UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

Departamento de Derecho Internacional, Eclesiástico y Filosofía del Derecho

LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL CONTEXTO DE HECHOS INTERNACIONALMENTE ILÍCITOS

Laura Odile Comino Castro
Tutor: Dr. Juan Emilio Suñé Cano

MÁSTER EN DERECHO INTERNACIONAL
Trabajo Fin de Máster, Convocatoria Ordinaria 2024-2025
Madrid, 2 de junio de 2025

TRIBUNAL CALIFICADOR:
Dra. Ana Gemma López Martín (Presidenta),
Dr. Juan Bautista Cartes Rodríguez, Dr. Joaquín González Ibáñez
CALIFICACIÓN: 8,5/10

RESUMEN: Este trabajo final de máster en Derecho internacional público observa el impacto de la inteligencia artificial (IA) sobre el cumplimiento y la violación de las obligaciones estatales. La investigación analiza el apoyo de la IA a la posibilidad de comisión de hechos internacionalmente ilícitos, e identifica las funciones de esta tecnología sobre las prácticas ilícitas de los Estados. Con una organización acorde a la teoría de tridimensionalidad del derecho, se analiza primero en el Capítulo I el valor de la IA para los Estados, analizando sus intereses y el cumplimiento de sus obligaciones internacionales mediante la tecnología. El Capítulo II revisa los hechos, siendo estos la práctica ilícita de los Estados fomentada por la IA. El Capítulo III concluye analizando las normas existentes en la comunidad internacional actual, en particular el Reglamento de la IA de la Unión Europea y el Tratado del Consejo de Europa. Así, este trabajo busca demostrar la necesidad de regulación adicional específica para la IA en Derecho internacional, y revisa los efectos de esta tecnología sobre el Estado de Derecho internacional.

PALABRAS CLAVE: Inteligencia artificial - Hechos internacionalmente ilícitos - Obligaciones estatales - Consejo de Europa - Estado de Derecho internacional

---

ABSTRACT: This master's thesis in Public International Law examines the impact of artificial intelligence (AI) on the fulfillment and breach of state obligations. The paper analyzes AI's support for the possibility of committing internationally wrongful acts and identifies the functions of this technology in the illicit practices of nation-states. Organized according to the three-dimensional theory of law, Chapter I first analyzes the value of AI for nation-states, analyzing their interests and the fulfillment of their international obligations through the technology. Chapter II reviews the current situation, specifically the illicit conduct of nation-states fostered by AI. Chapter III concludes by analyzing existing norms in the current international community, particularly the European Union’s AI Act and the Council of Europe’s Treaty. Thus, this paper seeks to demonstrate the need for additional regulation specific to AI in International Law, and reviews the effects of this technology on the International Rule of Law.

KEYWORDS: Artificial Intelligence - Internationally wrongful acts - State obligations - Council of Europe - International Rule of Law

LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL CONTEXTO DE HECHOS INTERNACIONALMENTE ILÍCITOS

ABREVIATURAS MÁS UTILIZADAS

IA: *Inteligencia Artificial*

HII: *Hecho internacionalmente ilícito*

UE: *Unión Europea*

CdE: *Consejo de Europa*

ONU: *Organización de las Naciones Unidas*

OECD: *Organización para la Cooperación y el Desarrollo Económico*

PA 2001: *Proyecto de Artículos sobre Responsabilidad del Estado por HII de la Comisión de Derecho Internacional del 12 de diciembre de 2001*

SAL: *sistema autónomo letal*

RIA: *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (Reglamento sobre la Inteligencia Artificial)*

TCdE*: Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y derechos humanos, democracia y Estado de derecho del 5 de septiembre de 2024 (Tratado del Consejo de Europa)*

I. INTRODUCCIÓN

Como advirtió el Secretario General de las Naciones Unidas António Guterres en el Foro Económico Mundial 2024, se necesita considerar "urgentemente" el rol de la inteligencia artificial (IA) en la comunidad mundial y los riesgos que presenta[1]. El reto actual que suponen los avances tecnológicos es apreciable en una multitud de aspectos a nivel global, y el Derecho internacional no se ve excluido. La innovación en el área de la IA en particular es un núcleo que presenta beneficios y riesgos importantes en cuanto a su uso y funciones en el comportamiento de los Estados y el cumpliento de sus obligaciones internacionales.

La complejidad del análisis del papel de la IA en el Derecho internacional, particularmente en su rol de apoyo a la comisión de hechos internacionalmente ilícitos (HII), se encuentra en su creciente uso en la práctica de los Estados. Existen igualmente grandes beneficios en su uso, lo que hace que esta tecnología se esté incorporando en varios aspectos de las instituciones de Derecho internacional igualmente. En 2023 por ejemplo, la Corte Penal Internacional desveló su "Proyecto Armonía" (en inglés "Project Harmony"), el cual incluye una aplicación de la IA para revisar pruebas presentadas en los casos. La Corte afirma que la tecnología permite revisar más documentos, y obtener "mayores conocimientos" asegurando simultáneamente cumplimento con los estándares apropiados para la gestión de estas pruebas[2].

Existen muchos casos similares a nivel de organizaciones internacionales; la Organización de las Naciones Unidas (ONU), por ejemplo, resalta el uso de la IA en varios de sus cuerpos por sus beneficios. Indica que hasta un 80% de los Objetivos de Desarrollo Sostenibles establecidos podrían ser acelerados con esta tecnología[3]. El empleo de la IA se esta convirtiendo en una necesidad institucional en muchos ámbitos, para el apoyo estatal; la UNESCO explicó por ejemplo en abril de 2025 que un curso dado a profesionales jurídicos

---

[1] A. Guterres, "Davos 2024: Special Address by António Guterres, Secretary-General of the United Nations", *World Economic Forum*, 17 de enero de 2024, disponible en https://www.weforum.org/stories/2024/01/davos-2024-special-address-by-antonio-guterres-secretary-general-of-the-united-nations/ (última consulta: 15 de marzo de 2025).

[2] Declaración, *"ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform: OTPLink"*, declaración del 24 de mayo de 2023. Publicado por la Corte Penal Internacional, disponible en https://www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink (última consulta: 31 de marzo de 2025).

[3] United Nations, "Artificial Intelligence (AI)", en *Global Issues*, disponible en https://www.un.org/en/global-issues/artificial-intelligence (última consulta: 17 de abril de 2025).

en Ruanda tenía que incluir la IA en el mismo marco de importancia que la protección de datos y el Estado de Derecho[4].

La presencia e influencia de la IA es extensa, y se resaltan a menudo sus beneficios en la práctica jurídica. Es sin embargo imprescindible entender el rol de esta tecnología en manos de los Estados, lo que incluye la consideración de la práctica ilícita mediante esta. Este trabajo se centrará por lo tanto en entender el interés estatal en la IA (en su Capítulo I), al mismo tiempo que su uso en apoyo a posibles HII (Capítulo II). Se revisarán igualmente en el Capítulo III las normas existentes, para analizar la capacidad del Derecho internacional vigente de asumir el riesgo de la innovación en este campo tecnológico.

1. Principios técnicos básicos

Se ha de reconocer ante todo la complejidad tecnológica de la IA—definida aquí como la habilidad de un ordenador de actuar como un ser humano inteligente[5]— y sus aplicaciones. Esta investigación no tiene la intención de profundizar sobre los detalles técnicos de su funcionamiento, pero sí es imprescindible adentrarse en los principios básicos de la IA para entender sus efectos así como para matizar el interés de su regulación en el Derecho internacional. Para ello, es primeramente importante entender que no es una tecnología nueva; pese de tener un renacimiento en la conversación mundial actual, la IA cumple ya varias décadas. Su apelación fue acuñada por informático John McCarthy en 1956[6], de un concepto que nació de la aparición del test de Turing (una prueba con objetivo de discernir si se está hablando con una persona o una máquina) en 1950[7].

En segundo lugar, se han de entender los dos pilares fundamentales que componen la IA *grosso modo*: los datos que se le proporciona, y los algoritmos que aprenden de ellos y sus patrones. De esta manera, la IA es capaz de analizar los datos que la componen para, por ejemplo, resolver problemas, dar respuestas a preguntas complejas, y realizar predicciones y

[4] UNESCO, "Shaping the future of justice in Rwanda: training of Judiciary on AI, Data Protection and the Rule of Law", 22 de abril de 2025, disponible en https://www.unesco.org/en/articles/shaping-future-justice-rwanda-training-judiciary-ai-data-protection-and-rule-law (última consulta: 24 de abril de 2025).
[5] United Nations Department for General Assembly and Conference Management, *Definition of AI*, disponible en https://unterm.un.org/unterm2/es/view/49e80eb5-7736-4861-8f62-ffacfde67208 (última consulta: 17 de abril de 2025).
[6] W. Barfield y U. Pagallo, *Advanced Introduction to Law and Artificial Intelligence*, Elgar Advanced Introductions series, Edward Elgar, 2020, p. 1.
[7] *Ibid*., p. 7.

tareas[8]. La IA necesita y revisa una cantidad masiva de información[9], permitiendo así a sus usuarios realizar actividades que una persona—o varias—físicamente no podría, en un tiempo mínimo. A nivel estatal, esto permite aventurarse en prácticas y proyectos que necesitarían un gran capital humano si fueran realizados sin IA, como los que se verán a continuación.

El campo de la IA es extenso; existen varios subtipos y aplicaciones dentro de esta disciplina[10]. Por su envergadura limitada, este trabajo no se puede adentrar a explicar cada uno de ellos; al centrarse en la responsabilidad estatal, se mencionara puntualmente algunas de dichas aplicaciones explicando en su momento en que consisten. Aún así, se ha de subrayar que la IA tiene más aplicaciones que las herramientas más conocidas en el día a día civil. Mientras que la persona con poco conocimiento de la disciplina puede reconocer la IA como siendo casi exclusivamente sistemas con las cuales cualquier usuario puede interactuar (tal y cómo ChatGPT[11] o DeepSeek[12]), estas son solo una fracción del universo de la IA. Este público conoce así esencialmente solo un subtipo concreto, llamado *large language models* (en castellano, grandes modelos de lenguaje) que aprenden de datos de texto humano para realizar tareas como redactar correos electrónicos o resumir contenidos[13]. Estos modelos son igualmente solo una pequeña parte de la llamada IA generativa, que permite como su nombre indica generar contenidos[14]. Los casos a nivel estatal vistos a continuación en Derecho internacional utilizan la IA de maneras más intrincadas que simples *large language models*; emplean concretamente la IA generativa para ir más allá de la interacción directamente con personas y fuera de sus varios usos en la vida civil[15].

---

[8] Colorado State University Global, "How Does AI Actually Work?", blog post, 9 de agosto de 2021, disponible en https://csuglobal.edu/blog/how-does-ai-actually-work#:~:text=AI%20systems%20work%20by%20combining,performance%20and%20develops%20additional%20expertise (última consulta: 15 de marzo de 2025).

[9] Universidad Complutense de Madrid, *Certificado en Inteligencia Artificial en las Ciencias Sociales y Jurídicas · 4ª edición*, disponible en https://empowertalent.com/ucm/inteligencia-artificial/ (última consulta: 15 de marzo de 2025).

[10] Colorado State University Global, "How Does AI… *op. cit.*.

[11] Una herramienta de IA generativa popular, contando con "cientos de millones" de usuarios, de la compañía estadounidense OpenAI https://openai.com/chatgpt/overview/ (última consulta: 15 de marzo de 2025).

[12] La competencia a OpenAI viniendo de China, de la cual se hablará a continuación. https://www.deepseek.com/ (última consulta: 15 de marzo de 2025).

[13] *Vid*. IBM, "What are large language models (LLMs)?", 2 de noviembre de 2023, disponible en https://www.ibm.com/think/topics/large-language-models (última consulta: 15 de marzo de 2025).

[14] Véase J. A. Sandhu, "What are LLMs and generative AI? A beginner's guide to the technology turning heads", Schwartz Reisman Institute for Technology and Society, 25 de enero de 2024, [en línea], disponible en https://srinstitute.utoronto.ca/news/gen-ai-llms-explainer#:~:text=While%20LLMs%20represent%20just%20one,%2C%20computer%20code%2C%20and%20more. (Última consulta: 18 de marzo de 2025).

[15] *Vid*. Colorado State University Global, "How Does AI… *op. cit.*. para entender algunos usos de la IA en la vida cotidiana; entre otros, recomendaciones en páginas de compra, verificaciones CAPTCHA en la web, o usos en áreas como las finanzas o la sanidad.

Finalmente, es importante entender que los sistemas de la IA, y los resultados que dan, son en sí mismos neutros. Sin embargo, la calidad de los datos proporcionados influye directamente en el comportamiento de la tecnología. Las posibilidades de tener mecanismos de IA sesgados, discriminatorios, o simplemente erróneos dependen de la información que se le da al sistema. Un ejemplo claro es uno que afecta alrededor del 50% de la población en cualquier lugar del mundo: los sistemas de IA con datos sesgados en contra de las mujeres. Si los datos de base carecen de información proporcionada por mujeres, la IA aprenderá de ello para regurgitar esos mismos sesgos en sus respuestas[16]. Estas realidades, aplicadas a nivel del Derecho internacional, son una consideración importante para el uso estatal de la IA y los posibles riesgos de sesgos o discriminación en la práctica.

2. Funciones de la IA en la práctica estatal

A través de esta investigación, este trabajo analiza dos funciones de la IA en su implementación en el Derecho internacional, y en particular en su relación frente al apoyo a la comisión de posibles HII. Primero, se determina que la IA tiene una *función catalizadora*[17], actuando como agente multiplicador y propagador. Con esta función, la tecnología permite a los Estados mejorar prácticas y actividades ya existentes, lo que permite cometer los mismos HII que se hayan podido realizar anteriormente pero de una manera impulsada o bien a mayor escala. En segundo lugar, la IA tiene una *función creadora*, siendo capaz de fomentar la innovación de tecnologías y métodos para la posible comisión de HII. Esto se observa en la creación de sistemas y prácticas estatales que simplemente no existían antes de la entrada en acción de la IA.

Ambas funciones suelen presentarse juntas, o existir paralelamente, en varios aspectos del Derecho internacional. Poder diferenciar entre ellas es sin embargo clave a la hora de analizar el rol de la IA en el impulso a HII, y por lo tanto el percibido Estado de Derecho internacional. Igualmente, se ha de notar que las funciones de la IA se pueden observar también en usos positivos hacía el cumplimiento de obligaciones internacionales, como demuestra el Capítulo I a continuación.

Se ha de notar igualmente que la función creadora de la IA es la más popular en conversaciones jurídicas actuales, en la prensa o en análisis académicos como la literatura

[16] Universidad Complutense de Madrid, *Certificado en Inteligencia Artificial… op. cit.*
[17] El término se usa jurídicamente aquí como en el texto de R. de la C. Hernández Rodríguez, "El amparo constitucional. Herramienta catalizadora de la función judicial en la nueva Constitución cubana", en *Cadernos de Dereito Actual*, n.º 12, 2019, p. 194-226.

revisada. Mientras que el aspecto de innovación y la preocupación por la regulación de herramientas completamente nuevas es claramente importante, este trabajo argumenta que tiene ligeramente menos relevancia que la función catalizadora de la IA a la hora de revisar la legislación existente y las prioridades en las cuales se ha de enfocar el Derecho internacional.

Este trabajo es de pequeña envergadura comparado con el análisis detallado que se puede hacer de cada uno de los temas expuestos. Por lo tanto, el ámbito de esta obra es servir de observación conjunta jurídica de estos conceptos, reconociendo la necesidad de profundizar en cada uno de ellos con expertos en sus respectivas materias. El tema de la IA no cesará de ser relevante en Derecho internacional, y necesita atención continua particularmente de juristas y académicos de derecho para regularla. Ante todo, se ha de reconocer que "la tecnología no se puede 'desinventar'"[18], y que las problemáticas aquí expuestas continuarán siendo temas de estudio relevantes hasta que se aborden jurídicamente en su totalidad.

[18] E. Dans, "Facial recognition is here to stay, but can we control its use?", disponible en https://www.forbes .com/sites/enriquedans/2020/06/11/facial-recognition-is-here-to-stay-but-can-we-control-itsuse/ (última consulta: 3 de febrero de 2025).

II. METODOLOGÍA

Con la intención de hacer de este trabajo una herramienta analítica, y no un simple informe del uso de la IA en Derecho internacional, esta investigación sigue pautas de metodología jurídica establecidas para responder a las cuestiones relevantes. De acuerdo con las definiciones publicadas por la Universidad de Chile, este es un estudio de carácter descriptivo y una investigación documental[19] en su mayoría. Esto se debe no solo a la centralización en observaciones de actuaciones y propuestas normativas ya realizadas (aunque recientemente) en el marco de la comunidad internacional, sino también a la dificultad que supondría realizar una investigación de campo y/o experimental[20] a esta escala.

Este trabajo se fundamenta adicionalmente en una investigación metodológica más que epistemológica según la distinción abordada en el campo científico[21]. Los resultados de la IA tratándose de hechos relativamente nuevos en el Derecho internacional, existen a fecha de presentación de este trabajo varias preguntas sin respuesta. Por lo tanto, el análisis de la explicación de los hechos se concibe como un paso futuro, una vez esta tecnología emergente se vea acostumbrada a la regulación nueva y pendiente en el Derecho internacional.

Finalmente, el interés metodológico central es la referencia a la teoría de la tridimensionalidad del derecho[22]. Relacionado con las cuestiones jurídicas vistas en el epígrafe a continuación, la separación del texto es conforme con el análisis tripartita del hecho, el valor y la norma[23]. El Capítulo I ("La inteligencia artificial y su impacto sobre los intereses de los Estados y el cumplimiento de sus obligaciones internacionales") engloba el elemento del valor, señalando así la *razón de ser* de la IA en la comunidad internacional. El Capítulo II ("Hechos internacionalmente ilícitos y las funciones de la inteligencia artificial en su impulsión") hace referencia al hecho del uso de la IA en la práctica. Finalmente, el Capítulo III ("Regulación actual de la inteligencia artificial en Derecho internacional") se refiere a las normas existentes en la comunidad internacional y sus limitaciones. Con este análisis, se abordan las cuestiones jurídicas y en torno los objetivos mencionados a continuación, para formular el argumento de este trabajo.

