# TRABAJO FIN DE GRADO

## **GRADO EN DERECHO**

# CURSO ACADÉMICO 2024 / 2025

## **TÍTULO:**

¿ESTAMOS EN LA SENDA CORRECTA? INTELIGENCIA ARTIFICIAL: LOS RETOS DEL MAÑANA

### **WORK TITLE:**

ARE WE ON THE RIGHT PATH? ARTIFICIAL INTELLIGENCE: THE CHALLENGES OF TOMORROW

**AUTOR:** 

VÍCTOR GUTIÉRREZ DE LA ROSA

DIRECTOR:

JOSÉ IGNACIO SOLAR CAYÓN





### ¿ESTAMOS EN LA SENDA CORRECTA? INTELIGENCIA ARTIFICIAL: LOS RETOS DEL MAÑANA

ARE WE ON THE RIGHT PATH? ARTIFICIAL INTELLIGENCE: THE CHALLENGES OF TOMORROW

VÍCTOR GUTIÉRREZ DE LA ROSA

Sumario: I. INTRODUCCIÓN, II. LA CONTROVERTIDA DEFINICIÓN DE INTELIGENCIA ARTIFICIAL, III. DEEPFAKE, ¿ES SUFICIENTE LA PROTECCIÓN DEL REGLAMENTO PARA EL RIESGO QUE SUPONE ESTA TECNOLOGÍA? IV. LA GOBERNANZA DE LA IA V. CONCLUSIONES VI. BIBLIOGRAFÍA

#### **SUMARIO**

La inteligencia artificial será la tecnología más importante de nuestro siglo. Es por esto por lo que este análisis se centra en evaluar algunos de los retos que aún nos quedan por delante. A pesar de la reciente aprobación del Reglamento sobre IA de la UE, y el creciente interés por reglamentar la IA a nivel global, una mirada crítica sigue siendo necesaria. La importancia de definir de común acuerdo la IA a fin de no descuidar el objeto a proteger, la inclusión y correcta valoración de prácticas tan cruciales como el *Deepfake* en las nuevas reglamentaciones o la esencial decisión de encaminarnos hacia a una gobernanza de la IA global o regional son algunos de los retos que se tratarán en este estudio. Resolverlos marcará el rumbo hacia una IA útil y fiable, o una IA peligrosa y desestabilizadora.

### **ABSTRACT**

Artificial intelligence will be the most important technology of our century. That is why this analysis focuses on evaluating some of the challenges that still lie ahead. Despite the recent approval of the EU's AI Regulation and the growing interest in regulating AI globally, a critical look remains necessary. The importance of collectively defining AI in order not to neglect the object to protect, the inclusion and proper assessment of practices as crucial as Deepfake in new regulations, or the essential decision to move towards global or regional AI governance are some of the challenges that will be addressed in this study. Resolving them will set the course towards either a useful and reliable AI or a dangerous and destabilizing one.





## I. INTRODUCCIÓN

En este estudio se abordará el tema de la inteligencia artificial desde tres problemáticas clave.

En la primera parte exploraremos el problema terminológico, analizaremos la definición proporcionada por el nuevo reglamento sobre IA de la UE y lo confrontaremos con las distintas opiniones de autores relevantes en la materia. Finalizaremos este primer bloque temático clasificando las diferentes inteligencias artificiales, enfocándonos sobre todo en la clasificación de riesgo proporcionada por el reglamento de la Unión Europea.

El segundo asunto que trataremos será el controvertido tratamiento que se le da a la tecnología deepfake en el Reglamento. Analizaremos sus capacidades, la protección que brinda el Reglamento y evaluaremos si la protección es suficiente para el peligro que supone, sobre todo respecto a la relación de la mujer con esta tecnología.

Por último, el bloque final pretende dar una visión acerca de cómo se está abordando el tema de la inteligencia artificial a nivel global. Analizaremos sucintamente los distintos modelos regionales de los tres grandes ejes de regulación mundial a nivel de inteligencia artificial, y propondremos una solución más vinculada a un esfuerzo conjunto que a regionalismos en competencia, dada la importancia que tiene y tendrá esta tecnología en nuestro siglo.

#### II. LA CONTROVERTIDA DEFINICION DE INTELIGENCIA ARTIFICIAL

## 1. EL PROBLEMA TERMINOLÓGICO DE LA IA

El término "inteligencia artificial" es controvertido. El concepto de IA nace de la mano de Alan Turing mediante la asociación de la idea de *inteligencia*, entendida como cualidad propia y única de los humanos, y la calificación de artificial, en oposición a lo *natural*<sup>1</sup>. El aval de la habilidad de estas máquinas para pensar y actuar como un humano proviene del denominado "*Imitation game*<sup>2</sup>" de Turing. Esta herramienta, también denominada "*Test de Turing*", es un método de

 $<sup>^{1}</sup>$  HAVLÍK, V., "The naturalness of artificial intelligence from the evolutionary perspective," AI & Soc 34, 2019, pág. 889.

<sup>&</sup>lt;sup>2</sup> TURING, A. M., "Computing machinery and intelligence," *Springer Netherlands*, 2009, págs. 23-65.





evaluación que mide la capacidad de una máquina para exhibir un comportamiento inteligente similar al de un ser humano o indistinguible de este<sup>3</sup>. Es aquí donde surgen las discrepancias. En primer lugar, porque, a mayor capacidad, mayor riesgo, lo que conllevará una regulación distinta, como veremos más adelante en nuestro análisis del reglamento sobre IA de la UE. Y, en segundo lugar, porque la tendencia reduccionista tiende a sobrevalorar las capacidades de la inteligencia artificial actual, atribuyendo a esta mayores capacidades de las que realmente posee.

John R. Searle elaboró su experimento "*Chinese room"* con el objetivo de rebatir lo propuesto por Turing. Searle afirma que la máquina carece de comprensión porque solo simula comprensión<sup>4</sup>. Este experimento pone de manifiesto la idea esencial de que la manipulación sintáctica de conceptos no implica el entendimiento de su significado semántico<sup>5</sup>.

Roger Penrose, por su parte, explica que una simulación computacional de un proceso físico es algo muy diferente del proceso real<sup>6</sup>. En esa línea, pero desde otra perspectiva, el problema de la ausencia de conciencia es clave para autores como Solum<sup>7</sup>, mientras que, siguiendo a Hawkins, el único ejemplo de inteligencia -entendida como la habilidad para aprender, planificar y ejecutar- es el cerebro<sup>8</sup>. Surden argumenta que la tecnología de la IA produce resultados

<sup>&</sup>lt;sup>3</sup> En términos muy simplificados, Turing partía de la premisa de que si la máquina logra convencer a un interrogador que es una persona la que responde se confirma el hecho que la máquina tiene la capacidad de pensar y, por lo tanto, es inteligente.

