe exigir la ciencia, la conciencia y liderazgo profesional de juristas, periodistas y sanitarios, pues somos garantes de intereses públicos y derechos humanos irrenunciables para la dignidad de las personas.

No podemos dejar que las realidades científicas y objetivas sean modificadas a capricho de la manipulación. Científicos y porfesionales de todos los ámbitos, y más del ámbito del derecho, del periodismo y la sanidad, tenemos una gran responsabilidad en el devenir de nuestra sociedad, pues si nos plegamos a este fenómeno de la posverdad, claudicaremos ante **la verdad de la mentira,** y es por esta razón por la que el liderazgo, competencia y función publica de instituciones como la Universidad tiene que quedar patente, para desarrollar sus competencias y reafirmar la vocación, la ciencia y la deontología profesional, médica y jurídica en nuestro caso, frente a las ideologías e intereses de todo tipo.

Desde mi punto de vista, el principio de trasparencia es una clave esencial para el mantenimiento de los Derechos Humanos, tal y como los tenemos concebidos y los disfrutamos en la Comunidad Europea, **mediante una regulación que exija trasparencia, basada en ciencia y conciencia profesional**, principalmente para los tecnólogos, al igual que es una exigencia para los informes y documentos de juristas y sanitaritos, pues estos valores deben formar parte de la vocación de los profesionales y el liderazgo, que aunque sea una palabra que pueda sonar muy poética, hoy en día se hace fundamental para los derechos y libertades un liderazgo desde la ética, y por su puesto desde los valores y los Derechos Humanos.

5.3.2. Principio de veracidad

Es un principio íntimamente relacionado con el propicio de trasparencia, y aunque su base doctrinal surge en relación con **la presunción de veracidad de la autoridad** pública, que constituye prueba *iuris tantum,* o también como elemento clave en el ámbito de la publicidad, concretamente como instrumento para distinguir la publicidad engañosa y **proteger al consumidor** (Martín García, 2002, págs. 81-110) este principio adquiere especial relevancia en cuanto la exigencia de información veraz en el ámbito sanitario, donde la Ley 41/2002 de autonomía del paciente[17] recoge el derecho a la información, una información completa y veraz, así se puede deducir indubitadamente de su articulado.

Este derecho, íntimamente relacionado como el principio de confianza legítima, que al igual que en el siguiente punto hacemos con el principio de competencia profesional, lo atraemos desde el ámbito de aplicación de las administraciones públicas hacia

17. Ley 41/2002. *Op. cit.*

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

el ámbito de los profesionales, en los que ciudadanos y más aún los pacientes - véanse como consumidores y usuarios de los servicios sanitarios– tienen derecho a la confianza legítima en el sistema sanitario y en sus profesionales.

Es por ello, por lo que existe un deber y obligación de transmitir una información veraz, que abarque a todos los aspectos sanitarios, y ello conlleva la información completa y transparente en cuanto el funcionamiento de los sistemas de inteligencia artificial, telemedicina y robótica.

5.3.3. Principio de competencia profesional

El principio de competencia, referido a las competencias, generalmente exclusivas y excluyentes, que tienen asignadas los diferentes órganos de las administraciones publicas, adquiere especial relevancia si lo aplicamos al ámbito sanitario.

La Real Academia de la Lengua lo define como la ordenación de las potestades consistente en la asignación de atribuciones[18], aunque también lo define en relación con las competencias normativas de los gobiernos de las distintas administraciones publicas.

Como antes hemos indicado, las competencias profesionales para desarrollar actos médicos están atribuidas, de forma exclusiva, a los licenciados en medicina que cumplan normativa de habilitación profesional, concretamente el artículo 6 de la Ley de Ordenación de las Profesiones Sanitarias[19] establece que a los médicos corresponde la indicación y realización de actividades dirigidas a la promoción y mantenimiento de la salud, la prevención de enfermedades, el diagnóstico, tratamiento terapéutica y rehabilitación de los pacientes, así como el enjuiciamiento y pronóstico de los procesos objetos de atención.

Con lo cual, quedarían zanjadas las dudas concernientes a la habilitación del robot o inteligencia artificial para operar en el ámbito médico. Al margen del profesional médico, no es posible, al menos conforme la legalidad vigente.