---

[19] G. Álvarez Undurraga, *Metodología de la investigación jurídica: hacia una nueva perspectiva*, Universidad Central de Chile, Santiago, 2002, p. 32-33.
[20] *Ibid*., y por el hecho que supondría observar en tiempo real la comunidad internacional, y/o someterla a experimentos jurídicos de una dimensión inapropiada para los recursos de este trabajo.
[21] M. Sánchez Zorrilla, "La metodología en la investigación jurídica: características peculiares y pautas generales para investigar en el derecho", en *Revista Telemática de Filosofía del Derecho*, n.º 14, 2011, p. 322-323.
[22] G. Álvarez Undurraga, *Metodología… op. cit.*, p. 25.
[23] *Ibid*., p. 26.

1. Cuestiones jurídicas vinculadas

En conjunto con los objetivos expuestos a continuación, se señalan varias cuestiones jurídicas vinculadas con este análisis de la regulación internacional de la IA. Concretamente, se analizan las siguientes:

I. ¿Cómo utilizan los Estados aplicaciones de IA para cumplir e incumplir sus obligaciones bajo el Derecho internacional en la práctica? En particular, como el título del trabajo indica, esta obra se centrará en el análisis relacionado con los HII según aparecen definidos por el *Proyecto de Artículos sobre la responsabilidad del Estado por Hechos Internacionalmente Ilícitos*, adoptado por la Comisión de Derecho Internacional en 2001[24]. Particularmente, se adentrará brevemente en la cuestión sobre la personalidad jurídica de la IA, y así la atribución relativa de su comportamiento a un Estado concreto.

II. ¿Cuáles son las limitaciones principales entre el Derecho actual vigente y la práctica ilícita de los Estados? Vinculando así la señalización de estos obstáculos con el argumento principal del trabajo, la investigación se fundará en analizar la regulación existente y la necesaria para mantener la paz y la colaboración propia del Derecho internacional[25].

III. ¿Cuáles son los riesgos planteados por la IA a lo que podría ser el Estado de Derecho internacional? Mientras que esta cuestión no será tratada en su totalidad, ya que el rápido desarrollo de la IA no permite limitar su análisis a este humilde trabajo, idear los riesgos mayores frente al Estado de Derecho internacional[26] es una consideración importante en la examinación de esta nueva tecnología en el contexto de HII.

2. Revisión de la literatura

La IA y su rol en la responsabilidad de los Estados en el marco del Derecho internacional ya ha sido objeto de investigación en varias ocasiones, por lo que resulta imprescindible conocer el marco literario que ya ha tratado de este tema. En 2020, el CEI International Affairs, la escuela diplomática de Barcelona, publicó en 2020 un trabajo de fin de máster sobre la responsabilidad estatal frente la IA, titulado “International Responsibility

[24] Comisión de Derecho Internacional, *Proyecto de Artículos sobre la responsabilidad del Estado por Hechos Internacionalmente Ilícitos* (2001).
[25] J. A. Perea Unceta, "Reflexiones sobre las restricciones a la soberanía del Estado en el Derecho Internacional contemporáneo", en *Anuario Jurídico y Económico Escurialense*, vol. XXXVII, 2004, p. 119.
[26] *Vid*. J. Ruiz Valerio, *El Estado de derecho internacional. Una aproximación cartográfica a su definición*, p. 35. Repositorio Universitario - Jurídicas de la UNAM, disponible en http://ru.juridicas.unam.mx:80/xmlui/handle/123456789/32432 (última consulta: 15 de marzo de 2025).

of States and Artificial Intelligence"[27]. Esta investigación examina la aplicabilidad del PA 2001 en los sistemas autónomos letales en particular, y concluye que la responsabilidad estatal es en estos casos "intrincada" sobre todo dado a la "falta general de disposiciones legales que aborden específicamente la IA"[28]. En comparación, este trabajo irá más allá que el análisis del CEI por su revisión de una mayor variedad de HII posibles mediante IA, no solo los sistemas autónomos letales. Igualmente, se analizarán disposiciones legales que se han aplicado a la comunidad internacional después de esta publicación del CEI.

La *Revista Húngara de Estudios Jurídicos* publicó en junio de 2022 un corto estudio sobre la personalidad legal y posible regulación de la IA en Derecho internacional**[29]**. Pese a incluir varias de las cuestiones jurídicas antes mencionadas, esta investigación carece igualmente del amplio conocimiento que vino a la disciplina después de su fecha de publicación. Esto incluye como ejemplo predominante la existencia de un tratado internacional sobre el uso de la IA, cuya hipotética creación se considera "utópica" en el texto[30]. La conclusión de este estudio tiene un enfoque en gran parte pesimista sobre la capacidad del Derecho internacional de regular la IA adecuadamente, considerando que esta se está desarrollando a un ritmo "prácticamente nunca visto"[31]. Esta perspectiva pesimista se matiza en este nuevo análisis, habiendo observado ya intentos exitosos de creación normativa. No obstante, se apoya la necesidad de ir más allá de lo existente, reforzando la idea que el ritmo de desarrollo de la tecnología representa un reto para el Derecho internacional.

En su *Revista Estudios en Derecho a la Información* de julio-diciembre 2022, la Universidad Nacional Autónoma de México publicó en 2022 un artículo titulado "La inteligencia artificial y la responsabilidad internacional de los estados"[32]. Esta publicación tiene un enfoque similar al trabajo del CEI ya mencionado; analiza en este caso la aplicación de responsabilidad del Estado en usos de la IA en general, pero sobre todo el punto de la creciente autonomía de la IA y del potencial de desviarse del control humano. Este tema de

---

[27] B. Pino, *International Responsibility of States and Artificial Intelligence*, CEI, Centro Adscrito a la Universitat de Barcelona, 8 de mayo de 2020, disponible en https://diposit.ub.edu/dspace/bitstream/2445/170430/1/TFM_Beatriz_Pino.pdf (última consulta: 20 de abril de 2025).
[28] *Ibid*., p. 43.
[29] A. Hárs, 'AI and international law – Legal personality and avenues for regulation*"*, en *Hungarian Journal of Legal Studies*, vol. 62, n.º 4, 2022, p. 321.
[30] *Ibid*., p. 335.
[31] *Ibid*., p. 339.
[32] J.S. Viveros Álvarez, "La inteligencia artificial y la responsabilidad internacional de los Estados", en *Revista Estudios en Derecho a la Información*, n.º 14, julio-diciembre de 2022, p. 83-105.

responsabilidad estatal se tratará de nuevo en menor parte en este trabajo para completar el argumento sobre el rol de la IA en HII.

En noviembre del 2022, las publicaciones de la Universidad de Cambridge compartieron un artículo sobre la responsabilidad estatal concretamente sobre las aplicaciones de la IA para uso militar[33]. En diciembre de ese mismo año, la universidad volvió a publicar sobre el tema en su prensa en línea, esta vez con enfoque en los sistemas autónomos letales[34]. Ambas publicaciones son relativamente limitadas en su enfoque, e igualmente precedentes a las regulaciones de la Unión Europea (UE) o del Consejo de Europa (CdE).

Este último argumento de precedencia a cambios legislativos llega a ser el más importante a la hora de invocar la necesidad de emprender este trabajo de investigación. El progreso técnico y la diversidad de aplicaciones de la IA están expandiéndose con inmensa velocidad; esto es sin duda un hecho nefasto para la publicación de investigación jurídica, la cual requiere cierto detenimiento a la hora de revisar y analizar la situación existente. Es sin duda una razón por la cual no se han publicado gran número de trabajos tratando sobre esta temática en particular desde 2022. Trás ello, se han publicado varios textos teniendo que ver con la legislación de la IA, pero con enfoques concretos diferentes como los derechos humanos[35] o la ayuda humanitaria en las organizaciones internacionales[36]. Paradójicamente, se trata entonces de una apertura necesaria para la realización de este trabajo en este campo. Con esto en mente, esta revisión de literatura combinada con actuaciones legislativas presentes se hará lo más eficientemente posible, para contribuir a la disciplina sin detenimiento.

3. Objetivos

Más allá de brindar una respuesta general a las cuestiones jurídicas planteadas en el Derecho internacional vigente, este trabajo sigue las conclusiones de la literatura mencionada anteriormente. Los fines de esta investigación se definen por lo tanto como:

[33] B. Boutin, “State responsibility in relation to military applications of artificial intelligence”, en *Leiden Journal of International Law*, vol. 36, n.º 1, 2023, p. 133-150.
[34] M. Pacholska, “Military Artificial Intelligence and the Principle of Distinction: A State Responsibility Perspective”, *Israel Law Review*, vol. 56, n.º 1, 2023, p. 3-23.
[35] I. Artíñano Ortiz, M. Balcerzak y J. Kapelańska-Pręgowska, Eds. 2024., “Artificial Intelligence and International Human Rights Law. Developing Standards for a Changing World”, en *Deusto Journal of Human Rights*, n.º 14, diciembre 2024, p. 377-384.
[36] M.T. Veber., "International Organizations and AI-Supported Humanitarian Aid: Navigating through the Applicable (Data Protection) Legal Regimes.", en *International and Comparative Law Review*, vol. 24, no. 2, Sciendo, 2024, p. 54-83.

I. Objetivo primero: reforzar el análisis académico de las funciones de la IA en su apoyo a la posible comisión de HII de parte de los Estados que la utilizan, para determinar la necesidad de la creación de obligaciones internacionales específicas frente a estas.

II. Objetivos secundarios: 1) demostrar la necesidad de textos jurídicos que alcancen el uso de la IA en el ámbito militar, de defensa, y de seguridad nacional en vez de asumir suficiente el derecho internacional existente, y 2) analizar los riesgos planteados la IA para la formación y fomento de lo que llegaría a ser el Estado de Derecho internacional.

Mientras que la envergadura de este trabajo no será la suficiente para producir la totalidad de las respuestas a las líneas de investigación que plantean estos objetivos, la intención dominante es avanzar soluciones a problemas actuales y próximamente materializables en el Derecho internacional.

III. LA INTELIGENCIA ARTIFICIAL Y SU IMPACTO SOBRE LOS INTERESES DE LOS ESTADOS Y EL CUMPLIMIENTO DE SUS OBLIGACIONES INTERNACIONALES

La teoría de la tridimensionalidad del derecho enfatiza la importancia de valor en la creación del ámbito jurídico[37]. Para poder explorar la regulación de la IA a nivel del Derecho internacional, es imprescindible adentrarse primero en los intereses de los Estados en la tecnología. En otras palabras, se ha de analizar el valor aportado por la IA a la práctica política de los sujetos primeros de esta rama del Derecho. Con el deber de este trabajo de mantener un enfoque jurídico, este primer Capítulo revisa por lo tanto los intereses estatales en la IA en el marco del cumplimiento de las obligaciones internacionales resultantes de las normas que contratan los propios Estados. Al poderse considerar que el seguimiento de estas es en sí mismo un interés estatal para la existencia en comunidad internacional, vemos a continuación la demostración del valor de la tecnología en ello.

Pese a gozar en el Derecho internacional contemporáneo de una existencia en comunidad, los Estados mantienen, desde su creación, intereses propios. Aunque un interés nacional reconocible sea el de promover un entorno pacifico y conforme a normas establecidas[38], los Estados mantienen objetivos individuales para su propia supervivencia y desarrollo. Estos intereses se agrupan en política internacional en dos categorías centrales: primero, el fomento de soberanía, para "garantizar la supervivencia, seguridad…y la defensa"[39], y secundariamente (pero con estrecha relación) lo asociado con el avance del Estado, concretamente "la búsqueda de poder, riqueza y crecimiento económico"[40].

En ambos de estos campos de intereses, que existen en equilibrio con el cumplimiento de obligaciones internacionales, la IA realiza las dos funciones establecidas anteriormente para su empleo positivo. Los Estados gozan de sus contribuciones a la revolución y propulsión de la práctica ya existente, por lo que la IA cumple su función catalizadora facilitando y promoviendo exponencialmente usos existentes. Igualmente, los intereses estatales son fomentados trás el uso de la tecnología para propósitos completamente nuevos, aprovechando la función creadora de la IA. A continuación, se demuestra que el uso de la IA

[37] G. Álvarez Undurraga, *Metodología… op. cit.*, p. 25. Véase igualmente Universidad Nacional Autónoma de México, *Teoría Tridimensional del Derecho*, disponible en https://repositorio-uapa.cuaed.unam.mx/repositorio/moodle/pluginfile.php/1466/mod_resource/content/4/contenido/index.html (última consulta: 7 de abril de 2025).
[38] R. Herrero, "Política exterior de España e intereses nacionales", en *UNISCI Discussion Papers*, n.º 27, octubre 2011, p. 88.
[39] Ídem.
[40] Ídem.

para los intereses estatales es así capaz de impulsar el cumplimiento de obligaciones internacionales relacionadas, y el apoyo a una comunidad internacional pacífica.

1. Soberanía y seguridad estatal

La soberanía es reconocida como la fundación del Derecho internacional[41]; los Estados y su consentimiento respectivo son imprescindibles para el mecanismo propio de las obligaciones internacionales que deciden contratar. La soberanía es sin embargo también un interés esencial de los Estados, que motiva intrínsecamente sus actuaciones. Este concepto de Derecho internacional que se conoce hoy en día es efectivamente "fruto de una tensión permanente"[42] entre las obligaciones internacionales que benefician a la comunidad en total y el foco de soberanía que mantienen los Estados.

El rol de la IA en el fomento de la soberanía es mejor identificado observando tres principios estructurales del Derecho internacional que se ven particularmente influenciados por y relacionados a esta: el de no injerencia, el de la prohibición del uso de la fuerza, y el de la resolución pacífica de controversias. Aunque la IA alcanza muchos más principios y obligaciones específicas del Derecho internacional, se registra en estos tres enfoques el claro impacto positivo de esta tecnología, particularmente en lo que interesa a los Estados.

1.1. Principio de no injerencia

Empezando por el principio estructural de Derecho internacional de la no injerencia en los asuntos internos o externos de otros Estados, el interés soberano es evidente: que cada Estado pueda seguir sus propio *modus operandi* dentro de su territorio. Vemos entonces las controversias territoriales como gran consideración soberana desde hace siglos[43], pero el principio de no injerencia queda aplicado sobre todo a las actividades y los desarrollos dentro del territorio soberano de un Estado en sí. De ello nace la obligación general homónima al mismo principio, la cual se recoge más conocidamente en los Artículos 2.4 y 2.7 de la *Carta*

[41] L. Bence Márquez y T. Diéguez La O, "Soberanía e inmunidad del Estado. Reflexiones a la luz del Derecho Internacional", en *Política Internacional*, vol. 6, núm. 1, 2024, Instituto Superior de Relaciones Internacionales "Raúl Roa García", Cuba, p. 144.
[42] J. A. Perea Unceta, "Reflexiones sobre las restricciones… *op. cit.*, p. 98.
[43] A.G. López Martín, "Principios y reglas de solución aplicables a las controversias territoriales a la luz de la jurisprudencia de la Corte Internacional de Justicia", en *Anuario Colombiano de Derecho Internacional,* Vol.6, 2013, p. 16.

de las Naciones Unidas del 26 de junio de 1945[44] y en el Artículo 8 de la *Convención sobre Derechos y Deberes de los Estados del 26 de diciembre de 1933*[45], entre otros textos.

Vemos aquí que la IA se utiliza en este ámbito estatal no para cumplir necesariamente con la obligación de no injerir o intervenir, si no con el interés opuesto de *no recibir* injerencia ajena. Aunque este último punto puede efectivamente considerarse no ser una obligación estatal, cabe señalar que la soberanía se ha visto en Derecho internacional estudiada como un posible deber de los Estados[46].

En cualquier caso, el papel de la IA en la defensa del interés soberano es notable. Se ven contribuciones sustanciales a programas de defensa y seguridad estatal que ya existían, apelando a la función catalizadora de la IA. Sin embargo, analizamos igualmente la función creadora de esta en el impulso de nuevos sistemas enteramente. Se observa en ambos casos el uso de la IA para vigilar lo que llegan a ser tres fronteras estatales: las delimitaciones físicas, la del espacio cibernético, y potencialmente la de la información.

Al utilizar el término de fronteras físicas, se entienden las vías terrestres, marítimas y aéreas, como así indica por ejemplo el Artículo 3(d) de la Resolución 3314 de la Asamblea General de la ONU[47] al hablar de actos de agresión. En estas tres fronteras, la IA cumple sobre todo su función catalizadora, mejorando y profundizando prácticas que se hubieran realizado antes de forma manual o con tecnología de generaciones previas. Existen en la actualidad muchas aplicaciones de la IA siendo exploradas a nivel mundial. En la UE, por ejemplo, se estaba en 2021 “explorando activamente” sus usos para seguridad regional y el control de las fronteras según un informe del Servicio de Investigación del Parlamento Europeo[48]. Hoy en día, los resultados se observan a través de usos predecidos, como por ejemplo el sistema de vigilancia de fronteras EUROSUR donde la IA aplica para obtener una imagen “óptima” de las tres fronteras[49]. Cabe destacar que además de estas nuevas implementaciones la Agencia Europea de la Guardia de Fronteras y Costas (también conocida

[44] Tratado entrado en vigor el 24 de octubre de 1945, publicado en la Colección de Tratados de las Naciones Unidas (registro s/n).
[45] Tratado entrado en vigor el 26 de diciembre de 1934, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 3802).
[46] A. Etzioni, “Sovereignty as Responsibility”, en *Orbis*, vol. 50, n.º 1, invierno 2006, p. 71.
[47] Asamblea General de las Naciones Unidas, Resolución 3314 (XXIX), Doc. A/RES/3314 (1974).
[48] C. Dumbrava, *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues*, Member’s Research Service, p. 10, disponible en https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf (última consulta: 27 de abril de 2025).
[49] A. Andreou, "e-Securing the EU Borders: AI in European Integrated Border Management", en *Journal of Politics and Ethics in New Technologies and AI*, vol. 2, n.º 1, 2023, p. 9.

como Frontex) continúa buscando aplicaciones, anunciando en febrero del 2025 un Día de la Industria dedicado a presentaciones de nuevas tecnologías IA para uso en puntos de cruce en fronteras europeas[50].

Para los cruces terrestres en particular, existen varias revisiones específicas en puntos de acceso estatales como los pasos de coches o la entrada a aeropuertos. En este respecto, el Departamento de Seguridad Nacional en Estados Unidos publicó en 2024 un reporte informativo para fomentar el uso ético de la IA en materia de su seguridad nacional[51]. Identifica en este la implementación en continuo desarrollo de la tecnología en sus aduanas y protección fronteriza, concretamente pasajes de vehículos y revisión por su Administración de Seguridad de Transporte presente en aeropuertos (TSA, por sus siglas en inglés)[52]. El Departamento promueve en particular el uso de la IA para mejorar un sistema de "inspección no intrusiva" capaz de detectar contrabando de fentanilo y otras "anomalías" con mejor precisión[53]. Estas aplicaciones son un claro ejemplo de la función catalizadora, ya que ambos la "inspección no intrusiva" y la detección de objetos se consiguen mediante el uso de tecnologías más antiguas, como las imágenes de rayos X, desde los años setenta[54]. La IA permite a las agencias estatales en este caso mejorar la precisión de los sistemas con el uso de datos generados por los mismos[55], lo que se entiende también como una reducción de tiempo dedicado por el personal en la revisión de imágenes.