<sup>&</sup>lt;sup>4</sup> SEARLE, J. R., "Minds, brains, and programs." *Behavioral and Brain Sciences*, 3, 1980, pág. 417–424.

<sup>&</sup>lt;sup>5</sup> NECHITA, E., "On the approaches of classical artificial intelligence and embodied artificial intelligence," *Scientific Studies and Research, Series Mathematics, and Informatics,* 21, 2011, pág. 176. Afirma que: "dado que la inferencia deductiva implica la manipulación sintáctica de las representaciones simbólicas de acuerdo con reglas que operan sobre la base de las formas de los símbolos en lugar de lo que los símbolos pueden representar, los programas que simulan el razonamiento humano mediante la manipulación de símbolos basada en reglas parecen estar en el camino correcto".

<sup>&</sup>lt;sup>6</sup> PENROSE, R., "Las sombras de la mente: hacia una comprensión científica de la consciencia". *Crítica*. 1996, págs. 340-360.

<sup>&</sup>lt;sup>7</sup> SOLUM. L., "Legal Personhood for artificial intelligences", *N. Carolina L. Rev.*, 70, 1992, págs. 1265-1272.

<sup>&</sup>lt;sup>8</sup> HAWKINS. J., "Special report: Can we copy the brain? - What intelligent machines need to learn from the Neocortex", *IEEE Spectrum*, vol. 54, no. 6, 2017, págs. 34-71.





inteligentes, pero sin inteligencia, "aprovechando patrones, reglas y *proxies* heurísticos que le permiten tomar decisiones útiles en ciertos contextos concretos<sup>9</sup>.

Como puede observarse, existe cierto disenso entorno a la definición de inteligencia artificial y a la concreción de sus capacidades<sup>10</sup>. Siguiendo a Linde y Schweizer, en referencia al término inteligencia, "si bien es un concepto amplio e integral, también es notoriamente elusivo<sup>11</sup>". Es fácil caer en simplificaciones y visiones demasiado antropocéntricas de la inteligencia, que nos hagan alejarnos de las verdaderas capacidades actuales de la IA. Algunos autores como Luc Julia llegan a criticar el uso de la expresión inteligencia por entender que se trata de una gran operación de marketing<sup>12</sup>. Postura que, aunque pueda resultar ciertamente extrema, puede llegar a entenderse fruto del auge actual de la IA y la obsesión mediática por incluirla, como reclamo y a discreción, en todo tipo de productos.

López de Mántaras es concluyente al advertir que el problema con la IA estriba en que "no es realmente inteligente ni, en realidad, aprende. Al menos no en el sentido que un humano les daría a los significados de aprender y de ser inteligente. Lo que hay ahora es una inteligencia artificial con unas competencias extraordinarias en áreas determinadas (...) competencias sin comprensión. Son máquinas competentes que no comprenden nada<sup>13</sup>". No hay que olvidar, por

\_\_\_

<sup>&</sup>lt;sup>9</sup> SURDEN, H., "Artificial Intelligence and Law: An Overview," Ga. St. U. L. Rev, 35, 2019, pág. 1337.

<sup>&</sup>lt;sup>10</sup> BROOKS, R. A., "Intelligence without representation," *Artificial Intelligence*, Volume 47, Issues 1–3, 1991, Págs. 139-159.

WINFIELD, A. F. T., "On the simulation (and energy costs) of human intelligence, the singularity and simulationism." *In A. Adamatzky, & V. Kendon (Eds.), From Astrophysics to Unconventional Computation*, Springer Nature Publishing AG, 2019, pág. 404.

<sup>&</sup>lt;sup>11</sup> LINDE, H. & SCHWEIZER, I., "A White Paper on the Future of Artificial Intelligence," White paper, 2019, págs. 1-10.

<sup>&</sup>lt;sup>12</sup> JULIA, L., "L'intelligence artificielle n'existe pas", *First Editions, París*, 2019.

LÓPEZ DE MÁNTARAS, R., & JAUME-PALASÍ, L., "Inteligencia artificial, robotización y cuarta revolución industrial", *Milenio*, 2019, pág. 49.





otra parte, que generalmente se opera con una visión básicamente antropocéntrica de la inteligencia<sup>14</sup>.

A través de estas aportaciones doctrinales podemos visualizar la magnitud de la problemática que plantea la definición de la IA, cubriendo un espectro que va desde la apología de la singularidad hasta la negación de la posibilidad misma de usar la expresión inteligencia para designar este fenómeno<sup>15</sup>. Explica Wang que la falta de consenso en el marco institucional y doctrinal es una carencia más grave de lo que, en principio, podría parecer para la construcción de un discurso teórico y para la propia ordenación de la IA16. Pero esta situación trae causa, en gran medida, de la tendencia a agrupar dentro de esa categoría programas, diseños o artificios muy diferentes entre sí y que, en algunos casos, no van más allá de la pura mecánica.

### 2. LA DEFINICION DE LA UNION EUROPEA

Visto el debate existente acerca de la definición de la inteligencia artificial, podemos entender mejor el insistente interés de la Unión Europea en encontrar "una definición ajustada, clara y precisa de la IA<sup>17</sup>" que sea capaz de "ser lo más tecnológicamente neutra posible y resistir al paso del tiempo lo mejor posible, habida cuenta de la rápida evolución tecnológica y del mercado en relación con la IA<sup>18</sup>".

<sup>&</sup>lt;sup>14</sup> WANG, P., LIU, K., & DOUGHERTY, Q. "Conceptions of artificial intelligence and singularity,"

Information, 9, 2018, pág. 82. HAVLÍK, V., "The naturalness of artificial intelligence from the evolutionary perspective," AI & Soc *34*, 2019, pág. 898.

<sup>&</sup>lt;sup>15</sup> Robles Carrillo, M. La gobernanza de la inteligencia artificial: contexto y parámetros generales. 2020, pág. 9.

<sup>&</sup>lt;sup>16</sup> WANG P., "On defining Artificial Intelligence". Journal of Artificial General Intelligence, vol. 10, nº 2, 2019, págs. 2-5.

<sup>&</sup>lt;sup>17</sup> COMISIÓN EUROPEA, "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". 2021, pág. 10.

<sup>&</sup>lt;sup>18</sup> COMISIÓN EUROPEA, "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". 2021, pág. 15.





Es por estos motivos que el reglamento confecciona la siguiente definición:

"«Sistema de IA»: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales<sup>19</sup>".