Esta competencia excluyente operaría con todas aquellas profesiones reguladas que velen por intereses públicos, con competencias propias exclusivas y excluyentes, como farmacéuticos, enfermeros o médicos, o no sanitarias como abogados, entre otras.

De esta manera, de cualquier intervención en el ámbito sanitario que sea llevada a cabo por un instrumento de IA deberá responder el titular jurídico del desarrollo tecnológico, como si de cualquier otro tipo de bien industrial se tratara, tanto en el ámbito administrativo, civil y penal, pudiendo incurrir el titular del sistema, incluso, en un delito de intrusismo profesional, si se valiera de una IA para prestar servicios médicos sin intervención directa de un médico.

Por ello, consideramos también, que dada esta complejidad técnica y tecnológica, la necesaria regulación de estos instrumentos debe pasar por el establecimiento de siste-

18. Diccionario de la Real Academia de la Lengua. https://dpej.rae.es/lema/principio-de-competencia. Consultado el 8 de diciembre de 2021.

19. Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias. *Op. cit.*

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

mas reguladores de matriculación y/o licencia, certificación de calidad e inspección técnica periódica, donde se incluyan exigencias de trasparencia algorítmica, códigos fuentes y cualquier otra información necesaria para comprender el funcionamiento y argumentación en la toma de decisiones, así como un seguro de responsabilidad civil obligatorio.

Alcanzada esta conclusión, la intervención de sistemas de robótica e inteligencia artificial en el ámbito sanitario solo puede serlo de forma instrumental y así debe de observarlos cualquier regulación, como desarrollos tecnológicos de gran utilidad para los sanitarios, para la innovación, la investigación y el desarrollo, considerando siempre que debido a su complejidad técnica conllevará la obligación de cumplimiento de condiciones y medidas de prevención para seguridad del paciente que se puedan exigir en cada caso.

VI. Conclusiones

En definitiva, aunque el marco regulador europeo se manifiesta con una incomprensible ambigüedad en lo que respecta a la aplicación de las tecnologías 4.0 en el ámbito sanitario, lo cierto es que de un análisis profundo rezuma la evidencia de que estos sistemas son instrumentos que deben actuar en los exactos límites que establece la normativa vigente, debiendo centrarse la regulación en desarrollar los aspectos y principios claves, que son la transparencia, la veracidad de la información, la competencia profesional, así cómo la regulación de cuestiones referentes a responsabilidad y seguridad análogas a las que ya pueden existir para otros bienes tecnológicos, con el establecimiento de sistemas de matriculación o licencia, inspección técnica periódica, certificaciones de calidad, y seguro de responsabilidad civil. En consecuencia, no es necesaria una nueva regulación disruptiva, aunque sí estén siendo disruptivos los cambios del desarrollo tecnológico.

Asimismo, la eventual regulación debe partir de la regulación profesional existente, así como las estrategias sanitarias y normativas que se están desarrollando sobre la seguridad del paciente; y estar íntegramente enfocada desde los principios claves enunciados, el principio de transparencia, el principio de veracidad y el principio de competencia profesional, como fuentes inspiradoras de las garantías previstas en nuestro ordenamiento ante los retos tecnológicos y sanitarios a los que nos enfrentamos.

Por ello, consideramos que en el debate abierto sobre regulación de la telemedicina, la IA y la robótica en el ámbito sanitario, y como estrategia de gobernanza europea prevista en el Libro Blanco sobre inteligencia artificial, así como para garantizar el establecimiento de un marco ético y jurídico apropiado, basado en los valores de la Unión Europea y en consonancia con la carta de Derechos Fundamentales de la propia Unión, de la manera establecida en la Comunicación de la Comisión al Parlamento Europeo sobre inteligencia artificial, es fundamental partir de estos conceptos, como premisas, para superar con éxito los retos tecnológicos, y para que las autoridades públicas puedan garantizar que el desarrollo y uso de tecnologías de inteligencia artificial está en consonancia con los derechos y valores enunciados.

Los principios de competencia profesional exclusiva y excluyente, la identificación transparente y veraz de la persona responsable de los sistemas de inteligencia artificial

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

y/o robótica, así como de cualquier sistema tecnológico a distancia, así como la información técnica trasparente de toda la información sanitaria y tecnológica son garantías irrenunciables para los Derechos Humanos.