Igualmente en cuanto a la vía terrestre, un estudio malasio de 2024 analizó tres beneficios inmediatos de la implementación de la IA en la frontera entre Malasia y Tailandia. Esto incluiría utilizar tecnologías de reconocimiento facial, "tecnología de detección de intrusiones" más moderna, y drones con detección térmica[56]. El plan se elabora como respuesta al alto volumen del contrabando y inmigración irregular sucediendo en la frontera

---

[50] Véase anuncio en la pagina web frontex.europa.eu por Frontex, *Industry Day on Artificial Intelligence Tools for Seamless Border Checks at European Border Crossing Points*, 23 de enero de 2025, disponible en https://www.frontex.europa.eu/innovation/announcements/industry-day-on-artificial-intelligence-tools-for-seamless-border-checks-at-european-border-crossing-points-lUTEhX (última consulta: 18 de febrero de 2025).
[51] Departamento de Seguridad Nacional de los Estados Unidos, *Artificial Intelligence Roadmap*, 15 de marzo de 2024, disponible en https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificial intelligence-ciov3-signed-508.pdf (última consulta: 18 de febrero de 2025).
[52] *Ibid.*, p. 4.
[53] *Ibid.*, p. 14.
[54] O. E. Wetter, "Imaging in Airport Security: Past, Present, Future, and the Link to Forensic and Clinical Radiology", en *Journal of Forensic Radiology and Imaging*, vol. 1, n.º 4, 2013, p. 153.
[55] Departamento de Seguridad Nacional de los Estados Unidos, *Artificial Intelligence Roadmap… op. cit.*, p. 14.
[56] N. Md Nor, *et. al*., "Leveraging Artificial Intelligence (AI) Technology for Enhanced Border Surveillance at the Malaysia-Thailand Land Border", en *e-Bangi: Journal of Social Sciences & Humanities*, vol. 21, n.º 4, 2024, p. 61.

entre los dos países[57]. La Agencia de Control y Protección Fronteriza se estableció pocos meses después de la publicación de ese estudio[58]. En la conferencia de prensa para su inauguración, el viceprimer ministro malasio Fadillah Yusof comentó específicamente el uso de la IA en la organización para mejorar cruces fronterizos en la región de la Asociación de Naciones de Asia Sudoriental (más conocida por sus siglas en inglés, ASEAN)[59].

Las vías marítimas se benefician adicionalmente de protección cada vez más entrelazada con IA. La Agencia Espacial Europea expuso en julio de 2024 sus aplicaciones de la IA en la tecnología de su misión inminente, usos que incluyen la generación de mapas basados en imágenes satelitales y la detección y clasificación de buques para fomentar la "seguridad marítima". Pese que menciona el uso específico contra la pesca ilegal[60], se entiende que esta tecnología es directamente aplicable a la vigilancia de cruce de fronteras marítimas y de aguas territoriales. Esto es lo que hizo por ejemplo el proyecto AI-ARC, que creó una sala de control virtual para las fronteras del Ártico y "validó" varias herramientas de control para "detección automática de anomalías" impulsadas por la IA[61]. Según reportes oficiales de la UE, el proyecto acabó progresando más allá del *state of the art* tecnológico en sus varias aplicaciones.[62]

Finalmente, las vías aéreas se ven afectadas igualmente por la IA con enfoque particular a este tipo de fronteras. Las zonas de cruce se ven cada vez más impactadas por monitoreo por vehículos aéreos que gozan de IA y sensores para analizar datos al momento[63] y prevenir intrusiones aéreas. Esto es comparable a lo que harán los drones de la Agencia Espacial Europea con su habilidad de comprimir imágenes y acelerar la recogida de

---

[57] *Ibid.,* p. 54.
[58] Segun un periodico malasio ″AKPS will ensure smooth, efficient border control, says DPM Fadillah″, *The Sun Daily*, 2 de febrero de 2025, disponible en https://thesun.my/malaysia-news/akps-will-ensure-smooth-efficient-border-control-says-dpm-fadillah-HE13605507 (última consulta: 18 de febrero de 2025).
[59] Segun una publicación vietnamita "Malaysia streamlines border control and protection forces", *Vietnam+*, 3 de febrero de 2025, disponible en https://en.vietnamplus.vn/malaysia-streamlines-border-control-and-protection-forces-post309212.vnp (última consulta: 18 de febrero de 2025).
[60] European Space Agency, *New satellite to show how AI advances Earth observation*, 2 de julio de 2024, disponible en https://www.esa.int/Applications/Observing_the_Earth/Phsat-2/New_satellite_to_show_how_AI_advances_Earth_observation (última consulta: 3 de febrero de 2025).
[61] CORDIS, *The Next Generation of Maritime Awareness and Surveillance*, disponible en https://cordis.europa.eu/article/id/452691-the-next-generation-of-maritime-awareness-and-surveillance (última consulta: 18 de febrero de 2025).
[62] CORDIS, *Periodic Reporting for Period 2 - AI-ARC (Artificial Intelligence based Virtual Control Room for the Arctic (AI-ARC))*, periodo de reporte: 2022-09-01 a 2024-02-29, disponible en https://cordis.europa.eu/project/id/101021271/reporting (última consulta: 18 de febrero de 2025).
[63] L. Arya, *et. al*., "Eyes in the Sky: Safeguarding Borders Security with AI-Powered Aerial Monitoring and IoT Integration", en *Proceedings of International Conference on Recent Innovations in Computing* (ICRIC 2023), vol. 2, en Z. Illés, *et. al.* (eds.), *Lecture Notes in Electrical Engineering*, vol. 1195, Springer, Singapur, 2024, p. 863-873.

información por vía aérea[64]. La IA cumple efectivamente el interés estatal de mejorar la protección de su espacio aéreo, permitiendo así conservar su soberanía sobre este.

Aunque las fronteras físicas sean las dominantes en la consideración del principio de no intervención, resulta importante destacar el rol de las fronteras digitales hoy en día y su estrecha relación con la IA. El ciberespacio en su creación como plataforma global no fue liderado por ningún Estado en particular[65], lo que se traduce actualmente en "retos continuos" para cada gobierno a la hora de controlar la actividad cibernética[66] y lo que se comparte dentro de su territorio. Esto resulta evidente especialmente cuando actividades estatales se llevan a cabo mediante plataformas digitales, como es el caso visto a continuación de las elecciones. Por lo tanto, entendiendo las fronteras digitales como los límites de los asuntos de otro Estado—en los que el principio de no intervención marca una clara línea roja—la IA facilita la protección de estas.

En el caso entonces de las elecciones, esta tecnología puede influir en un Estado de varias maneras. Teniendo en cuenta la peligrosidad de un ciberataque en el sistema electoral de un Estado, como fueron víctimas en años recientes la comisión electoral del Reino Unido[67] o el gobierno federal de Estados Unidos[68], la IA cumple ambas de sus funciones de apoyo a la violación del principio de no intervención; puede ser utilizada para reducir costes y tener mayor alcance en ciberataques[69], y permite crear nuevas herramientas perjudicadoras[70] cómo expuesto a continuación. No obstante, la IA puede ser también utilizada para *prevenir* ataques cibernéticos, como indicó el Centro de Ciberseguridad Nacional del Reino Unido en 2024. En un informe, este afirma que aunque los ciberataques ayudados por la IA en el país se multiplicarán en los dos próximos años, esto "será contrarrestado por el uso de la IA para

---

[64] European Space Agency, *New satellite… op. cit.*
[65] P. de Miguel Asensio, *Conflict of Laws and the Internet*, *Elgar Information Law and Practice series*, Edward Elgar, 2020, p. 2.
[66] *Ibid.,* p. 4.
[67] Ciberataque identificado en octubre 2022, por Electoral Commission, *"Information about Cyber Attack on Electoral Commission Systems"*, última actualización: 30 de julio de 2024, disponible en https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems/information-about-cyber-attack (última consulta: 21 de febrero de 2025).
[68] Interferencia atribuida a Rusia, segun el reporte estadounidense por Senate Select Committee on Intelligence, *Report of the Select Committee on Intelligence on Russian Active Measures* (vol. 5), disponible en https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf (última consulta: 21 de febrero de 2025).
[69] Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, *Consolidated Risk in Focus: Gen AI and Elections*, 18 de enero de 2024, disponible en https://www.cisa.gov/sites/default/files/2024-05/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf (última consulta: 20 de abril de 2025).
[70] J. Kenny, *Advanced Artificial Intelligence Techniques and the Principle of Non-Intervention in the Context of Electoral Interference*, Routledge, 2023, p. 235.

mejorar la resiliencia de la ciberseguridad"[71]. Esto se debe al uso de la misma tecnología para mejorar la seguridad de los sistemas, así como la detección de riesgos. Aunque esta fuente dice que se necesita más investigación para entender las máximas capacidades de este último punto[72], la implementación de la IA para asegurar la ciberprotección de servicios del gobierno está siendo investigada a tiempo real[73].

Finalmente, podemos considerar lo que sería la *frontera de la información*. Se trataría del límite teórico en el que un Estado sería capaz de controlar la información dada a sus ciudadanos dentro de su propio territorio, basándose en el interés que podrían tener en ello[74]. Siendo esta estrechamente relacionada con la del ciberespacio—al ser una mayoría de la información estatal en línea hoy en día—estas dos fronteras se pueden presentar en conjunto. Se ha de distinguir sin embargo lo que son las capacidades cibernéticas de un Estado en comparación con su habilidad de diseminar información (potencialmente en formato físico y no digital) entre su población. El análisis, aún así, se centra en la violación y protección de esta potencial frontera de manera exclusivamente digital.

En el caso de las elecciones, de nuevo, la IA ha demostrado nuevas maneras de intervenir en asuntos ajenos, así como usos interesantes para proteger contra eso mismo. Como primer ejemplo, el Estado queriendo intervenir puede utilizar la IA para la creación de *bots* en grandes cantidades, siendo estas cuentas falsas que puedan inflar una falsa impresión sobre el apoyo dado a ciertas opiniones. La IA permite igualmente la nueva proliferación de *deepfakes*, o videos falsos en parte o en su totalidad, demostrando en general información errónea que pueda influir políticamente en la población.[75] Para combatir ambos, sin embargo, se ha popularizado el uso de la IA contra la no intervención en su integración en *fact checkers*, o sistemas de verificación de hechos. Para combatir la injerencia extranjera en los sistemas de información, por ejemplo, la UE introdujo EUvsDisinfo[76], una base de artículos

[71] National Cyber Security Centre, *The Near-Term Impact of AI on the Cyber Threat*, 24 de enero de 2024, disponible en https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat (última consulta: 21 de febrero de 2025).
[72] Ídem.
[73] *Vid*. un artículo de R. K. Jha y M. Jha, "Optimizing E-Government Cybersecurity through Artificial Intelligence Integration", en *Journal of Trends in Computer Science and Smart Technology*, vol. 6, n.º 1, 2024, p. 67-87. al igual que un informe para el gobierno de Indonesia sobre el rol de la IA en su estrategia de ciberseguridad R. A. Gati, M. Rizki y R. Y. Posumah, *"Artificial Intelligence and Indonesia Government Cyber Security Strategies"*, en *International Conference on Public Organization*, 2020.
[74] S. Powers, *Towards Information Sovereignty*, en W. J. Drake y M. Price (eds.), *Beyond Netmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem*, University of Pennsylvania, agosto 2014, p. 90.
[75] J. Kenny, *Advanced Artificial Intelligence… op cit.*, p. 235.
[76] El proyecto EUvsDisinfo esta disponible en https://euvsdisinfo.eu/ (última consulta: 7 de febrero de 2025), y ha de no ser confundido con EU DisinfoLab, una ONG que también combate la desinformación y introduce

determinados como propaganda en comparación con información verificada. La Universidad de Sheffield se comprometió en 2022 a demostrar las avenidas del uso de esos datos como entrenamiento para sistemas de IA, que puedan en torno distinguir más información.[77]

Adicionalmente, algunos gobiernos enfatizan la utilización de la IA para proveer información directamente a los votantes, resaltando su "lado bueno" como la comunicación que alega la comisión electoral de Australia para la "inclusión de votantes" con materiales educativos[78]. Este último punto resalta el uso de la IA para mantener la soberanía de un Estado; sí bien se puede utilizar esta tecnología para promover propaganda y perspectivas ajenas, el propio Estado puede utilizarla para avanzar información de sus propias fuentes dentro de su territorio.

El conjunto de estas aplicaciones por todas las fronteras físicas de un país contribuye a su interés soberano, incrementando de tal manera su habilidad de prevenir injerencia ajena en sus asuntos internos. La otra cara de la moneda es sin embargo la creciente responsabilidad de los Estados de no utilizar estas aplicaciones de la IA para involucrarse ellos mismos en los asuntos de otros Estados, como expone el Capítulo II.

1.2. Prohibición de uso de la fuerza y resolución pacífica de controversias

Otros dos principios estructurales del Derecho internacional, el de prohibición del uso o amenaza de la fuerza así como la resolución pacífica de controversias, se ven apoyados por la IA a la hora de su cumplimento. Ambos principios se presentan juntos al estar estrechamente relacionados; sus mecanismos se entrelazan en la práctica, creando un conjunto indivisible[79] en el cual la IA tiene un papel similarmente reflejado.

Empezando por la prohibición del uso de la fuerza, vemos aquí otro principio estructural del Derecho internacional sobre el cual la IA tiene una doble influencia; existen aplicaciones sumamente positivas, al igual que unas negativas que se comentarán a continuación hablando de su rol en HII. En el marco positivo, la IA permite a los Estados más facilidad para cumplir con las obligaciones dimanantes del principio, y así mantener su

vocalmente IA en sus iniciativas https://www.disinfo.eu/ai-against-disinformation/ (última consulta: 7 de febrero de 2025).

[77] K. Bontcheva et al., *"EUvsDisinfo: A Dataset for Multilingual Detection of Pro-Kremlin Disinformation"*, en *Proceedings of the 31st ACM International Conference on Information & Knowledge Management (CIKM '22)*, 2022, p. 5380-5384.

[78] Australian Electoral Commission, *AI & Elections*, última actualización: 10 de febrero de 2025, disponible en https://www.aec.gov.au/Elections/electoral-advertising/ai-and-elections.htm (última consulta: 21 de febrero de 2025).

[79] J. A. Perea Unceta, "Reflexiones sobre las restricciones… *op. cit.*, p. 103.

interés soberano en no utilizar la fuerza. Dicho interés está en la protección de las actividades propias del Estado, que provee el "convivir en paz como buenos vecinos"[80] en el marco internacional.

El principio de no recurrir a la fuerza crea varias obligaciones para los Estados, las cuales el uso de la IA puede ayudar a respaldar. La obligación más evidente sin embargo resta en el Artículo 2.4 de la Carta de la ONU, prohibiendo así a los Estados utilizar la fuerza contra otro o amenazar a tal efecto[81]. Para apoyar este concepto, incluyendo obligaciones más concretas como "el deber de abstenerse de actos de represalia que impliquen el uso de la fuerza"[82], la IA beneficia sobre todo en el análisis de circunstancias. Existen por ejemplo *decision support systems* (en castellano, sistemas de apoyo a la toma de decisiones) impulsados por la IA para asistir a líderes militares con la decisión de utilizar—o no—la fuerza. Estos mecanismos promueven de tal manera elecciones "efectivas, rápidas y legítimas"[83] sobre el uso estatal de la fuerza armada. Mientras esto se puede entender como una promoción del uso de la fuerza en sí misma, es válido ver el argumento opuesto. Estos mecanismos pueden directamente servir para mejorar el cumplimiento de la obligación de abstenerse del uso de la fuerza. La IA puede por ejemplo ayudar a seguir el manejo de recursos del Estado adversario y la implementación de sus estrategias[84]. En el caso de una decisión militar, un Estado que se siente bajo potencial ataque puede utilizar esta tecnología para cuantificar los recursos de la amenaza e idealmente abstenerse de recurrir a la fuerza preventiva sin justificación bajo el Derecho internacional.

Adicionalmente, cabe destacar el papel de la IA en usos activos de la fuerza (o en su conclusión), ya sean dichos usos autorizados o no por el Consejo de Seguridad de la ONU según el Artículo 51 de la Carta. En Derecho internacional humanitario notablemente, la tecnología podría ayudar a suplementar los análisis de cumplimiento de los *Convenios de*

---

[80] J. A. Perea Unceta, "Reflexiones sobre las restricciones… *op. cit.*, p. 103.
[81] El Artículo 2.4 en su totalidad señala en particular uso o amenaza "contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas."
[82] Asamblea General de la ONU, Resolución 2625 (XXV), "Declaración sobre los principios de Derecho Internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas" (1970).
[83] Comité Internacional de la Cruz Roja (ICRC) y Geneva Academy, *Expert Consultation Report on AI and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts*, Ginebra, Comité Internacional de la Cruz Roja, marzo de 2024, p. 8, disponible en https://www.geneva-academy.ch/joomlatools-files/docman-files/Artificial%20Intelligence%20And%20Related%20Technologies%20In%20Military%20Decision-Making.pdf (última consulta: 16 de abril de 2025).
[84] K. Vold, "Human-AI cognitive teaming: using AI to support state-level decision making on the resort to force", en *Australian Journal of International Affairs*, vol. 78, n.º 2, 2024, p. 233.

Ginebra del 12 agosto de 1949 y sus Protocolos adicionales[85] en operaciones militares. En 2017, se utilizó un sistema de IA en Myanmar para analizar imágenes térmicas con el objetivo de identificar puntos prominentes de violencia étnica contra los Rohingyas. Asimismo, en 2018 se emplearon imágenes de satélites tomadas sobre Darfur para cuantificar mediante IA la destrucción de pueblos tras el conflicto[86]. Aunque este último sea un ejemplo de conflicto sin carácter internacional, siendo una guerra civil con moderado involucramiento global, el beneficio de la aplicación de la IA para los Estados es claro. La IA permite así escanear contenido mediático para determinar posibles crímenes de guerra, estimar la proporcionalidad de las armas utilizadas, o incluso calcular daños potenciales a poblaciones civiles[87].