Analizando esta definición podemos llegar a dos conclusiones:

En primer lugar, observamos que, gracias al profundo desglose realizado, superamos el problema de la concepción unitaria y homogénea de la inteligencia artificial. En la definición se describen una pluralidad de niveles de autonomía, así como resultados diversos posibles entre sí que dejan de estar incluidos de manera genérica en el concepto IA, para formar de manera individual sus grupos propios. (Además de dar una definición propia, enfocada eso si al riesgo que provoca cada tecnología diferenciada, para cada uno de los distintos ingenios derivados de la IA<sup>20</sup>.)

En segundo lugar, y al hilo de lo anterior, podemos observar como la definición de inteligencia artificial se desliga de esa visión antropomórfica<sup>21</sup> generalizada, y alimentada especialmente por la literatura y los medios de comunicación, que no

<sup>&</sup>lt;sup>19</sup> COMISIÓN EUROPEA, "Reglamento de Inteligencia Artificial". P9\_TA(2024)0138. 2024, pág. 166

<sup>&</sup>lt;sup>20</sup> Nos referimos a las definiciones contenidas en el Art. 3 del reglamento sobre IA, así como a los distintos niveles de riesgo que se enumeran en los capítulos subsiguientes.

<sup>&</sup>lt;sup>21</sup> El acercamiento clásico y básico identifica la IA "como una entidad que se separó de un soporte físico". NECHITA, E, "On the approaches of classical artificial intelligence and embodied artificial intelligence," *Scientific Studies and Research, Series Mathematics, and Informatics,* 21. 2011, pág. 176.





se corresponde con una realidad en la que hay distintas modalidades de IA y la mayoría de ellas no responde a ese patrón.<sup>22</sup>

# 3. CLASIFICACIÓN DE LOS DISTINTOS TIPOS DE IA, VISIÓN GENERAL Y DEL REGLAMENTO SOBRE IA DE LA UNIÓN EUROPEA.

Basándonos en el potencial de la IA podríamos distinguir entre una IA débil o fuerte<sup>23</sup>; o entre una IA específica, general o superinteligente<sup>24</sup>. Desde esta perspectiva, y como afirma Wang, "la inteligencia sigue siendo una cuestión de grados. Ningún sistema puede ser perfectamente inteligente, aunque un sistema pueda ser más inteligente que otro al ser capaz de adquirir conocimiento de más formas (...), de reorganizar sus creencias y habilidades de maneras más complicadas (...), o de adaptarse de manera más eficiente"<sup>25</sup>.

En este estudio nos centraremos en la inteligencia artificial débil o especifica por una simple razón, es la única de la cual disponemos actualmente. Sin embargo, las diferenciaremos de manera sucinta.

"Los sistemas con IA específica son capaces de realizar una tarea concreta incluso mejor que un humano, pero solamente esa tarea.

Los sistemas con IA general exhiben una inteligencia similar a la humana por ser múltiple, adaptable, flexible, eficiente, incremental.

Los sistemas con superinteligencia hacen referencia a una inteligencia superior a la humana<sup>26</sup>".

<sup>22</sup> OLIVER, N., "Inteligencia artificial: ficción, realidad... y sueños", *Discurso de ingreso en la Real Academia de Ingeniería*, 2018, pág. 1-30.

8

RUSSEL, S., & NORVIG, P., "Artificial Intelligence: A Modern Approach Pearson," London, 2010.
 WANG, P., LIU, K., & DOUGHERTY, Q. "Conceptions of artificial intelligence and singularity," Information, 9, 2018, pág. 82 y ss.

<sup>&</sup>lt;sup>25</sup> WANG P., "On defining Artificial Intelligence", *Journal of Artificial General Intelligence*, vol. 10, no 2, 2019, pág. 28.

<sup>&</sup>lt;sup>26</sup> OLIVER, N., "Inteligencia artificial: ficción, realidad... y sueños", cit., pág. 21.





En el estadio actual de desarrollo solo se dispone de IA específica, pues para lograr crear sistemas de inteligencia artificial general o superinteligencia es necesario alcanzar una serie de hitos (capacidad de los sistemas de inteligencia artificial para ser autoconscientes, desarrollo de un sentido común a la hora de razonar o la capacidad del sistema para definir y determinar sus propios objetivos y metas), y responder a numerosas preguntas desde una perspectiva ética, científica y tecnológica<sup>27</sup>.

Centrándonos, ahora sí, en la IA débil, debemos advertir la variedad inmensa de ingenios que esta inteligencia artificial encierra bajo el termino genérico de IA especifica. Para hacernos una idea y sin entrar en detalles, todas las diversas categorías recogidas en el reglamento sobre IA podrían contener en sí mismos una categoría diferenciada de IA especifica.

De manera general y sin entrar en detalles, estas podrían clasificarse por el tipo de automatización, así como en relación con las modalidades de exteriorización de la IA<sup>28</sup>. También, una distinción esencial basada en el modelo de aprendizaje, el procedimiento inductivo o deductivo y la autonomía del dispositivo<sup>29</sup>, entre Machine Learning<sup>30</sup> y Deep Learning o, más precisamente, incluso, entre aprendizaje supervisado, no supervisado, reforzado y profundo<sup>31</sup>, entre otras.

El reglamento opta por una forma mucho más pragmática de clasificación, en lugar de tratar de encajar todas las cientos de tecnologías distintas en sus

. .

 $<sup>^{27}</sup>$  AI HLEG, "AI High-Level Expert Group on AI. Ethics guidelines for trustworthy AI," 2019, pág. 5

<sup>&</sup>lt;sup>28</sup> KOSTOPOULOS distingue entre tres tipos de IA: intangible, tangible and embedded. (intangibles, tangibles e incrustados). "la IA intangible no tiene una forma física, sino que puede comunicarse a través de un sonido, una notificación en un dispositivo y/o computación invisible. (...) La IA tangible se encarna en una forma física, con la que los humanos pueden interactuar. Por último, la IA integrada es cuando se fusiona con nuestro cerebro ya sea a través de un mecanismo invasivo o no invasivo". KOSTOPOULOS, L., "The Emerging Artificial Intelligence Wellness Landscape: Opportunities and Areas of Ethical Debate," *California Western School of Law, AI Ethics Symposium Rev., 55,* 2018, págs. 235-255.

<sup>&</sup>lt;sup>29</sup> CHESTERMAN, S., "Artificial intelligence and the limits of legal personality," *International and Comparative Law Quarterly*, 69. 2020, págs. 819-844.

<sup>&</sup>lt;sup>30</sup> HAGE, J., "Theoretical foundations for the responsibility of autonomous agents." *Artificial Intelligence Law*, no 25, 2017, pags. 255-271.





categorías precisas (lo cual traería mucha polémica, sobre todo porque estas se interrelacionan entre sí) las clasifica en función del riesgo, ordenándolas entorno a cuatro estadios.