Estos instrumentos tecnológicos que tratamos no deben dejar nunca de ser herramientas o instrumentos, cuyos daños son cubiertos por el titular y propietario de las inteligencias fuertes o robots, como se responde de los daños causado por cualquier otro bien del que podamos ser titulares. Lo que sí habrá que definir es cuáles son esos instrumentos y qué características tienen; además de que todos deberán superar controles de calidad e inspecciones técnicas periódicas.

La identificación veraz de la persona, la veracidad científica y técnicamente describible, en definitiva, la trasparencia del informante y sus motivaciones, son garantías frente al fenómeno posverdad.

Por último, normas de calidad, códigos de conducta y códigos éticos, incluso recogiendo posibles declaraciones de conflicto de intereses, son elementos que deben de instaurarse en el ámbito, y que contribuirán a consolidar el núcleo de los derechos humanos (García San José, 2021, págs. 255-276).

VI. Bibliografía y otras referencias citadas

Asamblea General de la Asociación Médica Mundial, Reikiavik, 2018. https://www.wma.net/es/events-post/asamblea-general-de-la-amm-reykjavik-2018/

Asociación Médica Mundial. https://www.wma.net/es/quienes-somos/historia/. Consultada el 10 de diciembre de 2021.

Belloso Martín, N. "La necesaria presencia de ética en la robótica: La Roboética y su incidencia en los Derechos Humanos". *Cuadernos do Programa de Pos- Graduacao*. DIREITO/UFRGS, Vol. 13 (2), 2018, págs. 21-81.

Comisión Central de Deontología del Consejo General de Colegios Oficiales de Médicos. *"La Telemedicina en el acto Médico; Consulta médica no presencial o consulta online"*. https://medicostenerife.es/wp-content/uploads/2020/06/INFORME-E-CONSULTA_CCD_10_06_2020.pdf

Comisión Europea. Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza. Bruselas. 19 de febrero de 2020. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Comunicación de la Inteligencia artificial para Europa. COM/2018/237 final. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52018DC0237

De Asís Roig, R., Seoane, J.a., Wisner Glusko, C., Sepulveda Gómez, M. Ponencias Congreso Internacional sobre Inteligencia Artificial, Robótica y Filosofía del Derecho. Sevilla, 1 y 2 de diciembre de 2021.

Diéguez Lucena, A. "La filosofía de la técnica de Ortega como guía para la acción. Una comparación con Heidegger", *Revista internacional de tecnología, conocimiento y sociedad*. 2013. Págs. 73-97.

Estrategia mundial sobre salud digital 2020-2025. https://apps.who.int/iris/bitstream/handle/10665/344251/9789240027572-spa.pdf?sequence=1&isAllowed=y

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

Fernández-Coronado, A. Pérez Álvarez, S. *La protección de la salud en tiempos de crisis: Nuevos retos del bioderecho en una sociedad plural*. Tirant lo Blanch. Valencia, 2014, pág. 164.

Foro de Profesión Médica de España. *La Relación Médico Paciente. Patrimonio Cultural Inmaterial de la Humanidad*, CGCOM, Madrid, 2017.

García San José, D. "Implicaciones jurídicas y bioéticas de la inteligencia artificial. Especial consideración al marco normativo internacional". *Cuadernos de Derecho Transnacional*. Vol. 13, Nº1. Marzo 2021. Págs. 255-276.

García De Enterría, E., *Curso de Derecho Administrativo,* Tomo II, CIVITAS, Madrid, reimpresión 2001, pág. 107.

Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales. https://www.boe.es/buscar/act.php?id=BOE-A-1974-289

Ley 14/1986 General de Sanidad, de 25 de abril https://www.boe.es/buscar/act.php?id=BOE-A-1986-10499

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188

Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. https://www.boe.es/buscar/act.php?id=BOE-A-2003-10715

Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias. https://www.boe.es/buscar/pdf/2003/BOE-A-2003-21340-consolidado.pdf

Llano Alonso, F.H. Ponencia en VII Convención de Colegios de Médicos de Andalucía. Huelva. 25, 26 y 27 de noviembre de 2021.