Con respecto a la resolución pacífica de controversias, el interés colectivo del mantenimiento de la paz impone una "obligación de resultado"[88] para los Estados, desviando así el uso indiscriminado de la fuerza. Este fomento de resolución pacífica es de nuevo una requisito que beneficia el interés soberano de los Estados; aunque dependa de un "equilibrio" y de la "limitación progresiva" de dicha soberanía, es un contrapeso esencial para la convivencia internacional y el poder de ejercer la libre voluntad estatal[89] incluso en nuevos desafíos[90]. En estos ámbitos, la IA apoya de varias maneras a la obligación de resolución pacífica. El primer uso destacado de la IA para el fomento de la paz es el análisis de

[85] Los cuatro tratados que componen el total de los Convenios de Ginebra entraron en vigor el 21 de octubre de 1950, y están publicados en la Colección de Tratados de las Naciones Unidas (números de registro 970-973). Los Protocolos adicionales I y II fueron adoptados el 8 de junio de 1977 y entraron en vigor el 7 de diciembre de 1978. Están publicados en la Colección de Tratados de las Naciones Unidas (número de registro 17512 y 17513). El Protocolo adicional III fue adoptado el 8 de diciembre de 2005 y entró en vigor el 14 de enero de 2007. Está publicado en la Colección de Tratados de las Naciones Unidas (número de registro 43425).

[86] A. Dulka, "The Use of Artificial Intelligence in International Human Rights Law", en *Stanford Technology Law Review*, vol. 26, n.º 2, 2023, p. 330.

[87] T. Krupiy, *"What role artificial intelligence could play in evaluating the compliance of military operations with international humanitarian law: The case study of the conduct of hostilities in Ukraine"*, en *EJIL:Talk!, Blog of the European Journal of International Law*, 23 de febrero de 2024, disponible en https://www.ejiltalk.org/what-role-artificial-intelligence-could-play-in-evaluating-the-compliance-of-military-operations-with-international-humanitarian-law-the-case-study-of-the-conduct-of-hostilities-in-ukraine/#:~:text=It%20is%20put%20forward%20that,spreading%20terror%20among%20the%20civilian (última consulta: 23 de abril de 2025). Además, es importante señalar que la referencia utilizada en el artículo al hecho de que "varios países" están utilizando la IA para estimar daños civiles es al *Joint Technical Coordinating Group for Munitions Effectiveness* ("Grupo Conjunto de Coordinación Técnica para la Eficacia de las Municiones") https://www.dote.osd.mil/Portals/97/pub/reports/FY2022/dotemanaged/2022jtcg-me1.pdf?ver=-RQs-CHe5J_X7LaiGiUngA%3d%3d (última consulta: 26 de febrero de 2025), que pese de ser un programa apoyado por la OTAN según una presentación de su Organización de Ciencia y Tecnología con fecha 4 de noviembre 2024 https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SCI-SET-358/MP-SCI-SET-358-09P.pdf (última consulta: 26 de febrero de 2025) es del Departamento de Defensa de Estados Unidos.

[88] J. A. Perea Unceta, "Reflexiones sobre las restricciones… *op. cit.*, p. 103.

[89] *Ibid*., p. 99.

[90] Véase un breve análisis de futuros retos de la contradicción del principio de soberanía y el mantenimiento de la paz, en A. Spain, "Sovereignty and the Promotion of Peace in Non-International Armed Conflict", 106 *Am. Soc'y Int'l L. Proc*. 78 (2012), p. 78-80.

conflictos, destacado como herramienta clave para emprender cualquier paso hacia la paz[91]. Al estallar una controversia internacional, la importancia de tener una comprensión de esta que no sea "estática"[92] de parte de cualquier Estado involucrado sería ayudada por la IA. La tecnología podría también proporcionar una visión global del conflicto, en vez de informes segmentados por las aportaciones de diversas organizaciones[93]. Un beneficio adicional de la IA para estos análisis sería igualmente su neutralidad relativa, mediante datos con los menores sesgos posibles, que permitiría así recibir informes sin el tinte personal de autores humanos[94].

En relación con su capacidad de generar análisis, la IA se podría utilizar también como mecanismo de alerta para situaciones pudiendo quebrar la paz. La tecnología ya se utiliza para predecir eventos relacionados con el mercado de valores, o bien determinados problemas sociales como la involucración de servicios infantiles[95]. Con una base de datos única a cada situación, sea comercio transnacional, discusiones culturales o precios de recursos locales, la IA podría valorar con anticipación posibles conflictos[96], particularmente en zonas ya destacadas por tensión. El interés soberano de utilizar estas medidas se vería en este caso en el ahorro de presupuesto estatal que supondría el poder anticipar estas situaciones con mayor adelanto, ya que ambos el Banco Mundial y la ONU calculan la prevención de conflicto como medida más barata que el conflicto en sí mismo[97].

Por último, la IA ha demostrado gran capacidad de apoyo a la comunicación humana[98], lo que se podría aplicar directamente en negociaciones y mediaciones hacia la resolución pacífica de controversias y la diplomacia. En el proceso de discusión hacia una solución común entre dos o más Estados, la tecnología podría cubrir lagunas que la labor humana no sería capaz, ya sea por "cansancio, diferencias culturales o sesgos personales"[99]. Esto ya se demostró a pequeña escala con el proyecto *Habermas Machine*, el cual observó a más de 5.000 participantes en el Reino Unido en un ejercicio de redacción de declaraciones grupales. En el estudio, los participantes fueron divididos en equipos que fueron mediados

[91] N. Mäki, *Between Peace and Technology – A Case Study on Opportunities and Responsible Design of Artificial Intelligence in Peace Technology*, Laurea University of Applied Science, Vantaa, 2020, p. 64.
[92] Ídem.
[93] *Ibid.*, p. 65.
[94] *Ibid*., p. 66.
[95] *Ibid*., p. 69.
[96] *Ibid*., p. 70.
[97] United Nations & World Bank, *Pathways for Peace: Inclusive Approaches to Preventing Violent Conflict*, Washington DC, United States: World Bank, 2018, p. 2.
[98] N. Mäki, *Between Peace and Technology… op. cit*., p. 71.
[99] *Ibid*., p. 72.

por la IA o bien por humanos. De las declaraciones resultantes, las que generó la máquina de IA tuvieron más éxito entre los grupos asimismo que entre jueces externos, quienes apreciaron mayor "calidad, claridad, capacidad informativa y percepción de imparcialidad"[100]. Aplicado a un nivel interestatal, donde las declaraciones grupales serían así tratados u otro tipo de declaración, la posibilidad de éxito de un sistema de la IA para promover la comunicación es elevada. El uso de procesamiento de lenguaje natural—un subcampo propio de la IA, más conocido por su nombre en inglés *Natural Language Processing*, o NLP—permite igualmente una mayor diplomacia internacional, al ser capaz de manejar varios idiomas a la vez[101].

La IA apoyaría además la resolución pacífica de conflictos ya estallados. El Centro de Estudios Estratégicos e Internacionales en Washington DC encontró que un 60 por ciento de las guerras se acaban trás un compromiso de alguna forma[102]. En el caso del conflicto de Rusia con Ucrania, alegan que la IA sería el instrumento necesario para acabar con el desacuerdo. Concretamente, se utilizaría para su capacidad de análisis ya mencionada, que podría proveer una "fundación sólida" a la hora de buscar soluciones[103]. Así, se incorporaría la opinión de expertos para poder generar múltiples versiones de un mismo acuerdo de paz, anticipando contraofertas y avanzando intereses para el mejor resultado posible[104]. Sin embargo, es importante señalar que el Centro advierte que la IA no puede reemplazar del todo la negociación humana y sus aspectos estratégicos. La resolución mediante la IA se tiene que visionar no como una herramienta reemplazadora, sino como un "multiplicador de fuerzas"[105].

En síntesis, para los tres principios estructurales de no intervención, prohibición de uso de la fuerza, y resolución pacífica de controversias, la IA tiene usos sumamente positivos que apoyan el interés soberano de los Estados. Movilizando así la atención y el interés de la comunidad internacional, las obligaciones que nacen de los principios mencionados se ven igualmente apoyadas en este respecto.

---

[100] M.H. Tessler, et al., "AI can help humans find common ground in democratic deliberation", en *Science*, vol. 386, núm. 6719, octubre 2024, p. 1.
[101] M.K. Pasupuleti., "AI's Role in Global Stability, Diplomacy, and Peacebuilding", en *AI-Powered Diplomacy and Conflict Resolutions*, National Education Services, febrero de 2025, p. 4.
[102] I. Reynolds y B. Jensen, "Machine Learning Meets War Termination: Using AI to Explore Peace Scenarios in Ukraine", *Center for Strategic and International Studies*, febrero 2025, p. 1, disponible en https://www.csis.org/analysis/machine-learning-meets-war-termination-using-ai-explore-peace-scenarios-ukraine (última consulta: 15 de marzo de 2025).
[103] *Ibid*., p. 12.
[104] Ídem.
[105] *Ibid*., p. 13.

2. Innovación económica y desarrollo de industrias nacionales

Más allá de la soberanía, el interés económico de los Estados es evidente, yendo este mano a mano con el deseo de fomentar "poder, riqueza y crecimiento"[106]. La Organización para la Cooperación y el Desarrollo Económico (OECD, por sus siglas en inglés) explica claramente en un reporte de 2022 sobre la IA que esta ya está revolucionado economías nacionales, por su capacidad de aumentar eficiencia y productividad al mismo tiempo que reducir costes[107]. Este es un ejemplo claro de la función catalizadora, pero se presenta igualmente la función creadora en algunos aspectos; se están creando nuevos intereses económicos que no existían antes a nivel estatal. La observación más evidente de esto es que, aunque la IA sea valorada como herramienta para fomentar industrias, la nueva industria de la IA es en sí misma codiciada. Por lo tanto, el interés por esta tecnología de parte de investigadores y corporaciones se ha comparado a la fiebre del oro[108], y así mismo se podría cualificar a la atención prestada por los Estados en esta última década.

La IA es así un área y una herramienta con mucho valor, lo cual los Estados tienen en cuenta. Concretamente, se predice que el producto interior bruto (PIB) a nivel global será un 14 por ciento más alto en 2030 (lo que equivale a una representación de 15.7 mil millones de dólares estadounidenses) dado al desarrollo e implementación de esta tecnología[109]. La prueba *prima facie* de ello a presente es la "carrera espacial moderna"[110] que supone la competición de desarrollo de la IA entre varios países, notablemente entre los dos gigantes del sector: China y Estados Unidos. El debate de cara a las relaciones internacionales en el interés por esta tecnología se reafirmó con la aparición al mercado de DeepSeek a finales de 2024. Se trata así de una solución de IA proveniente de China, que presentó competencia inmediata a tecnologías liderando el mercado, (generalmente estadounidenses, como OpenAI y otros 35 del ranking 2024 de Forbes[111]) por su alto rendimiento y menor consumo de

[106] R. Herrero, "Política exterior…" *op. cit.*, p. 88.
[107] Organisation for Economic Co-operation and Development/CAF, *Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe*, en *Estudios de la OECD sobre Gobernanza Pública*, OECD Publishing, Paris, 2022, p. 10, https://doi.org/10.1787/5b189cb4-es (última consulta: 17 de abril de 2025).
[108] N. Bashir et al., *"The Climate and Sustainability Implications of Generative AI"*, en *An MIT Exploration of Generative AI*, marzo de 2024, disponible en https://doi.org/10.21428/e4baedd9.9070dfe7 (última consulta: 23 de febrero de 2025).
[109] PwC, *AI Analysis: Sizing the Prize Report*, PwC, p. 4., disponible en https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf (última consulta: 17 de marzo de 2025).
[110] Comentario de un grupo de acción estadounidense - D. Kelly, *A Modern-Day Space Race: Artificial Intelligence is the New Frontier*, disponible en https://americanedgeproject.org/a-modern-day-space-race-artificial-intelligence-is-the-new-frontier/ (última consulta: 27 de enero de 2025).
[111] Forbes, *AI 50 List*, ed. Kenrick Cai, 11 de abril de 2024, disponible en https://www.forbes.com/lists/ai50/ (última consulta: 17 de marzo de 2025).

microchips especializados[112]. El efecto político fue tal que el Congreso de Estados Unidos presentó un proyecto de ley, aún pendiente en su procesamiento gubernamental, para prohibir y criminalizar la descarga de la tecnología china en su territorio[113].

Además de la "carrera espacial" figurativa, centrando el interés en el Derecho internacional, cabe destacar que existe sin embargo una faceta *per se* espacial para la IA: su uso en satélites extraterrestres. El espacio ultraterrestre está ganando un "creciente protagonismo"[114] en su uso de recursos y oportunidades, por lo que los Estados se centran en nuevas maneras de conquistar su potencial sobre todo a través de nuevas tecnologías. La Agencia Espacial Europea expuso en julio de 2024 sus aplicaciones de la IA en el funcionamiento de su misión inminente, usos que incluyen la generación de mapas basados en imágenes satelitales y la detección y clasificación de buques marítimos "facilitando el monitoreo de actividades como la pesca ilegal"[115]. Esto es una versión reducida—pero comparable al—del empleo de la IA destacado por la NASA (la Administración Nacional de Aeronáutica y del Espacio estadounidense) en Estados Unidos en enero de 2025. Este último incluye notablemente la colección de datos "de manera autónoma" y el control de tráfico aéreo[116]. Adicionalmente, la Universidad China de Hong Kong lanzó en septiembre de 2024 el "primer satélite de observación terrestre a gran escala"[117] impulsado por IA. Este tiene como objetivo impulsar la detección de datos en el área de Hong Kong y su Gran Bahía, lo que la Universidad detalla como útil para "respuesta ante desastres, ciudades inteligentes, neutralidad en carbono, economía de baja altitud y otros campos"[118].

---

[112] C. Metz y M. Tobin, "How Chinese A.I. Start-Up DeepSeek Is Competing With Silicon Valley Giants," *The New York Times*, 23 de enero de 2025, disponible en https://www.nytimes.com/2025/01/23/technology/deepseek-china-ai-chips.html (última consulta: 15 de marzo de 2025).

[113] S. 321, "Decoupling America's Artificial Intelligence Capabilities from China Act of 2025", 119º Congreso de EE. UU., presentado por Sen. Josh Hawley, 29 de enero de 2025, p. 15-16.

[114] L.A. López Marcos, "Colaboración internacional en el ámbito de los recursos espaciales: sobre la necesidad de crear un instrumento internacional que regule la explotación y apropiación de los recursos espaciales en la Luna y otros cuerpos celestes", en *Revista Española de Derecho Aeronáutico y Espacial*, n.º 2022, Asociación Española de Derecho Aeronáutico y Espacial (AEDAE)/ATELIER, Madrid, 2022, p. 498.

[115] European Space Agency, *New satellite… op. cit.*

[116] National Aeronautics and Space Administration, *"2024 AI Use Cases"*, 7 de enero de 2025, disponible en https://www.nasa.gov/general/2024-ai-use-cases/ (última consulta: 3 de febrero de 2025).

[117] Según investigador del Foro Estratégico Internacional (ISF) en el Proyecto de Estudios Especiales de Competitividad (SCSP) S. Cheung, *"A Hong Kong University Launched the World's First Large-Scale AI Model Earth Observation Satellite"*, *The Diplomat*, 21 de octubre de 2024, disponible en https://thediplomat.com/2024/10/a-hong-kong-university-launched-the-worlds-first-large-scale-ai-model-earth-observation-satellite/ (última consulta: 3 de febrero de 2025).

[118] CUHK Communications and Public Relations Office, *"The Chinese University of Hong Kong satellite was successfully launched into space orbit to celebrate the 75th anniversary of the founding of New China"*, comunicado de prensa, 24 de septiembre de 2024, disponible en https://www.cpr.cuhk.edu.hk/tc/press/%E9%A6%99%E6%B8%AF%E4%B8%AD%E6%96%87%E5%A4%A7%E5%AD%B8%E8%A1%9E%E6%98%9F%E6%88%90%E5%8A%9F%E7%99%BC%E5%B0%84%E9%80%B2%E5%85%A5%E5%A4%AA%E7%A9

El objetivo global del uso de la IA para recopilar datos mediante satélites es evidente; la nueva tecnología da acceso a información accesible más rápidamente y en mayores cantidades, y permite procesarla con mayor facilidad[119]. El desarrollo de la IA, y en cuanto más avanzada este su aplicación, supone de tal manera un punto de inflexión para, por ejemplo, el seguimiento del *Acuerdo que debe regir las actividades de los Estados en la Luna y otros cuerpos celestes de 5 de diciembre de 1979*[120]. Como ejemplo ilustrativo, la utilización de satélites mencionados podría ayudar a cumplir con el Artículo 7 de este, el cual pide minimizar la perturbación del equilibrio lunar. La habilidad de obtener y tratar datos mediante satélites equipados con IA, y no misiones humanas, se podría entender como menos perjudicial al entorno, y por lo tanto un mejor seguimiento de esta obligación.

En el amplio mercado de la IA de nuevo a nivel terrestre, se vuelve a la bifurcación mencionada: la IA es una herramienta deseada por su propio potencial, pero también por el impacto que tiene sobre industrias existentes. Los gigantes comerciales lo entienden; más allá de OpenAI o DeepSeek, los buscadores buscan justamente dominar la IA. Google inauguró su chatbot[121] al estilo de ChatGPT en 2023, unos días después de que el buscador chino Baidu anunció planes de sacar su propia herramienta[122]. Estados Unidos y China son asi los dos líderes mundiales en IA, y oponentes en una nueva "guerra fría"[123] económica de notable importancia. Son igualmente parte de las dos regiones del mundo en las que más crecimiento se proyecta por razón de la IA; en 2030, China sería capaz de ver aumentado su PIB un 26.1 por ciento, y norteamérica un 14.5 por ciento[124].

No obstante, la IA apoya a industrias en cualquier parte del mundo donde se aplique, creando así la llamada "revolución industrial 4.0"[125]. La variedad de sectores que la IA ayuda a propulsar es inmensa; en el caso de la agricultura global por ejemplo, tiene expectativas de

%BA%E8%BB%8C%E9%81%93-%E7%8D%BB%E7%A6%AE%E6%96%B0%E4%B8%AD/ (última consulta: 3 de febrero de 2025).

[119] European Space Agency, *New satellite… op. cit.*

[120] Tratado entrado en vigor el 11 de julio de 1984, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 23002).