En el Capítulo II encontramos las Prácticas de inteligencia artificial prohibidas, en el Capítulo III los Sistemas de IA de alto riesgo, el Capítulo IV regula las obligaciones de transparencia para determinados sistemas de IA y por último los Modelos de IA de uso general contenidos en el Capítulo V<sup>32</sup>.

Esta segregación por riesgo viene ampliamente justificada en el preámbulo del reglamento. Sin embargo, creemos que hay una tecnología que se ha infravalorado, sobre todo respecto a sus capacidades de aumentar la desigualdad de género.

### III. DEEPFAKE, ¿ES SUFICIENTE LA PROTECCION DEL REGLAMENTO PARA EL RIESGO QUE SUPONE ESTA TECNOLOGIA?

# 1. DEEP LEARNING, ¿QUÉ ES Y CÓMO FUNCIONA?

El aprendizaje profundo (Deep Learning) funciona como una red neuronal, esto es, mediante arquitecturas de procesamiento inspiradas en las neuronas biológicas. Los datos que se introducen en un algoritmo de *Deep Learning* pasan por múltiples capas "ocultas"<sup>33</sup> de funciones de procesador discretas e interconectadas. Cada capa sintetiza y procesa los datos de la capa anterior antes de transmitirlos a la siguiente. Las redes neuronales de aprendizaje profundo pueden determinar y detectar características destacadas por sí mismas<sup>34</sup>. Además, desde 2014, gracias a las redes generativas antagónicas (en

<sup>31</sup> TALLEC, C. & BLIER, L. & OLLIVIER, Y., "Making Deep Q-learning methods robust to time discretization," International Conference on Machine Learning, 2019, págs. 6096-6104.

<sup>32</sup> MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. "El Reglamento Europeo de IA, en resumen", 2024, pág 1.

<sup>&</sup>lt;sup>33</sup> De ahí el empleo del calificativo Deep.

<sup>&</sup>lt;sup>34</sup> FLETCHER, J., "Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance," Theatre Journal, volumen 70, número 4, 2018, pp. 455-471.





adelante, GAN en sus siglas en inglés: *generative adversarial networks*<sup>35</sup>) se ha podido mejorar radicalmente los resultados.

Las GAN funcionan enfrentando dos redes neuronales: una red discrimina<sup>36</sup>, mientras que otra red genera datos que tratan de vencer al discriminador. Para que se entienda mejor, el modelo generativo puede considerarse análogo a un equipo de falsificadores, mientras que el modelo discriminativo hace las veces de la policía, que intenta detectar la falsificación. La competencia lleva a ambos bandos a mejorar sus métodos hasta que las falsificaciones son indistinguibles de las auténticas<sup>37</sup>. Pero, a diferencia de lo que sucede con los seres humanos, que pueden encontrar límites en función de su educación o capacidad, los algoritmos de *Deep Learning* sólo están limitados por la potencia de cálculo<sup>38</sup>.

# 2. REGULACIÓN DEL *DEEP FAKE* EN EL REGLAMENTO SOBRE IA DE LA UNIÓN EUROPEA

El reglamento define *Deep Fake*, en su artículo 3.1. 60) como:

"«ultrafalsificación»: un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares u otras entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos".

Los *Deep Fakes* se encuentran regulados en el tercer nivel de riesgo (Capitulo IV, articulo 50). Nivel en el que se exigen ciertas obligaciones de transparencia a los proveedores y responsables del despliegue de estos sistemas de IA.

<sup>36</sup> Por ejemplo, qué es perro de qué es gato.

<sup>&</sup>lt;sup>35</sup> Término acuñado por primera vez por GOODFELLOW, I. J., POUGET-ABADIE, MIRZA, XU, WARDE-FARLEY, OZAIR, COURVILLE y BENGIO, "Generative Adversarial Nets," *Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014)*, 2014.

<sup>&</sup>lt;sup>37</sup> GOODFELLOW, I. J., POUGET-ABADIE, MIRZA, XU, WARDE-FARLEY, OZAIR, COURVILLE y BENGIO, «Generative Adversarial Nets», cit., pág 1.





Las principales exigencias para los proveedores son:

- Art. 50.1: "Los proveedores garantizarán que las personas físicas (...) estén informadas de que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización".
- Art. 50.2: Los proveedores de sistemas de IA (...) que generen contenido sintético de audio, imagen, vídeo o texto, velarán por que la información de salida del sistema de IA esté marcada en un formato legible por máquina y que sea posible detectar que ha sido generada o manipulada de manera artificial<sup>39</sup>.

En cuanto a las exigencias para los responsables del despliegue:

Art. 50.4: "Los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrafalsificación harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial<sup>40</sup>".

A reglón seguido el reglamento explica que:

"Cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos o de ficción, las obligaciones de transparencia establecidas en el presente apartado se limitarán a la obligación de hacer pública la existencia de dicho contenido generado o

<sup>&</sup>lt;sup>38</sup> FLETCHER, J., "Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance," cit., págs. 455-471.

<sup>&</sup>lt;sup>39</sup> COMISIÓN EUROPEA, "Reglamento de Inteligencia Artificial". P9\_TA(2024)0138. 2024, págs. 282 y 283.





manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra".

Por tanto, de estos artículos podemos sacar dos conclusiones. En primer lugar, se observa que el Reglamento pone especial énfasis en señalar la importancia de exhibir de forma clara cuando un contenido ha sido manipulado por IA. Y en segundo lugar se puede comprobar que esta condición de transparencia puede quedar excepcionada cuando una persona actúe con la diligencia debida y haya sido convenientemente informada, o cuando se trate de una obra artística, y se haya explicitado la presencia de contenido manipulado o alterado. Es decir, el Reglamento insiste en la importancia de que la persona física sepa en todo momento que se encuentra frente a contenido alterado por IA.

Sin embargo, más allá de estas exigencias de transparencia, a estos sistemas no se les impone, al menos no de forma explícita, mayores limitaciones, lo cual resulta llamativo.

De forma indirecta, estos sistemas puedan entrar en la categoría de alto riesgo cuando afecten lo dispuesto en el Anexo III. En este anexo se recoge en concreto un supuesto en el que esta tecnología podría encajar a la perfección:

"Sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de personas físicas que ejerzan su derecho de voto en elecciones o referendos<sup>41</sup>."

La regulación de estos *deepfakes* es importante porque en la actualidad esta tecnología es capaz de realizar videos prácticamente indetectables, que podrían llegar a provocar crisis democráticas irreparables<sup>42</sup>.

<sup>40</sup> COMISIÓN EUROPEA, "Reglamento de Inteligencia Artificial". P9\_TA(2024)0138. 2024, pág. 284.