Martín García, M. L., *La Publicidad: Su incidencia en la contratación*. Dykinson, Madrid, 2002, págs. 81-110.

Ministerio de Sanidad. *Recomendaciones para el análisis de los incidentes de seguridad del paciente con daño (eventos adversos); Cuestiones metodológicas y legales*. Informe, estudios e investigación del Ministerio de Sanidad,2021. https://seguridaddelpaciente.es/resources/documentos/2021/05/Recomendaciones%20para%20el%20an%C3%A1lisis%20de%20los%20incidentes%20de%20seguridad%20del%20paciente%20con%20da%C3%B1o.%20Accesible.pdf

Ortega y Gasset, J. *Meditaciones sobre la técnica y otros ensayos sobre ciencia y filosofía.* ALIANZA, Madrid, 2000, pág. 13.

Palma Ortigosa, A. "Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos", *Revista General de Derecho Administrativo,* nº 50. Iustel. Enero de 2019. http://laadministracionaldia.inap.es/noticia.asp?id=1509629

Parlamento Europeo. *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión*. COM /2021/ 206 final. Bruselas, 21.4.2021. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206

Parlamento Europeo. *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*. https://www.boe.es/doue/2016/119/L00001-00088.pdf

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

Parlamento Europeo. *Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html

Parlamento Europeo. *Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre política industrial global europea en materia de inteligencia artificial y robótica*. https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_ES.html

Real Academia de la Lengua. *Diccionario*. https://dpej.rae.es/lema/principio-de-competencia. Consultado el 8 de diciembre de 2021.

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555

Troncoso Reigada, A. *La Protección de Datos personales: En busca del equilibrio*. Tirant Lo Blanch, Valencia, 2010, págs. 74 y 75.

Sentencia del Tribunal Constitucional 37/2011, de 28 de marzo. https://hj.tribunalconstitucional.es/es/Resolucion/Show/6819

Sentencia del Tribunal Constitucional 3/2013, de 17 de enero 2013. http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/23233

Sentencia del Tribunal Supremo 2791/2018, de 16 de julio de 2018. N http://www.poderjudicial.es/search/AN/openCDocument/47c54a4d73e1a1965a444dd3e915a50c327144d5ce39e908

Unesco. *Recomendaciones sobre ética de la inteligencia artificial publicada por la UNESCO*. 22 de noviembre de 2021. https://es.unesco.org/artificial-intelligence/ethics

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 152-173
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.10

RESEÑAS

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

MARTÍN RÍOS, P., *et al.*, *La Tecnología y la Inteligencia Artificial al servicio del proceso*. Colex, Madrid, 2023, 336 páginas. Isbn: 978-84-1359-779-9

Evelyn Téllez Carvajal
Investigadora del Centro de Investigación e Innovación en TIC INFOTEC, México
evelyn.tellez@infotec.mx 0000-0001-6136-6821

Con el sugerente título *La Tecnología y la Inteligencia Artificial al servicio del proceso*, se reúnen trece trabajos doctrinales, publicados con el sello de la prestigiosa editorial Colex y bajo la dirección de los profesores Villegas Delgado y Martín Ríos, de la Universidad de Sevilla.

La obra colectiva referida trae causa de la celebración, en la Facultad de Derecho de dicha Universidad, del II Congreso Internacional "La Administración de Justicia en España y en América", bajo el amparo del proyecto de investigación "Biomedicina, Inteligencia Artificial, Robótica y Derecho: los retos de jurista en la era digital".

No puede recensionarse el estudio que nos ocupa sin hacer cumplida alusión a su prólogo. Por su enjundia y profundidad, bien hubiera podido constituir un capítulo aparte. Sin duda, contar con la participación del magistrado Rodríguez Lainz, incontestable autoridad en la materia, constituye una inmejorable carta de presentación.