[121] El artículo de la cita menciona el chatbot como "Bard", pero Google cambió el nombre a "Gemini" en 2024, según J. Dastin, "Google rebrands Bard chatbot as Gemini, rolls out paid subscription", *Reuters*, 8 de febrero de 2024, disponible en https://www.reuters.com/technology/google-rebrands-bard-chatbot-gemini-rolls-out-paid-subscription-2024-02-08/ (última consulta: 17 de marzo de 2025).

[122] B. Ram y P. Verma, "Artificial intelligence AI-based Chatbot study of ChatGPT, Google AI Bard and Baidu AI", en *World Journal of Advanced Engineering Technology and Sciences*, vol. 08, n.º 01, 2023, p. 260.

[123] L. Romero, "US-China Cold War Is AI-Centric: Can OpenAI's Stargate Settle It?", *Forbes*, 23 de enero de 2025, disponible en https://www.forbes.com/sites/luisromero/2025/01/23/us-china-cold-war-is-ai-centric-can-openais-stargate-settle-it/ (última consulta: 17 de marzo de 2025).

[124] PwC, *AI Analysis: Sizing the Prize Report… op. cit.*, p. 7.

[125] A. Bin Rashid, M.D. Ashfakul Karim Kausik, "AI Revolutionizing Industries Worldwide: A Comprehensive Overview of Its Diverse Applications", en *Hybrid Advances*, vol. 7, 2024, 100277, p. 1.

producir una tasa de crecimiento anual compuesta (TCAC) del 25 por ciento de 2023 a 2031. El uso de aplicaciones impulsadas por IA ha permitido además un 20-30 por ciento de incremento en cultivos[126]. En el sector comercial, el *e-commerce* o las ventas por internet están viendo gran crecimiento con la ayuda de la IA también; en los próximos cinco años, se estima una TCAC del 23 por ciento debido a la gran efectividad de la IA en áreas como las relaciones con los clientes[127]. Finalmente, otro ejemplo de gran impacto es el sector financiero. En este, la TCAC se proyecta como un 28.1 por ciento hasta 2032, debido sobre todo al uso de sistemas de IA generativa y para analizar datos[128].

Un efecto saliente del creciente éxito de la IA sobre estas industrias es sin embargo su impacto medioambiental. El Programa de la ONU para el Medio Ambiente afirma que este es uno de los retos a nivel internacional que supone la IA[129], ya que su uso depende de centros de datos, los cuales utilizan entre otros grandes cantidades de electricidad y agua[130]. Su funcionamiento necesita además minar materiales de forma insostenible y resulta en la emisión de gases nocivos al medio ambiente[131]. Para cumplir con sus obligaciones bajo ciertos tratados y conservar los recursos naturales que permiten el funcionamiento de la tecnología, los Estados utilizan sin embargo la IA justamente para seguir estas obligaciones.

Los 165 firmantes de la *Convención Marco de las Naciones Unidas sobre el Cambio Climático del 9 de mayo de 1992*[132] (grupo que incluye a China y Estados Unidos como partes ratificantes) están así por ejemplo obligados a fomentar la aplicación de tecnologías para reducir gases de efecto invernadero en "todos los sectores relevantes" según el Artículo 4.1.(c) de la Convención. La IA ayuda en ello, a través de sistemas que analizan residuos (los cuales emiten un 16% de gases a efecto invernadero) y separan materiales reciclables ignorados[133]. La IA también ayuda, paradójicamente, a conservar el agua que utiliza. En el

---

[126] *Ibid*., p. 10.
[127] Grand View Research, *AI in Retail Market Analysis Report*, disponible en https://www.grandviewresearch .com/industry-analysis/ai-retail-market-report (última consulta: 17 de marzo de 2025).
[128] Statista Research Department, *Artificial Intelligence (AI) in Finance*, Statista, 5 de abril de 2024, disponible en https://www.statista.com/topics/7083/artificial-intelligence-ai-in-finance/#topicOverview (última consulta: 17 de marzo de 2025).
[129] Programa de las Naciones Unidas para el Medio Ambiente, *"*La IA plantea problemas ambientales. Esto es lo que el mundo puede hacer al respecto.*"*, 21 de septiembre de 2024, disponible en https://www.unep.org/es/ noticias-y-reportajes/reportajes/la-ia-plantea-problemas-ambientales-esto-es-lo-que-el-mundo-puede (última consulta: 21 de febrero de 2025).
[130] N. Bashir et al., *"The Climate and Sustainability… op cit.*
[131] *Programa de las Naciones Unidas para el Medio Ambiente*, *"La IA plantea... op. cit.*
[132] Tratado entrado en vigor el 21 de marzo de 1994, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 30822).
[133] World Economic Forum, "9 ways AI is helping tackle climate change," *World Economic Forum*, 12 de febrero de 2024, disponible en https://www.weforum.org/stories/2024/02/ai-combat-climate-change/#:~:text=

sector agrícola, usos de la IA han permitido una reducción de hasta un 25 por ciento de uso de agua para los cultivos[134].

Igualmente, la IA sirve como apoyo directo al *Acuerdo de París del 12 de diciembre de 2015*[135] y su meta de limitar el calentamiento global a una cifra de por lo menos debajo de 1.5 grados más que los niveles pre-industriales. Pese a que el gigante de la IA estadounidense se retiró nuevamente del Acuerdo en enero de 2025[136], la utilización de la tecnología para cumplir con este está demostrada[137]. En 2023, Microsoft se unió a la Convención Marco (UNFCCC por sus siglas en inglés) para medir emisión y seguir el progreso bajo el Acuerdo mediante analítica de datos impulsada por IA[138]. Además, la proyección del instituto de investigación Capgemini estima que la IA ayudará a completar el 11-45 por ciento de los objetivos de llamada "intensidad económica de emisiones", dependiendo de cómo se adopte la IA en cada sector. Calcula por ejemplo que el sector automóvil sería capaz de contribuir un 8 por ciento de la reducción del 37 por ciento requerida por el Acuerdo[139]. La ONU está igualmente reconociendo el potencial de la IA para apoyar a los Estados en sus obligaciones medioambientales, impulsando proyectos como el "Programa de Trabajo Conjunto del Mecanismo Tecnológico para 2023-2027", el cual "incluye un enfoque en tecnologías digitales que pueden ofrecer soluciones climáticas en múltiples sectores e industrias"[140].

El cambio climático no es el único problema industrial con solución en la IA. Otro uso notable en el desarrollo económico de los Estados consiste en el uso de herramientas para

---

The%20use%20of%20artificial%20intelligence,the%20World%20Economic%20Forum%20says (última consulta: 17 de marzo de 2025).

[134] A. Bin Rashid, M.D. Ashfakul Karim Kausik, "AI Revolutionizing Industries… *op. cit.*, p. 10.

[135] Tratado entrado en vigor el 4 de noviembre de 2016, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 54113).

[136] Veasé informe de la Casa Blanca - The White House, "Putting America First in International Environmental Agreements", 23 de enero de 2025, disponible en https://www.whitehouse.gov/presidential-actions/2025/01/putting-america-first-in-international-environmental-agreements/ (última consulta: 17 de marzo de 2025).

[137] Véase también C. E. Marinică, "Artificial intelligence – A possible key for better results on tackling climate change", en *Law Review*, vol. XII, núm. 1, Union of Jurists of Romania, 2022, p. 89-90.

[138] Microsoft y UNFCCC, *UNFCCC partners with Microsoft to use AI and advanced data technology to track global carbon emissions and assess progress under the Paris Agreement*, Microsoft News Center, 29 de noviembre de 2023, disponible en https://news.microsoft.com/2023/11/29/unfccc-partners-with-microsoft-to-use-ai-and-advanced-data-technology-to-track-global-carbon-emissions-and-assess-progress-under-the-paris-agreement/ (última consulta: 23 de abril de 2025).

[139] Capgemini Research Institute, *Climate AI: How artificial intelligence can power your climate action strategy*, disponible en https://www.capgemini.com/wp-content/uploads/2021/05/Report-Climate-AI-4.pdf, p. 2 (última consulta: 17 de marzo de 2025).

[140] United Nations Climate Change Technology Executive Committee, *Artificial Intelligence for Climate Action in Developing Countries: Opportunities, Challenges and Risks*, p. 17, disponible en https://unfccc.int/ttclear/misc_/StaticFiles/gnwoerk_static/AI4climateaction/28da5d97d7824d16b7f68a225c0e3493/a4553e8f70f74be3bc37c929b73d9974.pdf (última consulta: 17 de marzo de 2025).

proteger los derechos humanos, concretamente los de los trabajadores. Particularmente en cuanto a la labor forzada en fábricas, la IA podría mejorar las circunstancias de aquellos empleados actualmente asignados tareas repetitivas en condiciones no deseables. Siguiendo así por ejemplo el Objetivo de Desarrollo Sostenible número 8 de la ONU, la IA ayudará a automatizar trabajos repetitivos, y promover "un empleo pleno y productivo para todos"[141]. Los trabajadores en industrias intensivas en mano de obra—mujeres en particular—se beneficiarán igualmente de una promoción de la IA en el entorno laboral en forma de robótica[142]. Este cambio ya está en efecto; en la UE por ejemplo, un 5 por ciento de trabajadores en 2022 ya trataban con robots o máquinas que utilizaban alguna forma de IA[143]. Igualmente, se podría utilizar la IA para obtener grandes cantidades de datos sobre las condiciones de los trabajadores para analizar y vigilar situaciones potencialmente peligrosas, y así mitigar riesgos de esclavitud moderna y violaciones de derechos humanos segun la ONU[144].

Finalmente, es importante destacar el uso de la IA para monitorear similarmente el trabajo infantil. El Artículo 32.1 de la *Convención sobre los Derechos del Niño del 20 de noviembre de 1989*[145] prohíbe la "explotación económica" y el trabajo infantil nefasto para la educación o el desarrollo de dicho niño. Sin embargo, en 2020, se estimaba que aún había 160 millones de niños trabajando de tal forma nefasta, y 79 millones de estos en condiciones consideradas peligrosas[146]. Pese de ser una reducción desde el principio del milenio, resulta ser una cifra estable desde 2016[147]. La IA, o más específicamente su rama de *machine learning*[148] (literalmente aprendizaje de máquina, también traducido como aprendizaje automático) podría ayudar a mitigar el trabajo infantil trás el uso de algoritmos para revisar

---

[141] Y. Shen y X. Zhang., "The impact of artificial intelligence on employment: the role of virtual agglomeration", en *Humanit Soc Sci Commun* 11, 122 (2024), p. 1.
[142] Ídem.
[143] European Agency for Safety and Health at Work, *Integrating artificial intelligence at work: automation of tasks*, 27 de junio de 2024, https://healthy-workplaces.osha.europa.eu/en/media-centre/news/integrating-artificial-intelligence-work-automation-tasks (última consulta: 18 de marzo de 2025).
[144] United Nations University Centre for Policy Research, *Artificial Intelligence: Addressing or Distorting the Modern Slavery Challenge?*, octubre 2023, p. 3, disponible en https://unu.edu/sites/default/files/2023-10/AI%20addressing%20or%20distorting%20modern%20slavery%20challenge.pdf (última consulta: 18 de marzo de 2025).
[145] Tratado entrado en vigor el 2 de septiembre de 1990, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 27531).
[146] International Labour Organization (ILO) and UNICEF. *Executive Summary: Child Labour. Global Estimates 2020, Trends and the Road Forward*. 2020, p.2., https://www.ilo.org/media/384736/download. (última consulta: 18 de marzo de 2025).
[147] Ídem.
[148] El *machine learning* es un subtipo de la IA dedicado al aprendizaje de tareas imitando a humanos, para eventualmente poder realizar tareas independientemente. Véase: IBM. "What is machine learning?" *IBM*, 2025, https://www.ibm.com/think/topics/machine-learning. (última consulta: 18 de marzo de 2025).

datos de imagines de satelite y via teledetección[149]. Por lo tanto, los Estados podrían utilizar la IA para apoyar la aplicación de los derechos humanos; concretamente, la Organización Internacional del Trabajo estima que la abolición de la explotación infantil es un derecho fundamental del trabajo[150]. Se observa entonces el lado positivo de la IA en cuanto a su uso estatal en este ámbito.

En suma, los Estados se benefician ampliamente de la IA para sus intereses soberanos, de defensa, y de desarrollo nacional. Gracias a una tecnología que impulsa sus mecanismos militares, sus industrias, y hasta trabaja para resolver algunos de los mismos problemas que cree, la comunidad internacional tiene un gran potencial de avance técnico y económico. Vemos igualmente el beneficio aportado al Estado de Derecho; el hecho que una herramienta que se junte con los intereses de los Estados pueda ayudar igualmente a seguir obligaciones bajo el Derecho internacional es una gran fuente de potencial para la valoración de regulaciones apropiadas. El valor así demostrado por las partes estatales ha de ser aprovechado jurídicamente.

[149] M. Ahmad *et al*., "Leveraging Blockchain and Machine Learning to Promote Child Labor-Free Sustainable Development", en *Distrib. Ledger Technol.*, 4, 1, Article 7, March 2025, p. 6.
[150] A. G. López Martín, "La protección internacional de los derechos de los trabajadores en el marco de la centenaria OIT: una breve referencia a la situación de España como miembro de la misma", en *Anuario de los Cursos de Derechos Humanos de Donostia-San Sebastián: Donostiako Giza Eskubideei Buruzko Ikastaroen Urtekaria*, n.º 21, 2021, p. 161.

IV. HECHOS INTERNACIONALMENTE ILÍCITOS Y LAS FUNCIONES DE LA INTELIGENCIA ARTIFICIAL EN SU IMPULSIÓN

Habiendo visto así el valor aportado por la IA a los intereses de los Estados, y su apoyo en las obligaciones estatales que contribuyen al considerado Estado de Derecho internacional, se entiende el papel fundamentalmente positivo que juega esta tecnología en la comunidad global de la actualidad. Sin embargo, la faceta negativa de su uso es igualmente importante de analizar, exponiendo así sobre todo el *hecho* en la práctica como impulsa la teoría de la tridimensionalidad del derecho para llegar al interés regulatorio[151]. La IA destaca en su especial capacidad de promover HII, trás la generación de nuevas avenidas para violar obligaciones internacionales a nombre de Estados que la utilicen. Permite además impulsar dichos HII con una capacidad de alcance y eficiencia mayor que nunca, lo que resulta ser un punto de inflexión para dicha posible regulación sobre ello.

Al hablar de los HII, la referencia primaria es el *Proyecto de Artículos sobre la responsabilidad del Estado por Hechos Internacionalmente Ilícitos*, adoptado por la Comisión de Derecho Internacional en 2001[152] (en adelante referido como PA 2001). El Artículo 2 de este define los dos elementos constitutivos de un HII, los cuales se ven impactados por la interacción con la IA en casos relevantes. En primer lugar, el elemento subjetivo requiere que el hecho observado se pueda atribuir a un Estado. Más allá de identificar, en caso de posible HII mediante IA, que Estado en particular utilizó o contrató la tecnología, existe la complicación acerca de la autonomía en la operación; sí la IA toma sus propias decisiones, se habla entonces de su posible personalidad jurídica. Mientras que este trabajo no se enfoca en esta temática particularmente, es importante señalar las bases de la cuestiones jurídicas que suscita este caso en cuanto a la aplicación del primer elemento del Artículo 2 del PA 2001. Es especialmente relevante a la hora de analizar los sistemas autónomos letales, como ya mencionado en la revisión de literatura y tratado a continuación.

Secundariamente, el elemento objetivo del Artículo 2 necesita que el hecho atribuible sea en si una violación de una obligación internacional del Estado relevante. Este siendo el ámbito central de este Capítulo, se analizan así principalmente dos categorías generales de violaciones del Derecho internacional mediante la IA: las que ocurren a nivel internacional por actuaciones militares y de defensa de los Estados, y los hechos a nivel nacional que

[151] G. Álvarez Undurraga, *Metodología… op. cit.*, p. 25.
[152] Comisión de Derecho Internacional, *Proyecto de Artículos sobre la responsabilidad del Estado… op. cit.*

puedan ir en contra de una obligación de Derecho internacional contratada por el Estado donde ocurren.

1. Usos ilícitos a nivel internacional

El uso de la IA está "convirtiéndose en una herramienta clave" en la estrategia de las fuerzas militares de los Estados[153]. Como ya mencionado, la tecnología se ha adentrado en varios sistemas de protección estatal con el ámbito de promover la soberanía y las obligaciones de fomento de la paz que tienen los Estados. Permite proteger fronteras mediante su función creadora, impulsando varias técnicas de reconocimiento humano[154], tecnología de detección automática[155], o bien los *decision support systems*[156] vistos a continuación. La IA se utiliza igualmente en armas ya existentes, destacando su función catalizadora en campos como la energía nuclear[157]. Se emplea además en la robótica militar, dando a sistemas autónomos mayor eficacia y capacidad de navegación[158]. Esta utilización de la IA para la protección militar y la defensa de Estados concretos tiene los efectos positivos sobre el Derecho internacional vistos en el primer Capítulo, pero genera una presión internacional y preocupación jurídica significativa. Concretamente, se proyecta que la IA tendrá el mismo efecto sobre el ordenamiento mundial que el que se vio trás la creación de armas nucleares[159]. A continuación, se observan los casos más salientes en los cuales la IA juega un papel militar o defensivo en la comisión de HII de parte de los Estados que la utilizan a nivel internacional.

1.1. Sistemas autónomos letales

Las armas y la maquinaria que las detonan son un elemento destacado de las fuerzas militares y el concepto de defensa nacional. Históricamente, estas se desarrollaron con la intención de tener un efecto predecible en situaciones de guerra[160], pero la aparición de la IA en contextos tal y como los sistemas autónomos letales representó una contradicción con esta meta. Aunque ya existían armas con empleo autónomo—como las minas, siendo estas

[153] I. Szabadföldi, "Artificial intelligence in military application – opportunities and challenges", en *Land Forces Academy Review*, vol. XXVI, n.º 2(102), 2021, p. 157.
[154] N. Md Nor, *et. al*., "Leveraging Artificial Intelligence*... op. cit.* p. 62.
[155] CORDIS, *The Next Generation of Maritime Awareness… op. cit.*
[156] Comité Internacional de la Cruz Roja (ICRC) y Geneva Academy, *Expert Consultation Report… op. cit*.
[157] I. Szabadföldi, "Artificial intelligence in military… *op. cit.*, p. 161.
[158] *Ibid*., p. 162.
[159] *Ibid*., p. 161.
[160] R.L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression*, Oxford University Press, Nueva York, 1989, p. 7.

activadas por personas pero operadas con mecanismos de disparo propios[161]—la IA presenta una categoría nueva por su expresa habilidad de razonar para "buscar, detectar, identificar, rastrear o seleccionar" sus objetivos[162]. Así, se habla hasta de estas capacidades como siendo de "otra especie inteligente" con la cual los humanos han de convivir en el presente[163]. Dicha nueva especie crea así dos cuestiones fundamentales a la hora de analizar los HII. La primera, la de la posible personalidad jurídica de la IA, no se tratará directamente en este trabajo como indicado previamente. La segunda cuestión, vista a continuación, busca analizar el creciente impacto de esta tecnología sobre la comisión de HII.