<sup>&</sup>lt;sup>41</sup> COMISIÓN EUROPEA, "Reglamento de Inteligencia Artificial". P9\_TA(2024)0138. 2024, pág. 430.





Y es precisamente por la capacidad técnica de los *deepfakes* en la actualidad que sorprende y preocupa que en el reglamento no se disponga ninguna protección especial hacia el derecho a la propia imagen<sup>43</sup>, y más en concreto hacia la vulnerable posición de la mujer dentro del modelo de sociedad patriarcal<sup>44</sup>.

### 3. UN PELIGRO INCIPIENTE. ESPECIAL RIESGO PARA LAS MUJERES.

A continuación, desarrollaremos los motivos por los que creemos que las exigencias que dispone el reglamento son insuficientes, y por qué debería incluirse esta forma de violencia contra la mujer como un supuesto prohibido o al menos de alto riesgo.

Esta tecnología toma su nombre del seudónimo de un usuario de Reddit que en 2017 se hizo viral por publicar vídeos pornográficos protagonizados por actrices famosas realizados mediante esta tecnología. Es de hecho este el momento en que se populariza esta tecnología, por lo que la vinculación del *deepfake* con la violencia contra la mujer es absoluta<sup>45</sup>. Una abrumadora mayoría de videos *deepfakes* en internet se emplean en lo que se conoce como abuso de imagen íntima no consentida<sup>46</sup>, que, de acuerdo con el Instituto Europeo para la Igualdad de Género<sup>47</sup>, consiste en la creación no consentida y/o la difusión no consentida, principalmente en línea, de imágenes/vídeos íntimos o privados o de carácter sexual<sup>48</sup>, que, en su gran mayoría<sup>49</sup>, además, tienen a la mujer como

Ejemplos de las capacidades del *deepfake* en la actualidad: <a href="https://youtu.be/3wVpVH0Wa6E?si=Wno-4IB1UsYrIXVO">https://youtu.be/3wVpVH0Wa6E?si=Wno-4IB1UsYrIXVO</a>
<a href="https://youtu.be/oxXpB9pSETo?si=N8wHiYt1z6VfkF9E">https://youtu.be/oxXpB9pSETo?si=N8wHiYt1z6VfkF9E</a>

<sup>&</sup>lt;sup>43</sup> CABRERA, C., "El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial", *InDret*, 2023, págs. 74-113.

<sup>&</sup>lt;sup>44</sup> GARCÍA, E. C., & CALVO, E., "Perspectiva de género en Inteligencia Artificial, una necesidad", *Cuestiones de género: de la igualdad y la diferencia*, 17, 2022, págs. 111-127.

<sup>&</sup>lt;sup>45</sup> CERDAN, V. & PADILLA-CASTILLO, G., "Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso", *Historia y Comunicación Social*, 24, 2019, pág 506.

<sup>&</sup>lt;sup>46</sup> Termino traducido directamente del inglés: *non-consensual initimate image abuse.*"

<sup>&</sup>lt;sup>47</sup> Conocido por sus siglas en inglés, EIGE, European Institute for Gender Equality.

<sup>&</sup>lt;sup>48</sup> EUROPEAN INSTITUTE FOR GENDER EQUALITY, "Combating Cyber Violence against Women and Girls", *Lituania*, 2022, pág. 54, donde expresamente indican que "el término también puede incluir la creación y difusión de contenidos falsos y deepfakes, así como otras formas de violencia





objetivo<sup>50</sup>. Estos supuestos están cada vez más presentes en la sociedad, afectando tanto a personas famosas<sup>51</sup> como a personas anónimas<sup>52</sup>. Es a través de escenas eróticas y pornográficas ficticias que las mujeres son cosificadas y despojadas de su identidad, lo cual contrasta con la utilización que se les da a estas mismas herramientas respecto a los hombres<sup>53</sup>. Estos, de manera general, son desprestigiados o desacreditados, pero rara vez desnudados y vejados, como sucede con las mujeres<sup>54</sup>.

Es por todo lo previamente descrito que creemos insuficientes las exigencias del reglamento. No se trata de un problema menor o de una situación que pueda resolverse con una simple marca de agua que acredite que esos videos son falsos, se trata de un problema global que afecta de forma sistemática a la mujer y cuyo daño es muy difícil de resarcir o mitigar, pues el realismo es tal que a veces incluso siendo falso y sabiéndose falsos producen indefensión<sup>55</sup>.

basada en la imagen, como el voyeurismo digital y el ciberflashing [esto es, el envío de material obsceno a extraños a través de Bluetooth o Airdrop]".

págs. 74-113.

<sup>&</sup>lt;sup>49</sup> HAO afirma que "entre el 90% y el 95% de todos los videos *deepfake* que pueden encontrarse online son de pornografía no consentida. Y de ellos, en torno al 90% lo es de mujeres." HAO. "Deepfake porn is ruining women's lives. Now the law may finally ban it," *MIT Technology Review*, vol. 124, número 1, 2021.

<sup>&</sup>lt;sup>50</sup> DE VIDO Y SOSA, consideran que "el uso o la difusión de imágenes íntimas o privadas está condicionado por el género. Los estudios y los datos han demostrado que las mujeres y las niñas son los principales objetivos de la violencia sexualizada digital en línea y, como proyección de la violencia no en línea contra las mujeres, se ven afectadas de forma desproporcionada. Además, los estereotipos y las normas sociales persistentes, junto con un modelo de relaciones de poder históricamente construido, tienden a culpar a la mujer víctima". DE VIDO y SOSA. "Criminalisation of gender-based violence against women in European States, including ICT-facilitated violence," *A special report*, Bruselas, 2021, pág. 136.

<sup>&</sup>lt;sup>51</sup> El País, "Rosalía denuncia la foto falsa en la que aparece desnuda, creada y publicada por el cantante JC Reyes: "Es violencia."" El País, 2023.

<sup>&</sup>lt;sup>52</sup> El País, "Decenas de menores de Extremadura denuncian que circulan fotos de falsos desnudos suyos creadas por inteligencia artificial: "Me dio un vuelco el corazón."" El País, 2023.

<sup>&</sup>lt;sup>53</sup> TRIPATHI, S., "Women and Online Harassment." *Feminist Dissent,* 6, 2022, págs. 133-158. LUCAS, K. T., "Deepfakes and domestic violence: perpetrating intimate partner abuse using video technology." *Victims & Offenders,* 17(5), 2022, págs. 647-659.