A las sesudas reflexiones de reputados y consagrados profesores de Derecho Procesal de diversas Universidades españolas (Profesores Calaza López, Castillejo Manzanares, Etxeberria Guridi, Fontestad Portalés, Garcimartín Montero, Gómez Colomer, González Navarro, Nieva Fenoll y Ortiz Pradillo), se aúnan las contribuciones de dos jóvenes y prometedoras profesoras de la Universidad de Sevilla (Profesoras Domínguez Barragán y García Sánchez). El necesario enfoque internacional de una materia que -a todas luces- no conoce de fronteras, se consigue gracias a las ilustrativas aportaciones de Jorge Cerdio Herrán, Profesor del Instituto Tecnológico Autónomo de México, y Pier Paolo Paulesu, Catedrático de Derecho procesal penal de la Universidad de Padua.

Tratándose de una materia tan poliédrica, con tantas implicaciones distintas, resulta realmente complejo limitar su examen a solo una de ellas, sin exponerse al riesgo de resultar excesivamente limitado. Pese a ello, la mera lectura del índice hace abandonar tales recelos. Siempre desde una óptica jurídica, que es la que vertebra el estudio, se observa un abordaje de la cuestión que podríamos calificar de exhaustivo.

La obra que se presenta es una fiel radiografía del mundo que nos circunda, y no deja de ser reflejo de cómo la tecnología supone una parte considerable -de creciente importancia, además-

de nuestra vida. Se trata, en suma, de una materia que, sin ser novedosa, no abandona nunca su actualidad ni su relevancia. No es aventurado predecir -y el signo de los tiempos así parece evidenciarlo- que ambas crecerán exponencialmente en los próximos tiempos, de forma directamente proporcional al desarrollo técnico que el ser humano alcance.

Es bien sabido que la implantación práctica de las nuevas tecnologías a la Administración de Justicia, en general, y a los procesos civil y penal, en particular, trae consigo una serie de problemas añadidos. Es esencial que se parta de la base del necesario respeto a la protección de derechos y garantías procesales y al principio de "seguridad judicial electrónica" en todas sus dimensiones (autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad y conservación), lo que constituye el punto de partida de varios de los trabajos que componen la obra comentada. Iniciativas como estas contribuyen a dotar de mayores certezas a las múltiples incógnitas que acompañan a cualquier incursión en este terreno, sometido a permanente mutación.

Todos los estudios que se incorporan presentan un mismo hilo conductor, aun cuando lo transversal de la temática abordada explica que se aprecien múltiples enfoques en los diferentes trabajos que aglutina. Entre otros aspectos, en ella se analizan las complejidades que plantea la digitalización de los expedientes físicos en el tránsito hacia el Expediente Judicial Electrónico, con los retos que supone la creación de una sede judicial electrónica y las exigencias de interoperabilidad que comporta.

Se examinan, igualmente, las repercusiones prácticas que, para el ciudadano, supone ese tránsito (acceso a la justicia, transparencia, facilidad de comunicación y de conocimiento, economía de medios, ahorro temporal…), así como la repercusión de la brecha digital ante la pretensión de generalización del empleo de las nuevas tecnologías por parte de los profesionales de la justicia. Ninguna de estas dificultades, pese a lo complejo de su tratamiento, ha sido soslayada.

Era inevitable, y de ello han sido conscientes los editores, el examen del posible campo de actuación (así como de sus límites) de la -omnipresente- Inteligencia Artificial en la Administración de Justicia. Esta cuestión es analizada desde distintas ópticas: su impacto en el proceso penal (especialmente, por cuanto se refiere a la investigación y prueba de delitos), la contratación civil, la navegación marítima, la justicia administrativa o los Objetivos de Desarrollo Sostenible.

Como era de esperar en un libro de estas características, los análisis que en él se contienen tienen muy presente las implicaciones que la reconversión tecnológica de la Justicia tiene respecto de la debida protección de datos, como ámbitos claramente interrelacionados. Se parte de la base, para ello, de la capital importancia que revisten los datos en la sociedad contemporánea digital (considerados, no en vano, como el petróleo del siglo XXI). Del mismo modo, se aprecia una preocupación común por algo que no es baladí: las exigencias que han de respetarse en cuanto al aseguramiento de la conservación de forma segura (integridad y autenticidad) de la información generada como resultado de la citada reconversión.

En definitiva, por la amplitud de sus planteamientos, lo fundado y riguroso de sus argumentos y la rabiosa actualidad de las diferentes problemáticas que aborda, no po-

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 175-177
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.11

demos sino recomendar, vivamente, la detenida consulta de esta obra colectiva, así como felicitarnos por el hecho de que la Universidad aliente la realización de esfuerzos en esta dirección.