Los sistemas autónomos letales (abreviados aquí como SAL, y en algunas fuentes llamados *sistemas de armas letales autónomos*[164]) son un sistema de armas que se utilizarían con fines mortales y funciones autonómicas, pero sin definición decidida en Derecho internacional[165]. Como parte de la *Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados del 10 de octubre de 1980*[166] (en adelante, Convención sobre ciertas armas), la ONU publicó una compilación de definiciones estatales[167]. Para tratar el tema en este Capítulo, se emplea aquí la definición de Argentina *et al.*, la cual indica:

> "…un sistema de armas puede ser caracterizado como un [sistema de armas autónomo] si incorpora autonomía en las funciones críticas de seleccionar y atacar para aplicar fuerza contra los objetivos, sin intervención humana.
>
> …la letalidad no es una característica intrínseca de un sistema de armas, sino un efecto o una forma de uso, y…cualquier sistema de armas puede ser contrario al Derecho internacional, independientemente de si es letal o no."[168]

Además, se señala la importancia de la distinción propuesta por España en conjunto con varios otros países de la UE en 2022. Estos Estados extienden así una separación entre los SAL "totalmente autónomos que operen sin control humano ni cadena de mando

[161] United Nations Office for Disarmament Affairs, *Lethal Autonomous Weapon Systems (LAWS)*, disponible en https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/ (última consulta: 18 de marzo de 2025).
[162] N. Davison, "A legal perspective: Autonomous weapon systems under international humanitarian law", en *UNODA Occasional Papers No. 30, November 2017*, enero 2018, p. 5.
[163] I. Moll Santa-Isabel, "El desarrollo normativo, ético y tecnológico de los Sistemas Autónomos Letales", en *Araucaria*, vol. 26, n.º 57, 2024, p. 55.
[164] S. Leal W, "Los Sistemas de Armas Letales Autónomos", en *Frónesis. Revista de Filosofía Jurídica, Social y Política*, vol. 31, n.º 1, Universidad del Zulia, 2023, p. 52.
[165] United Nations Office for Disarmament Affairs, *Lethal Autonomous… op. cit.*
[166] Tratado entrado en vigor el 2 de diciembre de 1983, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 22495).
[167] Grupo de Expertos Gubernamentales sobre Sistemas de Armas Letales Autónomas, *Non-exhaustive compilation of definitions and characterizations*, CCW/GGE.1/2023/CRP.1, 2023, p. 4.
[168] *Ibid.*, p 2-3.

responsable" (que buscan prohibir) y "otros", los cuales sí gozan de control humano pero han de ser regulados para seguir las obligaciones del Derecho internacional humanitario[169]. Si bien a día de hoy no existe un SAL capaz de cumplir con una misión totalmente sin control humano[170], el riesgo de comisión de HII mediante estos es inminente. A continuación, se analizan dos casos de implementación de los SAL y sus aplicaciones prácticas frente al cumplimiento de las obligaciones estatales.

Alrededor de 2006, Corea del Sur desarrolló el robot SGR-A1, equipado con un sistema autónomo con armas de fuego para vigilar la zona desmilitarizada entre las dos Coreas. Este sistema podía reconocer a humanos entre animales y otras figuras, y podía disparar[171]. Mientras se alegaba que el robot caía en la segunda categoría de distinción establecida por España *et al*., al necesitar control humano para ser operado, el Comité de Seguridad Internacional y Control de Armamentos (CISAC, por sus siglas en inglés) acusa la maquinaría de aún así tener capacidad de actuar por sí misma e incrementar daños civiles[172]. Esta es la misma inseguridad que el Comité Internacional para el Control de Armas Robóticas (en inglés conocido por sus siglas ICRAC) respaldo en 2010 al pronunciar "inaceptable" el hecho de que una máquina pueda aplicar la fuerza sin supervisión y responsabilidad jurídica humana[173]. Tras el robot coreano, el cual parece estar aún en uso[174], hubo protestas que resultaron en la creación de pronunciaciones sobre la ética de estos sistemas[175] como la *Carta*

[169] *Ibid.*, p. 4.
[170] E. Hunter Christie *et al.*, "Regulating lethal autonomous weapon systems: exploring the challenges of explainability and traceability", en *AI and Ethics*, vol. 4, 2024, p. 230.
[171] H.-K. Kim, "Sentry Robots in Action: Ethical and Legal Issues of Automated Weapon in South Korea," en *ICRES 2022: 7th International Conference on Robot Ethics and Standards*, Seúl, Corea del Sur, 18-19 de julio de 2022, p. 41.
[172] *Ibid*., p. 42.
[173] International Committee for Robot Arms Control, *Berlin Statement*, octubre 2010, disponible en https://www.icrac.net/statements/? (última consulta: 23 de abril de 2025).
[174] La información es escasa y de fuentes contradictorias y de poca fiabilidad. Existe un artículo publicado en LinkedIn en marzo de 2025 que alega que es una "implementación actual" - véase A.P. Pokharel, "AI in Warfare: The Rise of Autonomous Weapons and the Future of Global Security," *LinkedIn*, 10 de marzo de 2025, disponible en https://www.linkedin.com/pulse/ai-warfare-rise-autonomous-weapons-future-global-adrian-pokharel-zg3ee/ (última consulta: 25 de marzo de 2025). Una publicación mediática de 2023 habla del robot en tiempo pasado, véase E. Shayotovich, "Everything we know about Samsung's machine gun robots", *SlashGear*, 1 de febrero de 2023, https://www.slashgear.com/825074/everything-we-know-about-samsungs-machine-gun-robots/ (última consulta: 23 de marzo de 2025). La agencia de noticias turca Anadolu Agency publicó en 2024 un artículo sobre nueva tecnología de la IA implementada por Corea del Sur en su frontera con Corea del Norte, sin especificar particularmente sobre medios ya existentes. Véase R. ul Khaliq, "South deploys AI-powered systems to 'better monitor' North Korea," *Anadolu Agency*, 23 de mayo de 2024, disponible en https://www.aa.com.tr/en/artificial-intelligence/south-deploys-ai-powered-systems-to-better-monitor-north-korea/3228037 (última consulta: 25 marzo 2025).
[175] H.-K. Kim, "Sentry Robots in Action: Ethical… *op. cit.*, p. 43.

de Ética de la Inteligencia Artificial de la Asociación de Ética de la Inteligencia Artificial de Corea[176].

En la actualidad más reciente, Israel reporta utilizar la IA en sistemas autónomos, aunque estos no se puedan calificar de sistemas de armas *per se* basado en las definiciones mencionadas anteriormente. Los sistemas mencionados a continuación no aplican la fuerza directamente, sino que hacen recomendaciones para que las fuerzas militares la apliquen ellos mismos. Así es por ejemplo el caso del algoritmo "Lavender", desplegado por las fuerzas israelíes a principios de 2024. Este sistema se usa para identificar decenas de miles de objetivos humanos, que la IA entrenada con su base de datos juzga ser afiliados con Hamas o el grupo Yihad Islámica Palestina[177]. Por cada uno de los 37.000 objetivos que la IA calculó, los soldados israelíes reportan haber obtenido permiso para matar hasta "20 civiles no involucrados"[178]. Las fuerzas armadas tardaban unos 20 segundos en aprobar manualmente los incriminados que generaba la IA; según el testimonio de los operadores, el algoritmo se equivoca en un 10 por ciento de los casos[179]. Al mismo tiempo, el sistema "The Gospel" hace las mismas recomendaciones a las fuerzas israelíes pero para edificios y estructuras que considera interesantes atacar[180].

Jurídicamente, el riesgo que suponen ambos el ejemplo de Corea y el de Israel es importante. Independientemente de que el sistema de la IA aplique en sí mismo la fuerza, la confianza casi completa en el algoritmo israeli atrae las mismas preocupaciones que los SAL; un usuario de "Lavender" reporta así no sentir tener "valor añadido" a la máquina como ser humano, y preguntarse si realmente su rol en la práctica tiene sentido[181]. Se entiende así que la confianza en las decisiones de la IA es casi absoluta, y que no hay aplicación crítica de juicio humano en la toma de cada decisión. Más allá de la atribución mencionada en la introducción de este Capítulo, esto es importante para cumplir con el elemento de

[176] H. Ha y P. Min-Hye, "The Threat of AI and Our Response: The AI Charter of Ethics in South Korea", en *Asian Journal of Innovation and Policy*, vol. 9, no. 1, 2020, p. 56-78.
[177] Y. Abraham, "'Lavender': The AI machine directing Israel's bombing spree in Gaza", *+972 Magazine*, 3 de abril de 2024, disponible en https://www.972mag.com/lavender-ai-israeli-army-gaza/ (última consulta: 23 de marzo de 2025).
[178] B. McKernan and H. Davies, "'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets", *The Guardian*, 3 de abril de 2024, disponible en https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes (última consulta: 23 de marzo de 2025).
[179] H. Gusterson, "It's all Lavender in Gaza", en *Anthropology Today*, vol. 40, 2024, p. 2.
[180] Human Rights Watch, "Questions and Answers: Israeli Military's Use of Digital Tools in Gaza", 10 de septiembre de 2024, disponible en http://hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza#:~:text=Another%2C%20which%20the%20military%20calls,labeling%20them%20as%20military%20targets. (última consulta: 25 de marzo de 2025).
[181] B. McKernan and H. Davies, "'The machine did it… *op. cit.*

subjetividad del PA 2001, al ser un riesgo a la hora de valorar el seguimiento de las obligaciones del Estado. Una máquina autónoma cuya IA cumple con objetivos determinados no tendrá la misma valoración de la vida humana, esto siendo relevante particularmente a la hora de cumplir con las obligaciones de *ius in bello* y los principios de proporcionalidad y de distinción.

El principio de proporcionalidad queda recogido en Derecho internacional en el Protocolo adicional I de los Convenios de Ginebra previamente mencionados. El Artículo 51(5)(b) prohíbe a los Estados atacar cuando se pueda hacer daño "excesivo" a civiles en comparación con el beneficio militar obtenido. Adicionalmente, el Artículo 57 pide en su apartado (1) que haya "cuidado constante" para minimizar daños a poblaciones civiles, y en su apartado (2)(a) que "quienes preparen o decidan un ataque" hagan lo posible para velar sobre ello. Una máquina que pueda matar o aconsejar objetivos humanos sin consideración estudiada de parte de una persona al cargo puede así incumplir con el Artículo 57. La confianza total en sistemas como los mencionados en uso por Israel sería de tal manera conductiva a la comisión de un HII. El uso de robots como los de Corea, si pueden disparar autónomamente, frena igualmente el cumplimento con la obligación de atención constante de parte de un comandante.

Los SAL sufren además de la llamada *operational unpredictability* (en castellano, imprevisibilidad operacional), al estar diseñados para operar en ámbitos que un programador humano no puede anticipar[182]. Esta consideración añade otro matiz al posible incumplimiento del principio de proporcionalidad. El Comité Internacional de la Cruz Roja respalda esta perspectiva, alegado que la imprevisibilidad es un riesgo frente al cumplimento del Derecho internacional humanitario si los comandantes no pueden predecir las consecuencias del uso de sistemas autónomos[183]. Finalmente, el principio de proporcionalidad se ve igualmente en riesgo si no se dispone de la capacidad humana de asesorar una situación. Si, como ejemplo ilustrativo, un SAL como el robot coreano fuera programado con las permisiones de las fuerzas israelíes de matar hasta 20 personas no involucradas[184], el riesgo de causar daño no proporcional es alto. Si el objetivo militar se escondiera en un aula escolar, es posible que el

[182] A. Blanchard y M. Taddeo, "Predictability, Distinction & Due Care in the use of Lethal Autonomous Weapon Systems," 3 de mayo de 2022, SSRN, p. 8, http://dx.doi.org/10.2139/ssrn.4099394 (última consulta: 25 de marzo de 2025).
[183] Comité Internacional de la Cruz Roja, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, Ginebra, agosto 2019, p. 11, https://www.icrc.org/sites/default/files/document/file_list/autonomy_artificial_intelligence_and_robotics.pdf (última consulta: 25 de marzo de 2025).
[184] B. McKernan and H. Davies, "'The machine did it…" *op. cit.*

SAL considere aceptable atacar a 20 alumnos en búsqueda del objetivo, lo que se puede entender que un soldado humano tendría menos capacidad ejecutiva de hacer, bien por ética, razonamiento moral, o simplemente al ser humano y no máquina. Las fuerzas de defensa de Australia critican de esta manera la inhabilidad de "pensamiento dinámico y creativo" de los SAL y el riesgo que conlleva frente a la falta de seguimiento del derecho aplicable en conflictos[185].

El principio de distinción del Derecho internacional humanitario aplica igualmente frente al uso de SAL y similares. Recogido en el Protocolo adicional I igualmente, el Artículo 48 obliga a los Estados distinguir "en todo momento" personas civiles de combatientes, para dirigirse únicamente contra estos últimos. Además, el Artículo 51(2) prohíbe atacar civiles, y su apartado (4) especifica que tampoco se permiten ataques indiscriminados sin claros objetivos militares. Descontando el riesgo de sistemas como el de Israel, que como mencionado se equivoca en un 10 por ciento de sus calculaciones[186], el riesgo de equivocación en SAL sin ninguna involucración humana puede ser alto. Un ejemplo de ello es la involucración, de nuevo, del problema de *operational unpredictability* a la distinción entre civiles y combatientes[187]. Otro riesgo importante son las "numerosas interpretaciones" del principio de distinción. Al existir un debate académico sobre la permisibilidad de los ataques *no intencionales* a civiles, una perspectiva que entienda una brecha de debido cuidado de parte del Estado en estos casos juzgaría los SAL como un riesgo inaceptable[188].

El futuro de los SAL es una amenaza jurídica y una oportunidad de regulación inminente, al combinar ambas funciones de la IA en su impulso a HII. Los SAL son una amenaza completamente nueva, pero recogen ciertos elementos que catalizan las prácticas estatales ya existentes en conflictos. Reconociendo esta realidad, se introdujo un borrador de Resolución a la Asamblea General de la ONU a finales de 2024, con el objetivo de entre otros de apoyar la regulación de los SAL[189] bajo la Convención sobre ciertas armas mencionada anteriormente. Dicha Convención ya fue capaz de prohibir ciertas categorías de armas, como

[185] J. Mackay Stanhope, "Opposing Inherent Immorality in Autonomous Weapons Systems", *The Forge*, Australian Defence College, 6 de abril de 2021, https://theforge.defence.gov.au/article/opposing-inherent-immorality-autonomous-weapons-systems (última consulta: 25 de marzo de 2025).
[186] H. Gusterson, "It's all Lavender in Gaza... *op. cit.* p. 2.
[187] A. Blanchard y M. Taddeo, "Predictability, Distinction… *op. cit.*, p. 8.
[188] *Ibid.*, p. 10.
[189] Asamblea General de las Naciones Unidas, borrador de Resolución "Sistemas de armas autónomos letales", Doc. A/C.1/79/L.77 (2024).

las químicas[190]. La prohibición/fuerte regulación de los SAL se basa por lo tanto en este precedente y el Grupo de Expertos Gubernamentales sobre tecnologías emergentes en el área de sistemas de armas autónomas letales que establece la Convención.

El debate en el seno de la ONU es actual, por el hecho de que las potencias occidentales, China, y Rusia están desarrollando sus estrategias frente a estas armas[191]. A medida que estas fuerzas armadas se familiarizan con la IA, se crea igualmente una amenaza sobre el mantenimiento del principio de abstención de uso de la fuerza. Si estas tecnologías progresan sin regulación y supervisión humana, corren el riesgo de estallar conflictos que no sean capaces de ser resueltos por intervención humana[192]. En suma, las especificaciones técnicas de estos sistemas requieren un entendimiento de los beneficios que aportan a los combatientes, pero igualmente—y más urgentemente—de las lagunas que presentan en comparación con humanos a la hora de cumplir con obligaciones del Derecho internacional.

1.2. Drones y otros sistemas militares similares

A diferencia de los SAL, otros sistemas militares utilizan la IA sin considerarse armas *per se* o servir para aplicar la fuerza directamente. La tecnología de la IA se puede integrar en la autonomía de varias herramientas, tales como drones, cámaras, o sensores[193], considerando entonces la función catalizadora de la IA para impulsar sistemas ya existentes. Con particular referencia a los drones, mientras que algunas publicaciones utilizan una definición de "drones armados" que se alinea más bien con las SAL[194], se han de entender en el ámbito de este Capítulo como simplemente drones capacitados con I (caso ya estudiado en el Capítulo I cuando se trató el apoyo de estos al principio de no intervención).

---

[190] United Nations Office for Disarmament Affairs, *The Convention on Certain Conventional Weapons*, disponible en https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/ (última consulta: 26 de abril de 2025).
[191] I. Moll Santa-Isabel, "El desarrollo normativo, ético… *op. cit.*, p. 56.
[192] H. M. Roff, "Lethal Autonomous Weapons and Jus Ad Bellum Proportionality", en *Case Western Reserve Journal of International Law*, vol. 47, 2015, n.º 1, p. 47.
[193] Véase un artículo promocional de una compañía estadounidense especializada en la venta de *software* - F. Hicks, *AI in Military Drones: Redefining National Defense Strategies*, Aegis Softtech, disponible en https://www.aegissofttech.com/insights/ai-in-military-drones/#:~:text=AI%20in%20Drone%20Navigation&text=By%20integrating%20AI%20algorithms%20with,in%20planning%20their%20routes%20dynamically (última consulta: 25 de marzo de 2025).
[194] E. Blanco Niyitunga, "Armed drones and international humanitarian law", en *Digital Policy Studies*, vol. 1, n.º 2, University of Johannesburg, 2023, p. 19.