<sup>&</sup>lt;sup>54</sup> CERDAN, V. & PADILLA-CASTILLO, G., "Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso". *Historia y Comunicación Social*, 24, 2019, págs 516 y 517. <sup>55</sup> CABRERA, C., "El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial", cit.,





Ya en su momento, y al respecto de la legislación española, Carlos Trujillo Cabrera planteó la posibilidad de que se articularan especiales medidas frente al fenómeno del *deepfake*. Su conclusión fue que:

"el ordenamiento jurídico cuenta con herramientas suficientes para ofrecer al titular de los derechos vulnerados los mecanismos necesarios para actuar frente a tales ataques, restaurar la integridad de sus derechos y resarcirse, en su caso, del daño sufrido". (...) Ahora bien, pudiera ser recomendable plantear una actualización del régimen jurídico"

De la misma forma es esto mismo lo que se propone en este estudio. Sería adecuado considerar esta situación con la entidad que merece y, al menos, regularla explícitamente en el reglamento de la misma forma que se hace con el peligro que supone el *deepfake* respecto a la democracia. Entendemos que quizás existan otros mecanismos en los que esta problemática pueda encajarse sin necesidad de introducir un subapartado en el Anexo III, sin embargo, nuestra opinión es que esta situación debería reglamentarse como supuesto de alto riesgo por la especial situación de vulneración que provoca en la mujer y la gran desigualdad de género que alimenta.

### IV. LA GOBERNANZA DE LA IA

1. LOS DISTINTOS MODELOS INTERREGIONALES

La creación por parte de la Unión Europea de un reglamento sobre IA es una noticia verdaderamente positiva. Este reglamento no solo da un giro al paradigma internacional, que se había enfocado sobre todo en realizar propuestas de *soft law*<sup>56</sup>, sino que además logra dar una gran protección al

 $<sup>^{56}</sup>$  VEGA IRACELAY, J.J., afirma que  $soft\ law$  consiste en un grupo de principios capaces de garantizar la transparencia y responsabilidad en materia de algoritmos [emitidos por la US





mercado europeo, a los derechos de los consumidores, a la privacidad y a los derechos ya consagrados en la CEDH. Sin embargo, vivimos en un mundo global, y no podemos permitirnos el lujo de establecer regulaciones interregionales que ignoren la realidad internacional.

El problema de la IA es un problema mundial, y es por esto por lo que autores como Yannick Meneceur defienden una gobernanza global de la IA. Yannick afirma que una tecnología como la IA, que transformará profundamente la sociedad, reclama normas adoptadas de conformidad a un sistema internacional jurídico<sup>57</sup>. En suma, debe ser un organismo internacional, como la ONU, quien regule de manera internacional el asunto de la IA, de la misma forma que ya ocurrió con otros asuntos tan apremiantes como con el tratado de no proliferación de armas nucleares. Actualmente existen tres actores principales en la regulación de la IA, y cada uno toma un camino diverso.

En primer lugar, tenemos a la Unión Europea, cuya propuesta se basa en la garantía de los derechos del consumidor, y las ideas que están en la base de su ordenación, como es la Carta de los Derechos Fundamentales de la Unión Europea, a través de un enfoque basado en el riesgo.

En segundo lugar, encontramos a EE. UU. con un enfoque desarrollado por el Departamento de Defensa del NSCAI, que promueve la llamada Open Society, una alianza de Estados que busca competir con China en la carrera por desarrollar la IA<sup>58</sup>. Recientemente Biden emitió una orden ejecutiva destinada a establecer una serie de normas para limitar los riesgos de los sistemas más avanzados, pero sin intención de proponer mayores restricciones ni limitaciones,

Asociation for Computing Machinery (ACM)] sin carácter vinculante. VEGA IRACELAY, J.J., "Inteligencia artificial y derecho: principios y propuestas para una gobernanza eficaz", Informática y Derecho: Revista Iberoamericana de Derecho Informático, segunda época, segundo semestre, 5, 2018, págs.13-48.

<sup>&</sup>lt;sup>57</sup> MENECEUR, Y., "L'intelligence artificielle en procès", cit., pág. 325-327.

<sup>&</sup>lt;sup>58</sup> NSCAI, "The Full Report," 2021, pág 13. NSCAI, "The Final Report," 2021, págs. 1-2.





más allá de la exigencia de notificar a los usuarios cuando las imágenes o el texto haya sido generado por IA<sup>59</sup>.

En tercer lugar, tenemos a China, que desde 2017 lleva desarrollando su legislación sobre IA, la cual fue actualizada en 2021 y recientemente en 2023 y que adopta básicamente un modelo tecnoautoritario, permitiendo muchas de las practicas que la UE ha prohibido en el reglamento, como el uso de tecnologías biométricas para el control de la población<sup>60</sup>.

En conclusión, tenemos tres modelos distintos, el de la UE que busca ser garantista con los derechos afianzados por la Unión, el de EE. UU. más libertario, y el de China que se inclina más por el uso autoritario y de control de esta tecnología<sup>61</sup>.

## 2. UNA SOLUCIÓN GLOBAL

Yannick Meneceur afirma que no es descabellado pensar que sea necesario el diseño de una nueva arquitectura legal para la regulación de la IA<sup>62</sup>. Estamos frente a una de las tecnologías más revolucionarias, complejas e invasivas, capaz de dejar obsoleto el actual sistema.

Sea como sea, lo que es seguro es que el problema del control de la IA tendrá que abordarse de forma global, en una gobernanza conjunta de la ONU o mediante tratados internacionales sectoriales, como propone Themistoklis Tzimas<sup>63</sup>. De lo contrario, y sin una intervención decidida del Derecho Internacional o de la ONU, todo apunta a que la legislación sobre IA se dividirá en dos bloques legales: el democrático y el de la sociedad de la vigilancia, sin

62 MENECEUR, Y., "L'intelligence artificielle en procès", cit., 2020.

<sup>&</sup>lt;sup>59</sup> GOVERNMENT OF EE. UU., "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," 2023.

<sup>&</sup>lt;sup>60</sup> MORENO, L., Y PEDREÑO, A., "Europa frente a EE. UU. Y China. Prevenir el declive en la era de la inteligencia artificial". *Autoeditado en Amazon*, 2020.

<sup>&</sup>lt;sup>61</sup> VÁZQUEZ PITA, E., "La UNESCO y la gobernanza de la inteligencia artificial en un mundo globalizado, la necesidad de una nueva arquitectura legal", *UNED*, 2021, págs. 284-295.





perjuicio de que, en el futuro, puedan suscribirse acuerdos o tratados internacionales sobre armas autónomas (AWS), como ya sucedió con las armas nucleares.