Nos movemos a ciegas en un escenario en constante cambio; sean bienvenidos estudios de este género, óptimos faros en la bruma jurídica.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 175-177
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.11

IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023
CC BY-NC-ND 4.0.

VALLESPÍN PÉREZ, D., *Inteligencia Artificial y Proceso: eficiencia vs garantías*. Juruá, Oporto, 2023, 279 páginas. IBSN: 978-989- 712-909-4

Luis Ernesto Orozco Torres
Profesor del Instituto de Ciencias Sociales y Administración
Universidad Autónoma de Ciudad Juárez, México.
luis.orozco@uacj.mx 0000-0003-4659-5153

A mediados del siglo pasado Ulrich Beck nos advertía en su "sociedad del riesgo" que vivimos en una "aldea" global, inter e hiperconectada, una sociedad, en definitiva, caracterizada por las amenazas globales -como la derivada de la crisis sanitaria que padecimos los últimos tres años-. En efecto, vivimos en un mundo de creciente complejidad, movilidad e incertidumbre en el que la globalización se nos presenta como un proceso irreversible, que ha tenido tanto efectos positivos como negativos sobre la vida de cientos de millones de seres humanos. El desarrollo de la técnica y la tecnología, la internacionalización de los capitales, la revolución en los medios de comunicación (que han dado lugar a la sociedad de la información) y el perfeccionamiento de los medios de transporte (que han acortado, y algunas veces desaparecido prácticamente las distancias) han hecho del mundo contemporáneo una realidad social cada vez más global e interdependiente pero no menos conflictiva ni más segura.

En el contexto de esta sociedad del riesgo global, y en plena era digital, el libro dirigido por el profesor David Vallespín Pérez analiza aquellos retos y desafíos que los Sistemas de Inteligencia Artificial (IA) han introducido en la ciencia del Derecho. Una IA que ha llegado para quedarse y que genera, a partes iguales, tanta fascinación como desconfianza. Como es sabido, son muchas las ventajas de la aplicación de la IA en el proceso, pero también lo son sus riesgos, tal como reconoce el director de la obra que hoy tenemos el privilegio de reseñar (véase el prólogo de la misma). Las ventajas son por todos conocidas: reducción de la carga de trabajo de los órganos encargados de administrar justicia, agilizar los tiempos de respuesta de los órganos jurisdiccionales, así como la previsión cuasi matemática de su contenido entre otras muchas. Por otro lado, la cara obscura de la IA nos ubica en la deshumanización de la justicia, la invasión de la intimidad, el desajuste de la administración de justicia con las exigencias de la protección de datos, así como el alejamiento de la ponderación real, en cada caso concreto, de las circunstancias particulares que le rodean. De ahí, precisamente, que tenga sentido plantearse la definición de un conjunto de reglas éticas que hagan posible no sólo definir una IA fiable, sino también una IA ajustada al irrestricto cumplimiento de los derechos humanos (en particular de las garantías del debido proceso

legal) consagrados tanto en las constituciones nacionales como en los instrumentos jurídicos internacionales que limitan la actuación de los actores tanto estatales como subestatales dentro del marco del desarrollo y puesta en práctica de los cada vez más avanzados sistemas de IA.

La obra titulada *Inteligencia Artificial y Proceso: eficiencia vs garantías*, editado por Juruá, está integrada por 15 estudios científicos especialmente vinculados a la ciencia del Derecho con una marcada carga hacia su vertiente procesal. Los autores, todos ellos voces autorizadas en la materia, provienen de distintas latitudes, tanto de Europa como de América Latina. Precisamente, temas como los abordados en esta obra están caracterizados por la difuminación del tiempo, del espacio y de las fronteras toda vez que no existe nada más global que los sistemas de IA.