Un ejemplo de drones dotados de IA que no sirvan funciones de SAL son los que se utilizan para patrullar aéreamente[195]. Visto entonces anteriormente en el texto en el uso de ciertas fronteras como la de Malasia y Tailandia[196], estos drones utilizan su capacidad de IA para analizar, por ejemplo, intrusiones e irregularidades. En estos mismos usos sin embargo, se destacan riesgos éticos, como "sesgos [y] discriminación", asi que daños potenciales a "la privacidad de datos personales, seguridad nacional, y estabilidad social y economica", así que a los derechos humanos vulnerados por tales riesgos[197]. Efectivamente, dependiendo del razonamiento de la IA, esta puede por ejemplo concluir que la manera más sencilla de detectar "intrusiones" es enfocándose en todas las personas de cierto color de piel. Este ejemplo concreto supondría por lo tanto una posible violación de derechos humanos como recoge la *Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial del 21 de diciembre de 1965*[198].

Este último ejemplo de análisis de parte de la IA queda estrechamente relacionado con el llamado razonamiento de caja negra[199], un reto saliente en la validez jurídica de esta tecnología en Derecho internacional. Dicho razonamiento es el resultado de una falta de "entendimiento humano"[200] en algunas operaciones de la IA; algunos sistemas no tienen un proceso claro y explicable, por lo que el producto se lleva a cabo trás un razonamiento demasiado complejo para que un humano lo entienda[201]. Al no existir certeza en como operan, y sin transparencia de pensamiento, no se puede determinar qué factores se priorizaron, sin algunos datos se excluyeron, *etc*. El hecho que no se pueda determinar entonces la intención del razonamiento de estos sistemas de IA causa una inhabilidad de comprobar una actuación de buena fe, lo que sería una brecha de las obligaciones de, por ejemplo, el principio de proporcionalidad en su uso en conflictos[202].

Una consideración de los drones apoyados por la IA en la comisión de HII es también de nuevo su imprevisibilidad, en particular con lo relacionado con la soberanía espacial[203]. Si

[195] J. Saura, *Implications of the use of drones in international law*, International Catalan Institute for Peace, disponible en https://www.icip.cat/perlapau/en/article/implications-of-the-use-of-drones-in-international-law/ (última consulta: 25 de marzo de 2025).
[196] N. Md Nor, *et. al*., "Leveraging Artificial Intelligence*... op. cit.,* p. 62.
[197] Ídem.
[198] Tratado entrado en vigor el 4 de enero de 1969, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 9464).
[199] E. Hunter Christie *et al.*, "Regulating lethal autonomous… *op. cit*., p. 231.
[200] J.S. Viveros Álvarez, "La inteligencia artificial… *op. cit.*, p. 92.
[201] Universidad Complutense de Madrid, *Certificado en Inteligencia Artificial… op. cit.*
[202] E. Hunter Christie *et al.*, "Regulating lethal autonomous… *op. cit*., p. 231.
[203] J. Saura, *Implications of the use of drones in international law… op. cit.*

bien un operador humano puede tener en cuenta elementos jurídicos como el consentimiento del Estado ajeno, o bien la legítima defensa a la hora de adentrarse con un dron en el espacio aéreo correspondiente a otro territorio, la IA puede no tener el mismo debido cuidado por razón de su programación. Se identifican igualmente otros riesgos a la soberanía aérea mediante los drones, aún sin utilizar la IA; siendo pequeños en tamaño y un sistema generalmente de bajo coste, pueden entre otros ser utilizados para atascar y destruir maquinaria de defensa, y igualmente evadir radares preventores[204]. La IA representa, de nuevo con su *operational unpredictability*, un riesgo de agravación al cumplimiento de la obligación del Derecho internacional de no adentrarse militarmente en un territorio ajeno sin permiso.

1.3. Involucración en armas nucleares

Otro uso considerable de la IA en la promoción de la comisión de HII es su función catalizadora por su involucración en el sector de la energía nuclear y las armas relacionadas. Este uso es innovador es considerable tanto para los Estados reconocidos en el *Tratado de No Proliferación Nuclear del 1 de julio de 1968*[205] como para el resto de la comunidad internacional que manipula esta energía[206]. Por el impacto sin embargo global de las armas nucleares, y la consideración en el Preámbulo de dicho Tratado de "las devastaciones que una guerra nuclear infligiría a la humanidad entera", la comunidad del Derecho internacional en su totalidad tiene un interés intrínseco en la regulación de la combinación de las tecnologías nucleares de uso militar y de la IA.

Una primera consideración para el Derecho internacional que el uso de la IA en armas nucleares fomenta es la vulnerabilidad de la ciberseguridad de los sistemas que ocupan[207]. El Tratado de No Proliferación pide, en su Artículo 1, que los Estados poseedores de armas nucleares no permitan traspasar control "directa o indirectamente; y a no ayudar, alentar o inducir en forma alguna" a que otro Estado no poseedor controle dichas armas nucleares. El Artículo 2 del Tratado pide igualmente que dichos Estados no poseedores no acepten recibir control de manera directa o indirecta. Si el uso de la IA en sistemas de armas nucleares conlleva riesgos de seguridad para dichos sistemas, esto representa un riesgo jurídico para

[204] F. Safraoui, "Security Challenges and Air Sovereignty: Between Escalating Threats and the Need for Fortification", en *Qədim Diyar Beynəlxalq Elmi Jurnal*, vol. 7, n.º 2, 2025, p. 413.
[205] Tratado entrado en vigor el 5 de marzo de 1950, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 10485).
[206] M. Herrera, "La Intersección entre Inteligencia Artificial y Armas Nucleares: Riesgos, Beneficios y Recomendaciones", en *Revista UNISCI / UNISCI Journal*, n.º 67, enero 2025, p. 88.
[207] *Ibid*., p. 98-99.

cualquier Estado poseedor de armas nucleares que lo utilice y deje una metafórica puerta abierta al incumplimiento de estas obligaciones del Tratado.

Es importante notar igualmente que la IA en sí misma, o bien la que no esté vinculada a los sistemas de armas nucleares, se puede utilizar para llevar a cabo "ataques más avanzados y selectivos" en contra de instalaciones nucleares, sean militares o no[208]. El Organismo Internacional de Energía Atómica destaca por lo tanto sus recomendaciones frente a la ciberseguridad nuclear en la implementación de la IA, al igual que sus pautas para decidir qué procesos necesitan seguir siendo controlados por humanos[209].

Las armas nucleares se ven igualmente impactadas por la *operational unpredictability* de la IA en su funcionamiento frente al Derecho internacional y las obligaciones que tienen los Estados. Un sistema de la IA necesita, de nuevo, datos para funcionar y aplicarse. Por la simple razón de que el uso de armas nucleares es escaso en el mundo actual, crear un modelo de la IA que funcione dentro de estas significa utilizar datos sintéticos. Estos datos no sólo significarian mayor riesgo de alucinaciones—información incorrecta que la IA inventa pero alega ser cierta[210]—y vulnerabilidad en la ciberseguridad[211], sino también posibles omisiones frente a uso en tiempo real.

Finalmente, las armas nucleares presentan de nuevo la consideración del juicio humano en comparación con la actuación de una máquina. Asumiendo de nuevo que el elemento subjetivo del Artículo 2 del PA no se cuestiona, es decir, que el Estado asume responsabilidad trás el Artículo 11 u otro, el control de armas nucleares a mano de la IA conlleva riesgos. Estados Unidos, tras un reporte sobre esta tecnología emitido por su Comisión de Seguridad Nacional sobre Inteligencia Artificial, afirma como recomendación

[208] M. Hewes, ″Cómo la inteligencia artificial cambiará la seguridad informática y la seguridad física de la información en el mundo nuclear″, *Boletín del OIEA*, junio de 2023, p. 14. Publicado por el Organismo Internacional de Energía Atómica, disponible en https://www.iaea.org/sites/default/files/6421415es.pdf (última consulta: 31 de marzo de 2025).
[209] *Ibid.,* p. 15.
[210] Universidad Complutense de Madrid, *Certificado en Inteligencia Artificial… op. cit.*
[211] A. Saltini, "To avoid nuclear instability, a moratorium on integrating AI into nuclear decision-making is urgently needed: The NPT PrepCom can serve as a springboard", *European Leadership Network*, 28 de julio de 2023, disponible en https://europeanleadershipnetwork.org/commentary/to-avoid-nuclear-instability-a-moratorium-on-integrating-ai-into-nuclear-decision-making-is-urgently-needed-the-npt-prepcom-can-serve-as-a-springboard/ (última consulta: 31 de marzo de 2025). Véase igualmente M. Herrera, "La Intersección entre Inteligencia Artificial… *op. cit.*, p. 99.

de política nacional que las armas nucleares sólo puedan ser lanzadas por seres humanos, y "busca compromisos similares de parte de Rusia y China"[212].

1.4. Inteligencia estatal

El campo de la inteligencia estatal —la colección de información estratégica[213]— se ha beneficiado igualmente de la IA para desarrollarse. Si la obtención de datos mediante ordenadores empezó hace unos 50 años entre guerras[214] (alrededor de los propios comienzos de la IA en sí, como ya mencionado), la IA representa un cambio radical en el uso y procesamiento de esta información a través de su función catalizadora.

La colección de datos por ordenadores y otras tecnologías en general brindó muchas nuevas capacidades al Estado, pero también dio luz al concepto de *data smog*, una sobrecarga informativa por la magnitud de datos nuevamente disponibles[215]. Un ejemplo ilustrativo ofrecido por un ex miembro de la Agencia de Inteligencia Central de Estados Unidos (CIA, por sus siglas en inglés) es el de una operación del gobierno afgano en 2017, en la que se obtuvieron 40 terabytes de datos de una instalación de Al Qaeda. Si solo un cuarto de esos datos fueran de video, un agente tardaría más de seis meses trabajando sin parar, 24 horas al día, en revisar las grabaciones para identificar contenido potencialmente relevante[216]. La IA ofrece una solución completa a este problema, pudiendo así separar y preparar datos aún sin procesar para la revisión de profesionales en una fracción del tiempo que necesitaría una persona manualmente[217]. Por lo tanto, aunque los fundamentos de la inteligencia consisten aún en la obtención y protección de secretos de Estado, las maneras de manipulación están en una revolución de innovación[218].

---

[212] U.S. National Security Commission on Artificial Intelligence, *Final Report - National Security Commission on Artificial Intelligence*, 2021, p. 10, disponible en https://assets.foleon.com/eu-central-1/de-uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf (última consulta: 29 de marzo de 2025).
[213] R. J. Buchan, "The International Legal Regulation of Cyber Espionage", en A.-M. Osula y H. Rõigas (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn, 2016, p. 1, disponible en https://eprints.whiterose.ac.uk/id/eprint/98791/10/Russell_The%20International%20Legal%20Regulatio (última consulta: 5 de abril de 2025).
[214] G. Dimitrov, "A Brief History of Cyber Intelligence: How Did Computer Data Evolve to Be Used for Intelligence Operations", en *American Intelligence Journal*, vol. 37, n.º 1, 2020, p. 107.
[215] C. R. Moran, J. Burton y G. Christou, "The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying", en *Journal of Global Security Studies*, vol. 8, n.º 2, 2023, p. 10.
[216] E. Washabaugh, "The Robot, the Targeter and the Future of U.S. National Security", *The Cipher Brief*, 8 de marzo de 2021, disponible en https://www.thecipherbrief.com/the-robot-the-targeter-and-the-future-of-u-s-national-security (última consulta: 4 de abril de 2025).
[217] C. R. Moran, J. Burton y G. Christou, "The US Intelligence… *op. cit.*, p. 10.
[218] A. Vinci, "The Coming Revolution in Intelligence Affairs: How Artificial Intelligence and Autonomous Systems Will Transform Espionage", *Foreign Affairs*, 31 de agosto de 2020, disponible en https://www.foreignaffairs.com/articles/united-states/2020-08-31/coming-revolution-intelligence-affairs (última consulta: 3 de abril de 2025).

Desde un punto de vista estratégico y político, la potencias mundiales reconocen este poder revolucionario. En 2018, el entonces jefe del Servicio Secreto de Inteligencia britanico, Alex Younger, declaró la IA parte de la "cuarta generación del espionaje"[219] por su habilidad de dinamizar la inteligencia con máquinas en vez de personas. En Estados Unidos, el crecimiento hacia el desarrollo de la IA en la CIA ha crecido a un ritmo sin precedentes desde 2015, cuando la organización anunció su nueva Dirección de Innovación Digital[220]. En Suiza, un objetivo de su Plan de acción de ciberdefensa es implementar los "aspectos ciber" de su Ley de inteligencia, punto destacado en el reporte de 2021 sobre estrategias nacionales de la IA publicado por la Comisión Europea[221].

Jurídicamente, las implicaciones de la IA en la inteligencia complican la cuestión, pero no la transforman de manera drástica, como señala un comentario sobre el espionaje en particular publicado por la Universidad de Chicago[222]. El espionaje siendo un método destacable de obtener inteligencia[223], se entiende que el aspecto *no autorizado*[224] de esta se ve afectado por la IA en su totalidad. Tratando concretamente de espionaje, el Derecho internacional ha sido históricamente "extrañamente silencioso" al hablar de este en tiempos de paz, y limitado en su pronunciación en conflictos[225]. Efectivamente, el recurso jurídico más efectivo al hablar de la comisión de HII que involucran el uso de inteligencia estatal (y el espionaje en particular) es la potencial violación de la soberanía del Estado receptor de las medidas.

Mientras no existe un tratado internacional que regule directamente el espionaje (fuera de los acuerdos en contra recogidos en la *Convención de Viena sobre Relaciones Diplomáticas del 18 de abril de 1961*[226] y la *Convención de Viena sobre Relaciones Consulares del 24 de abril de 1963*[227]) en tiempos de paz, se entiende que la "actividad

[219] A. Younger, "MI6 'C' speech on fourth generation espionage", publicado por *Foreign & Commonwealth Office, Secret Intelligence Service*, 3 de diciembre de 2018, disponible en https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage (última consulta: 3 de abril de 2025).
[220] C. R. Moran, J. Burton y G. Christou, "The US Intelligence… *op. cit.*, p. 4.
[221] V. Van Roy *et al*, "AI Watch - National strategies on Artificial Intelligence: A European perspective", *Publications Office of the European Union,* 2022, p. 139, https://publications.jrc.ec.europa.eu/repository/handle/JRC129123 (última consulta: 27 de abril de 2025).
[222] J. Beim, "Enforcing a Prohibition on International Espionage", en *Chicago Journal of International Law*, vol. 18, n.º 2, art. 6, 2018, p. 671.
[223] R. J. Buchan, "The International Legal Regulation… *op. cit.*, p. 1.
[224] *Ibid.*, p.
[225] J. Beim, "Enforcing a Prohibition on International… *op. cit.*, p. 649.
[226] Tratado entrado en vigor el 24 de abril de 1964, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 7310).
[227] Tratado entrado en vigor el 19 de marzo de 1967, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 8638).

transfronteriza intrusiva" como el uso de la IA en dicho espionaje puede quebrar principios del Derecho internacional. Concretamente, vemos analizado de nuevo los que afectan directamente a la soberanía estatal[228], como argumento hacia la ilicitud del espionaje internacional en general[229] pero por usos de la IA en particular.

La IA mantiene su efecto catalizador al afectar a la soberanía primeramente por las nuevas posibilidades de intrusión en territorio ajeno que brinda. Si el control del territorio es una base fundamental de la soberanía estatal[230], la presencia de sistemas de vigilancia de parte de otros Estados que no cuenten con el consentimiento del Estado en cuyo territorio estén es una violación del Derecho internacional. Estas presencias de sistemas se multiplican con el beneficio de la IA, como es el caso ya observado de *Pegasus* de parte de Israel. Este sistema de vigilancia compuesto de IA se instala en teléfonos móviles para su monitorización total, y fue utilizada en primera instancia en Palestina. Su uso propagado hizo que la compañía creadora, NSO, llegará hasta tribunales por demandas de WhatsApp y Apple[231].

El aspecto del espionaje mediante la IA es por lo tanto un concepto fácil de imaginar. Si organizaciones como la Agencia Espacial Europea, previamente mencionada, tienen la capacidad de utilizar la IA para detectar y clasificar objetos tales como buques, nubes, "anomalías marinas", e incendios[232], las posibilidades para un Estado queriendo obtener información de otro son estas y muchas más. Además, la IA se utiliza igualmente a presente para coordinar ataques y facilitar la evasión de sistemas de seguridad a la hora de obtener información[233]. La cuestión jurídica a nivel de la inteligencia, y el espionaje en particular, resulta entonces estar en la posibilidad de regulación de una tecnología cataclísmica para la comisión de HII por la violación de estos principios y las obligaciones que resultan.

1.5. Injerencia en elecciones ajenas

Dentro de las operaciones militares estratégicas de los Estados, y más allá de la inteligencia a nivel fundamental, el acto de intervención en las elecciones de otros Estados se beneficia igualmente del uso de la IA, como comentado en el Capítulo I. La práctica política de injerencia en el proceso electoral de Estados clave tiene siglos de historia, y la estrategia

[228] R. J. Buchan, "The International Legal Regulation… *op. cit.*, p. 3.
[229] J. Beim, "Enforcing a Prohibition on International… *op. cit.*, p. 653.
[230] R. J. Buchan, "The International Legal Regulation… *op. cit.*, p. 4.
[231] C.H. Gray, *AI, Sacred Violence, and War—The Case of Gaza*, Palgrave Macmillan Cham, 2025, p. 89-90.
[232] European Space Agency, *New satellite… op. cit.*
[233] W. R. W. Rosli, "Waging Warfare Against States: The Deployment of Artificial Intelligence in Cyber Espionage", en *AI and Ethics*, vol. 5, 2025, p. 49-50.

en sí no ha cambiado[234]. Sin embargo, la innovación mediante la IA genera nuevas métodos para violar la soberanía estatal de esta manera. Se ha expuesto ya la incrementación de ciberataques a plataformas de elecciones, una clara manifestación de la función catalizadora de la IA[235]; se verá a continuación la prevalencia igualmente de la función creadora de la IA en el apoyo a comisión de HII. En particular, se analizan dos innovaciones utilizadas en tiempos recientes: los *bots* y los *deepfakes*[236].

Los *deepfakes* tienen creciente popularidad. Antes de las elecciones al Parlamento Europeo en junio de 2024, la involucración rusa en la UE intentó por ejemplo mitigar el apoyo a Ucrania mediante vídeos falsos. Para ello, Rusia se apoya en una respuesta "desigual y descoordinada" en Europa, más allá de los esfuerzos del Parlamento Europeo de incrementar la transparencia de contenido de IA en las plataformas que lo distribuyen[237]. Se puede apreciar igualmente la función catalizadora de la IA en este contexto. El uso de esta ha "reducido la barrera técnica de las capacidades requeridas para llevar a cabo tales operaciones"[238]. Se puede considerar por lo tanto que esto promueve una mayor atención y apoyo a la creación de estos contenidos falsos de parte de Estados con menos recursos técnicos, lo que se puede ver como una oportunidad de "reequilibrar" la jerarquía mundial en cuanto a la influencia estatal[239].