En este respecto, avances como los de la UNESCO<sup>64</sup> o la reciente resolución de la ONU<sup>65</sup> son pasos clave. En concreto la citada resolución de la ONU, encaminada al uso de la IA en la consecución de los ODS<sup>66</sup>, recuerda a lo defendido por Christiana Figueres y Tom Rivett-Carnac, que afirmaban que la supervisión y la gobernanza de las políticas sobre la IA seria decisiva para la descarbonización, recordando la importancia que tuvo el acuerdo de París de 2015, el cual fue decisivo para que los países adoptasen políticas comunes para reducir el calentamiento global<sup>67</sup>. Es importante recordar en este punto, sobre todo vista la regulación realizada por la Unión Europea basada en el riesgo, que, si bien es cierto que la IA supone un peligro en ciernes, también presenta una oportunidad irrepetible de mejora y evolución en la consecución de los principales desafíos de la raza humana. Es por esto por lo que este estudio considera esencial que exista un común acuerdo a la hora de regular esta tecnología, pues lo contrario alimentará una guerra por el control de esta y no un avance unido hacia la consecución de los objetivos que nos unen como planeta.

Para finalizar, Robles Carrillo incide en la importancia de adoptar, en el plano normativo, "un enfoque proactivo y abierto, no formalista, para la organización de la gobernanza sobre la base del Derecho internacional en vigor, donde existen normas imperativas y obligatorias aplicables a la IA y mecanismos de desarrollo

<sup>&</sup>lt;sup>63</sup> TZIMAS, T., Legal and Ethical Challenges of Artificial Intelligence from an International Law Perspective", Cham (Suiza): Springer, 2021.

<sup>&</sup>lt;sup>64</sup> UNESCO, "Proyecto de texto de la recomendación sobre la ética de la inteligencia artificial", 2021.

<sup>65</sup> ASAMBLEA DE LAS NACIONES UNIDAS, "A/RES/78/265", 2024.

<sup>66 &</sup>quot;Objetivos de desarrollo sostenible".

<sup>&</sup>lt;sup>67</sup> FIGUERES, C. y RIVETT-CARNAC, T., *El futuro por decidir. Cómo sobrevivir a la crisis climática*, Madrid: Debate. Penguin Random House Grupo Editorial, 2021, págs. 148-152.





normativo capaces de enfrentar el desafío que supone la regulación internacional de la IA<sup>68</sup>".

### V. CONCLUSIONES

La inteligencia artificial es la gran tecnología de nuestra época. Definirla ha sido el gran quebradero de cabeza de muchos autores. Las opiniones se han extendido desde la apología de la singularidad hasta la negación de la posibilidad de usar la expresión inteligencia para designar este fenómeno. Por fortuna, los distintos organismos internacionales han dado definitivamente el paso hacia la regulación de esta tecnología.

La UE ha resuelto el problema terminológico, desarrollando una definición y un marco regulatorio que será imperativo a partir de su entrada en vigor, dando seguridad y certeza jurídica a los ciudadanos, empresas e instituciones de la Unión Europea. Sin embargo, este reglamento también revela algunos vacíos normativos que preocupan especialmente a este estudio. El auge de los deepfakes, y la perfección técnica que han ido desarrollando en los años recientes, desvela una amenaza en ciernes para ciertos sectores claves de nuestra sociedad. Algunos han sido adecuadamente controlados por el reglamento, como el peligro que estas nuevas tecnologías presentan frente a las instituciones democráticas, categorizando estas como de alto riesgo. Sin embargo, otros como la posición de vulnerabilidad de la mujer respecto a esta tecnología no han sido, desde el punto de vista de este estudio, controlados de manera propicia, dejando ciertamente desprotegido a este colectivo. Los deepfakes como categoría genérica vienen regulados en el Reglamento como una tecnología a la cual se la requieren obligaciones de transparencia. No obstante, visto el creciente número de deepfakes en línea de contenido pornográfico protagonizado por mujeres, de los cuales más del 90% de estos son

<sup>68</sup> ROBLES CARRILLO, M., "La gobernanza de la inteligencia artificial: contexto y parámetros





no consentidos, creemos que esta obligación de transparencia es insuficiente. La propuesta de este estudio es que se aborde de la misma forma que se hace con el peligro a las instituciones democráticas, categorizando este supuesto como de alto riesgo, en aras de preservar la igualdad de género.

Otro punto que nos interesa especialmente es la aparición de modelos interregionales de regulación de la inteligencia artificial. Estos modelos, lejos de propiciar una mirada común y coordinada del problema, están alimentando la división de las regulaciones en dos vertientes ciertamente polarizadas, las democráticas y la de la sociedad de la vigilancia. Estas tres posturas, defendidas por los principales actores geopolíticos, EE. UU., la UE y China, son una troika descontrolada sin jinete. El peligro de una regulación interregional no es otro que la repetición de una carrera armamentista y la inseguridad de los ciudadanos ante la aparición de gobiernos que usen la IA como herramienta de control y opresión. La propuesta de este estudio es que los organismos internacionales sean los que se encarguen de dirigir esa troika, dando un giro de 180º a la IA para enfocarla en resolver los principales problemas globales recogidos en los objetivos de desarrollo sostenible.

En conclusión, podríamos decir que nos encontramos en el momento clave, las decisiones que tenemos que tomar de ahora en adelante, respecto a la IA, marcaran el rumbo de nuestra relación con la misma. Articular una regulación global, en pro de abordar los retos planetarios como el cambio climático, o limitar de manera más contundente el *deepfake* para prevenir las desigualdades de género, son algunas de las propuestas que desde aquí impulsamos para una IA más fiable y útil. Como hemos podido observar, no son pocos los autores que nos acompañan en nuestras propuestas, y solo el tiempo y la voluntad de las partes determinará si podremos terminar por hacer de la Inteligencia Artificial una herramienta más de nuestro día a día, o una peligrosa arma de control, destrucción y vulneración de derechos descontrolada.





## VI. BIBLIOGRAFÍA

**AI HLEG,** "AI High-Level Expert Group on AI. Ethics guidelines for trustworthy AI", 2019, pág. 5.

ASAMBLEA DE LAS NACIONES UNIDAS, "A/RES/78/265", 2024.

**BROOKS, R. A.,** "Intelligence without representation", Artificial Intelligence, Volume 47, Issues 1–3, 1991, Págs. 139-159.

**CABRERA, C.,** "El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial", InDret, 2023, págs. 74-113.

**CERDAN, V. & PADILLA-CASTILLO, G.,** "Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso". Historia y Comunicación Social, 24, 2019, págs 506-517.

**CHESTERMAN, S.,** "Artificial intelligence and the limits of legal personality", International and Comparative Law Quarterly, 69. 2020, págs. 819-844.

**COMISIÓN EUROPEA,** "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". 2021.

**COMISIÓN EUROPEA,** "Reglamento de Inteligencia Artificial". P9 TA(2024)0138. 2024.

**DE VIDO y SOSA.** "Criminalisation of gender-based violence against women in European States, including ICT-facilitated violence", A special report, Bruselas, 2021, pág. 130-140.