Los estudios que componen la presente obra están relacionados con temas de notable actualidad y desafío futuro como lo son, por ejemplo, los relativos a la robotización de la valoración probatoria (pp. 13-21); los juicios telemáticos (pp. 23-36); los testigos virtuales y los testigos *on line* (pp. 37-53); los *Smart Contracts* y la prueba en el proceso (pp. 55-80); los títulos ejecutivos inteligentes (pp. 81-105); los riesgos del mediador avatar (pp. 133-145); los puertos, el transporte marítimo y la navegación inteligentes (pp. 147-156); la IA en la mediación (pp. 157-170); los aspectos éticos del uso de la IA en la toma de decisiones a la luz del Derecho de la Unión Europea (pp. 171-189); la Administración Pública en la era de la IA (pp. 191-204); la IA, las decisiones judiciales y la rendición de cuentas (pp. 205-212); la IA, las garantías judiciales y la motivación de las sentencias (pp. 213-233); la criminalidad informática en el sistema penal (pp. 235-254); el empleo de algoritmos en la función jurisdiccional (pp. 255-273), así como los enormes desafíos que imponen la gobernanza algorítmica, la ética de la IA y el Estado (Algorítmico) de Derecho a todos los juristas en la era digital (pp. 107-131). En efecto, se trata de temas de acuciante actualidad y de enorme trascendencia legal.

De forma particular, la obra analiza los retos derivados de la transformación digital de la administración pública, en la que la implantación de sistemas de IA se ha convertido en un arma de doble filo. Por un lado, la IA tiene el potencial para transformar nuestro mundo para bien, pero, por otro lado, su implantación práctica habría generado importantes inconvenientes para garantizar los derechos fundamentales de las personas.

Por otro lado, los autores de la obra analizan el complejo debate que se ha generado en torno a la denominada gobernanza algorítmica o de la IA. La gobernanza de la IA debe ser afrontada de manera urgente por nuestros representantes políticos, existe, en este sentido, una imperiosa necesidad de asegurar que los procesos de toma de decisiones y los sistemas institucionales se centren en las personas (como propone el modelo de gobernanza de la Unión Europea) y que se pueda rendir cuentas de ellos para, a su vez, garantizar la transparencia y la calidad de la gestión en la prestación de los servicios públicos.

Asimismo, se discuten las directrices éticas para una IA fiable, elaboradas por el Grupo Independiente de Expertos establecido en el seno de la Comisión Europea en 2018 -mismas que constituyen la base del modelo europeo de gobernanza de la IA- y de las que el principio del estado de Derecho integra una parte esencial.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 178-180
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.12

En línea con lo anterior, los autores se preguntan hasta qué punto sería legalmente admisible, a la luz del principio del estado de Derecho, todo lo que es posible lograr gracias a los adelantos científicos y tecnológicos en el campo de la IA. Para tal finalidad, se analizan las connotaciones particulares de este principio en el ámbito regional europeo para, posteriormente, analizar algunas propuestas que se han elaborado para adaptar este principio constitucional del orden jurídico europeo a la nueva era digital, llegándose incluso a hablar de un hipotético "Estado algorítmico de Derecho" para poner de manifiesto que deben existir mecanismos legales para evaluar la exactitud, relevancia y calidad de los datos de entrenamiento de los algoritmos, la publicidad del código fuente, y la fiscalización algorítmica, la evaluación *ex ante* y *ex post* de los sistemas de IA, los medios para determinar y gestionar el sesgo en los sistemas de aprendizaje automático o la trazabilidad, la fundamentación de las decisiones adoptadas y las posibilidades de defensa y recurso frente a ellas.

En suma, los trabajos que componen la obra que hoy reseñamos hacen un balance de los retos y desafíos que el Derecho debe afrontar ante una nueva y desconocida realidad: la era de la Inteligencia Artificial, cuyas luces y sombras integran las dos caras de una misma moneda.

Por último, debemos señalar que se trata de un libro muy bien escrito, a pesar de la complejidad técnica de los temas abordados el mensaje llega con facilidad al lector, su claridad expositiva no le resta profundidad a las cuestiones materiales que aborda y sobre las que no sólo se limita a plantear las diferentes posturas del debate científico, sino que se posiciona ante él. En definitiva, *Inteligencia Artificial y Proceso: eficiencia vs garantías* –dirigida por el profesor David Vallespín Pérez– constituye una obra de obligada lectura no sólo para los distintos operadores del sistema de justicia, sino también para cualquier otra persona interesada en la incidencia de las nuevas tecnologías en el campo del Derecho.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 178-180
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.12