**El País,** "Decenas de menores de Extremadura denuncian que circulan fotos de falsos desnudos suyos creadas por inteligencia artificial: "Me dio un vuelco el corazón."" El País, 2023.

**El País,** "Rosalía denuncia la foto falsa en la que aparece desnuda, creada y publicada por el cantante JC Reyes: "Es violencia."" El País, 2023.





**EUROPEAN INSTITUTE FOR GENDER EQUALITY**, "Combating Cyber Violence against Women and Girls", Lituania, 2022, pág. 54.

**FIGUERES, C. y RIVETT-CARNAC, T.,** El futuro por decidir. Cómo sobrevivir a la crisis climática, Madrid: Debate. Penguin Random House Grupo Editorial, 2021, págs. 140-152.

**FLETCHER, J.,** "Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance", Theatre Journal, volumen 70, número 4, 2018, pp. 455-471.

**GARCÍA, E. C., & CALVO, E.,** "Perspectiva de género en Inteligencia Artificial, una necesidad", Cuestiones de género: de la igualdad y la diferencia, 17, 2022, págs. 111-127.

**GOODFELLOW, I. J., POUGET-ABADIE, MIRZA, XU, WARDE-FARLEY, OZAIR, COURVILLE y BENGIO**, "Generative Adversarial Nets", Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014), 2014.

**GOVERNMENT OF EE. UU.,** "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", 2023.

**HAGE, J.,** "Theoretical foundations for the responsibility of autonomous agents". Artificial Intelligence Law, no 25, 2017, págs. 255-271.

**HAO.** "Deepfake porn is ruining women's lives. Now the law may finally ban it", MIT Technology Review, vol. 124, número 1, 2021.

**HAVLÍK, V.**, "The naturalness of artificial intelligence from the evolutionary perspective", AI & Soc 34, 2019, pág. 889-898.

**HAWKINS. J.,** "Special report: Can we copy the brain? - What intelligent machines need to learn from the Neocortex", IEEE Spectrum, vol. 54, no. 6, 2017, págs. 34-71.

JULIA, L., "L'intelligence artificielle n'existe pas", First Editions, París, 2019.

**KOSTOPOULOS, L.,** "The Emerging Artificial Intelligence Wellness Landscape: Opportunities and Areas of Ethical Debate", California Western School of Law, AI Ethics Symposium Rev., 55, 2018, págs. 235-255.





**LINDE, H. & SCHWEIZER, I.,** "A White Paper on the Future of Artificial Intelligence", White paper, 2019, págs. 1-10.

LÓPEZ DE MÁNTARAS, R., & JAUME-PALASÍ, L., "Inteligencia artificial, robotización y cuarta revolución industrial", Milenio, 2019, pág. 49.

**LUCAS, K. T.,** "Deepfakes and domestic violence: perpetrating intimate partner abuse using video technology". Victims & Offenders, 17(5), 2022, págs. 647-659.

MENECEUR, Y., "L'intelligence artificielle en procès", cit., 2020, pág. 320-330.

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN

DIGITAL. "El Reglamento Europeo de IA, en resumen", 2024, pág 1.

**MORENO, L., Y PEDREÑO, A.,** "Europa frente a EE. UU. Y China. Prevenir el declive en la era de la inteligencia artificial". Autoeditado en Amazon, 2020.

**NECHITA, E,** "On the approaches of classical artificial intelligence and embodied artificial intelligence", Scientific Studies and Research, Series Mathematics and Informatics, 21. 2011, pág. 170-180.

**NSCAI,** "The Final Report", 2021.

**NSCAI**, "The Full Report", 2021.

**OLIVER, N.,** "Inteligencia artificial: ficción, realidad... y sueños", Discurso de ingreso en la Real Academia de Ingeniería, 2018, pág. 1-30.

**PENROSE, R.,** "Las sombras de la mente: hacia una comprensión científica de la consciencia". Crítica. 1996, págs. 340-360.

**ROBLES CARRILLO, M.** La gobernanza de la inteligencia artificial: contexto y parámetros generales. REEI, nº. 39, 2021, pág. 1-30.

**RUSSEL, S., & NORVIG, P.,** "Artificial Intelligence: A Modern Approach Pearson", London, 2010.

**SEARLE, J. R.,** "Minds, brains, and programs". Behavioral and Brain Sciences, 3, 1980, pág. 410–424.

**SOLUM. L.,** "Legal Personhood for artificial intelligences", N. Carolina L. Rev., 70, 1992, págs. 1265-1272.





SURDEN, H., "Artificial Intelligence and Law: An Overview", Ga. St. U. L. Rev, 35, 2019, pág. 1337.

**TALLEC, C., BLIER, L. & OLLIVIER, Y.,** "Making Deep Q-learning methods robust to time discretization", International Conference on Machine Learning, 2019, págs. 6096-6104.

**TRIPATHI, S.,** "Women and Online Harassment". Feminist Dissent, 6, 2022, págs. 133-158.

**TURING, A. M.,** "Computing machinery and intelligence", Springer Netherlands, 2009, págs. 23-65.

**TZIMAS, T.,** Legal and Ethical Challenges of Artificial Intelligence from an International Law Perspective", Cham (Suiza): Springer, 2021.

**UNESCO,** "Proyecto de texto de la recomendación sobre la ética de la inteligencia artificial", 2021.

**VÁZQUEZ PITA, E.,** "La UNESCO y la gobernanza de la inteligencia artificial en un mundo globalizado, la necesidad de una nueva arquitectura legal", UNED, 2021, págs. 284-295.

**VEGA IRACELAY, J.J.,** "Inteligencia artificial y derecho: principios y propuestas para una gobernanza eficaz", Informática y Derecho: Revista Iberoamericana de Derecho Informático, segunda época, segundo semestre, 5, 2018, págs.13-48.

**WANG P.,** "On defining Artificial Intelligence", Journal of Artificial General Intelligence, vol. 10, no 2, 2019, pág. 1-28.

**WANG, P., LIU, K. & DOUGHERTY, Q.** "Conceptions of artificial intelligence and singularity", Information, 9, 2018, pág. 70-90.

**WINFIELD, A. F. T.,** "On the simulation (and energy costs) of human intelligence, the singularity and simulationism". In A. Adamatzky, & V. Kendon (Eds.), From Astrophysics to Unconventional Computation, Springer Nature Publishing AG, 2019, pág. 400-422.

### **YOUTUBE:**





https://youtu.be/3wVpVH0Wa6E?si=Wno-4lB1UsYrlXVOhttps://youtu.be/oxXpB9pSETo?si=N8wHiYt1z6VfkF9E