Los *bots* son similares a los *deepfakes* como ejemplo de la función creadora de la IA. No vienen de una práctica necesariamente existente; no hay comparación para el tipo de propaganda que se hace creando tal cantidad de "voces" falsas en la historia antes de la IA. Se considera por lo tanto que su uso nacional e internacional en las elecciones de Estados Unidos en 2016 fue "un hito en el desarrollo de la estrategia de comunicación política"[240]. Pese que el uso de *bots* sea aún una práctica "clandestina" en la cual se carece a menudo de toma de responsabilidad[241], tiene un impacto importante en la práctica y adherencia al Estado

---

[234] G. Hardesty, "Foreign Election Interference Has a Long History", University of Southern California – Sol Price School of Public Policy, 1 de noviembre de 2024, disponible en https://priceschool.usc.edu/news/foreign-election-interference-has-a-long-history/ (última consulta: 6 de abril de 2025).
[235] Cybersecurity and Infrastructure Security Agency… *op. cit.*
[236] J. Kenny, *Advanced Artificial Intelligence… op. cit.*, p. 235.
[237] I. Sánchez y G. Verdi, *Engaños digitales: Cómo un Escudo Europeo de la Democracia puede ayudar a hacer frente a la desinformación rusa*, 6 de junio de 2024, publicado por European Council on Foreign Relations, disponible en https://ecfr.eu/madrid/article/enganos-digitales-como-un-escudo-europeo-de-la-democracia-puede-ayudar-a-hacer-frente-a-la-desinformacion-rusa/ (última consulta: 31 de marzo de 2025).
[238] J. Kenny, *Advanced Artificial Intelligence… op. cit.*, p. 224.
[239] Ídem.
[240] D. Ramírez Plascencia *et. al*., "Digital Partisans: An Inquiry on the Use of Bots for Political Propaganda in Mexico", en *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, avance en línea, 2025, p. 3.
[241] *Ibid*., p. 4.

de Derecho internacional. Pese de venir en gran cantidad de Estados que violen "flagrantemente" otras de sus obligaciones, tal y como Rusia[242] (quien Meta calculó como la mayor fuente de desinformación en Facebook en 2021[243]), la práctica presenta un riesgo legislativo importante, especialmente en su popularización entre Estados. Al ver el extenso uso por Estados para intentar controlar los resultados políticos de otras regiones, como es el caso de Rusia o China con América Latina[244], nace la cuestión jurídica del nacimiento de HII otra vez mediante la IA. La injerencia de tal manera en la opinión pública de otro Estado es causa de llamamiento a la toma de "medidas concretas"[245] en la esencial totalidad de la literatura al respecto, señalando en particular la necesidad de "mecanismos legales" para ello[246].

Todas estas consideraciones respecto a armas e intervención internacional reflejan por lo tanto la idea que el uso de la IA facilita el estallido de conflictos y contribuye a una diferencia de poderes entre los Estados que pueden permitirse manipular sistemas de IA, en comparación con los que no[247]. Mientras que dicha diferencia de poderes no consta en sí misma de un riesgo adicional hacía la comisión de HII, la progresiva mejora en la accesibilidad de la IA y su función catalizadora en particular son riesgos de propagación a un mayor número de Estados. Si las grandes potencias utilizan esta herramienta tecnológica para avanzar sus intereses de manera ilícita, es cuestión de tiempo para que la práctica infiltre la comunidad global y de luz a un quebrantamiento de lo que sería el Estado de Derecho internacional.

2. Usos nacionales que constituyen hechos internacionalmente ilícitos

Más allá de lo que pueda hacer un determinado Estado con el empleo de la IA en sus fuerzas militares y para defenderse de ataques ajenos, hay otros usos de la tecnología que suceden a nivel nacional. Sin embargo, estos pueden igualmente llegar a ser HII si violan una

[242] N. de Rivière, "Russia Continues to Blatantly Violate International Humanitarian Law", declaración ante el Consejo de Seguridad, Misión Permanente de Francia ante las Naciones Unidas en Nueva York, 9 de octubre de 2023, disponible en https://onu.delegfrance.org/russia-continues-to-blatantly-violate-international-humanitarian-law (última consulta: 5 de abril de 2025).
[243] C. Hernandez-Roy, R. Bledsoe y G. Marma-Gutierrez, "Ensuring Information Integrity in Electoral Processes in the Americas", Center for Strategic & International Studies, 28 de julio de 2023, disponible en https://www.csis.org/analysis/ensuring-information-integrity-electoral-processes-americas (última consulta: 5 de abril de 2025).
[244] Ídem.
[245] Ídem.
[246] D. Ramírez Plascencia *et. al*., "Digital Partisans: An Inquiry… *op. cit*., p. 7.
[247] M. Giovanardi, "AI for Peace: Mitigating the Risks and Enhancing Opportunities", en *Data & Policy*, vol. 6, e41, 2024, p. 3.

obligación de Derecho internacional contratada por el Estado que cometa el hecho en cuestión. Los casos analizados aquí son por lo tanto sucesos a nivel nacional, aunque no se puede negar la existencia de situaciones similares a escala internacional igualmente.

2.1. Vigilancia nacional

La vigilancia de los integrantes de un Estado, es decir, en uso estrictamente nacional, puede presentar un riesgo ante obligaciones internacionales como las procedentes de los tratados que regulan los derechos humanos. Los sistemas de reconocimiento facial mediante IA, por ejemplo, al ser utilizados para vigilancia policial presentan un "dilema real" a la hora de cumplir con dichos derechos[248].

En el caso de esta aplicación en particular, el Tribunal Europeo de Derechos Humanos (TEDH) se pronunció en 2023, con el caso de *Glukhin versus Rusia*. Trás haber sido rastreado mediante reconocimiento facial, el demandante fue arrestado y recibió cargos administrativos[249]. Su caso llegó al TEDH, el cual determinó verse competente[250] para revisar la aplicación del *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales del 4 de noviembre de 1950*[251]. El Tribunal encontró así que los hechos representaban una violación del Artículo 8 del Convenio (que establece el derecho a la vida privada) y del Artículo 10 (la libertad de expresión)[252]. La pronunciación sobre el uso de la tecnología fue la siguiente:

> "...el Tribunal concluye que el uso de tecnología de reconocimiento facial altamente intrusiva en el contexto del ejercicio por parte del solicitante de su derecho a la libertad de expresión, amparado por el Convenio, es incompatible con los ideales y valores de una sociedad democrática regida por el Estado de derecho, que el Convenio fue diseñado para mantener y promover. El tratamiento de los datos personales del solicitante mediante tecnología de reconocimiento facial en el marco de procedimientos administrativos… no puede considerarse 'necesario en una sociedad democrática'"[253]

La vigilancia estatal no es una práctica nueva, por lo que se puede entender que la IA cumple aquí su función catalizadora al apoyar al Estado en sus actividades ya existentes. Sin embargo, se observa igualmente la función creadora al hablar de tecnologías completamente

[248] M. Giovanardi, "AI for Peace: Mitigating…" *op. cit.*, p. 4.
[249] STEDH de 13 de diciembre de 2022, *Asunto de Glukhin v. Rusia* (Aplicación no. 11519/20).
[250] *Ibid.*, párrafo 41. Pese a que Rusia cesó de ser parte del Convenio que establece la jurisdicción del Tribunal en 2022, se admite saber del caso ya que los hechos ocurrieron antes de la separación.
[251] Tratado entrado en vigor el 3 de septiembre de 1953, publicado en la Colección de Tratados del Consejo de Europa (número de registro ETS No. 005).
[252] F. Palmiotto y N. Menéndez González, "Facial Recognition Technology, Democracy and Human Rights", *Computer Law & Security Review*, vol. 50, 105857, 2023, p. 1.
[253] STEDH de 13 de diciembre de 2022, *Asunto de Glukhin v. Rusia*… *op. cit.*, párrafo 90.

nuevas que puedan crearse. En la práctica de revisar evidencia visual y identificar a individuos, por ejemplo, aunque se pueda hacer manualmente, la IA facilita el hecho a "una escala masiva e indiscriminada"[254] con su habilidad de crear novedosas herramientas de reconocimiento facial. El riesgo relacionado a la comisión de HII es por lo tanto el potencial de la tecnología para innovar en métodos que vayan en contra de los derechos humanos.

2.2. Uso de datos personales

Como mencionado previamente, la IA depende de una gran cantidad de datos para su análisis y funcionamiento. Para su uso en el ámbito nacional en herramientas que se basen en la población de un país determinado, es por lo tanto esencial obtener dichos datos dentro del propio Estado. Sin embargo, no todas las recolecciones de información por un Estado dentro de su mismo territorio son lícitas bajo el Derecho internacional, ya que se pueden infringir algunas obligaciones internacionales con respecto al uso de datos personales, creando así un potencial HII. La IA permite en estas instancias ejercer sobre todo su función creadora en la innovación de sistemas que facilitan la obtención de estos datos potencialmente en contra de las obligaciones de un Estado.

Este trabajo se apoya en la definición de datos personales establecida en el Artículo 4(1) del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*[255] (más conocido como la Ley de Protección de Datos de la UE). Concretamente, este dicta que los datos personales son:

> "…toda información sobre una persona física identificada o identificable…; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"

La Ley de Protección de Datos es por lo tanto clara sobre lo que compone dichos datos, y como su propio título indica trata sobre lo "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". Este apartado se sirve entonces de la definición proporcionada por esta Ley, siguiendo el

[254] Consejo de Derechos Humanos de las Naciones Unidas, Informe A/HRC/44/24*, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests* (2020), p. 9.
[255] Reglamento entrado en vigor el 25 de mayo de 2018, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 32016R0679).

argumento de que esta es "la legislación de protección de datos más influyente" y que su alcance en la práctica se extiende más allá de Europa[256].

Para los Estados miembros de la UE, el uso de la IA que no cumpla con la Ley de Protección de Datos podría ser un potencial HII. Al ser parte de la UE, estos Estados se comprometen a seguir las obligaciones generadas por el *Tratado del Funcionamiento de la Unión Europea del 13 de diciembre de 2007*[257]. Una de estas obligaciones, recogida en el Artículo 288, es que "[cada] reglamento…[es] obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro". A causa de esto, los elementos delineados en el Artículo 2 del PA 2001 se verían potencialmente cumplidos para establecer la comisión de un HII, generando así la responsabilidad internacional del Estado en cuestión.

En el Derecho internacional más allá de la UE, sin embargo, cuenta con una mención importante hacia la privacidad en general, que ha sido en torno adaptada a los datos personales. Se analiza en este caso el Artículo 17(1) del *Pacto Internacional de Derechos Civiles y Políticos del 16 de diciembre de 1966*[258] (en adelante PIDCP), que concreta que "[n]adie será objeto de injerencias arbitrarias o ilegales en su vida privada…". La interpretación de este artículo ha sido ampliamente compatible con la privacidad en el ámbito digital, como aclara el propio comentario de la ONU indicando que "[l]a recopilación y el registro de información personal en computadoras… deben estar reglamentados por la ley" y que "toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados…"[259].

Fuera de las obligaciones estatales generadas por el Derecho internacional, resoluciones de la Asamblea General de la ONU cristalizan la importancia de la protección de datos personales en la práctica jurídica global. Este es el caso por ejemplo de la Resolución 68/167, aprobada por la Asamblea General en 2013[260], la cual reafirma el Artículo 17 del PIDCP y "[e]xhorta a todos los Estados" que analizen y mantengan sus sistemas nacionales de recopilación de datos en armonía con el derecho a la privacidad.

---

[256] C. Kuner et al., "The GDPR as a Chance to Break Down Borders", en *International Data Privacy Law*, vol. 7, n.º 4, 2017, p. 231.
[257] Tratado entrado en vigor el 1 de diciembre de 2009, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 12016ME/TXT).
[258] Tratado entrado en vigor el 23 de marzo de 1976, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 14668).
[259] Comité de Derechos Humanos, Observación general núm. 16 (32º período de sesiones, 1994), doc. ONU HRI/GEN/1/Rev.1, (1994), p. 27, párr. 10.
[260] Asamblea General de las Naciones Unidas, Resolución 68/167, "El derecho a la privacidad en la era digital", Doc. A/RES/68/167 (2013).

La cuestión vuelve entonces sobre la IA, y su función creadora en el apoyo al posible incumplimiento de estas obligaciones y recomendaciones. Hemos visto anteriormente el caso de *Glukhin versus Rusia*[261] como ejemplo, que pese a estar enfocado en la vigilancia estatal incluye este mismo uso de datos personales en contra del derecho a la privacidad establecido no solo en el Convenio para la Protección de los Derechos Humanos del Consejo de Europa ya mencionado, sino también en el PIDCP (del cual Rusia es Estado parte desde 1973). La creación de herramientas de IA que permitan el rastreamiento y reconocimiento facial (lo que consiste un dato personal al basarse en "elementos propios de la identidad física"[262]) impulsó en este caso un potencial HII, dentro del propio territorio ruso.

Finalmente, es importante considerar que el caso de protección de datos con respecto a la IA es un tema con amplia consideración e interpretación nacional. Otros Estados emplean una política defensiva frente a las nuevas herramientas creadas, la cual se puede argumentar ayuda a prevenir la posible comisión de HII. Hasta en países de la UE, que gozan de una Ley de Protección de Datos considerada académicamente un "paso en la dirección correcta"[263], nuevas aplicaciones de la IA pueden ser consideradas una amenaza jurídica con respecto a dicha Ley.

Un caso evidente de esta presentación es el de Italia. Unos seis meses después de la entrada al mercado del conocido ChatGPT[264], la herramienta fue prohibida en el territorio italiano, bajo la autoridad de su agencia nacional de protección de datos (en italiano, *Garante per la protezione dei dati personali*). La organización citó dos preocupaciones: la falta de verificación de edad para menores, y la colección de datos de manera ilícita. Para esta última razón, se señaló una "falta de información" dada a las personas cuya información estaba siendo almacenada, y la "ausencia de una base jurídica" que permita la colección y conservación de datos de usuarios italianos con fin de entrenar y mejorar la plataforma[265]. La

[261] STEDH de 13 de diciembre de 2022, *Asunto de Glukhin v. Rusia… op. cit.*
[262] Según la definición mencionada en Artículo 4(1) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.
[263] A. D. Vanberg, "Informational Privacy Post GDPR – End of the Road or the Start of a Long Journey?", en *The International Journal of Human Rights*, 25(1), 2020, p. 2.
1789109 (última consulta: 5 de abril de 2025).
[264] OpenAI, "Introducing ChatGPT", 30 de noviembre de 2022, disponible en https://openai.com/index/chatgpt/ (última consulta: 14 de abril de 2025).
[265] Garante per la protezione dei dati personali, "Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori", 31 de marzo de 2023, disponible en https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847 (última consulta: 14 de abril de 2025).

agencia italiana consideraba de esta manera que la plataforma no cumplía con ciertos requisitos de la Ley de Protección de Datos[266].

ChatGPT fue eventualmente reinstaurado con unas modificaciones técnicas, como entre otras la posibilidad del usuario de borrar sus datos personales recogidos, o bien de optar por no participar en el entrenamiento del algoritmo con dichos datos igualmente[267]. Se puede argumentar que, trás este suceso en algunos casos criticado por haber sido "impopular e ineficaz"[268], Italia consiguió protegerse de una herramienta que podría potencialmente conducir al Estado a infringir la Ley de Protección de Datos. En particular, el Artículo 57 de esta describe las funciones que "la autoridad de control principal" (en este caso, el *Garante per la protezione dei dati personali)* tiene que desempeñar, una de estas siendo "un seguimiento de cambios que sean de interés" según el apartado (i).

2.3. Algoritmos discriminatorios/en contra de los derechos humanos

Otra amenaza de la IA en sus usos nacionales que constituye un HII en determinadas situaciones es su incorporación en algoritmos con sesgos determinados hacía parte de una población. La discriminación estatal no es una novedad en la historia, por lo que la IA aplica a ello su función catalizadora para desarollar sistemas de práctica que permiten a los Estados promover estas estrategias, sea activamente en contra o por omisión al seguimiento[269] de los derechos humanos.

El primer ejemplo de esta función aplicada está en la ya mencionada posibilidad de sesgos en los datos de la IA. Las bases de información que informan estos sistemas tienen la alta probabilidad de ser sesgados por quien los proporcione; siguiendo el ejemplo dado previamente, un sistema que funciona en base a lo que le proporciona un equipo enteramente compuesto de hombres corre el riesgo de estar sesgado para discriminar a favor de los hombres y/o en contra de las mujeres[270]. A la hora de crear algoritmos para herramientas de uso estatal, si estos sesgos no son corregidos, el Estado podría estar en contra una de sus

[266] F. Gualdi y A. Cordella, "Theorizing the Regulation of Generative AI: Lessons Learned from Italy's Ban on ChatGPT", en *Proceedings of the 57th Hawaii International Conference on System Sciences*, 2024, p. 2026.
[267] F. Gualdi y A. Cordella, "Theorizing the Regulation… *op. cit.*, p. 2027.
[268] F. Bolici *et al*., "Unpopular Policies, Ineffective Bans: Lessons Learned from ChatGPT Prohibition in Italy", en *ECIS 2024 Proceedings European Conference on Information Systems (ECIS)*, Università di Cassino e del Lazio Meridionale, junio 2024, p. 11.
[269] Se resalta de esta manera la relevancia de la omisión como base válida para la comisión de un HII. Véase J. B. Cartes Rodríguez, "*Clase sobre los Hechos Internacionalmente Ilícito*s", en *El Ordenamiento Jurídico Internacional: Sujetos y Normas*, Máster en Derecho internacional 2024-2025, Universidad Complutense de Madrid, 29 de octubre de 2024.
[270] Universidad Complutense de Madrid, *Certificado en Inteligencia Artificial… op. cit.*

obligaciones internacionales, como por ejemplo el derecho a la no discriminación recogido en el Artículo 26 del PIDCP. A estos efectos, aunque el Estado utilizando el algoritmo no lo haya diseñado o establecido activamente en contra del grupo que está discriminando, la violación por omisión de las obligaciones de un Estado sigue siendo, según el Artículo 2, elemento constitutivo de un HII.

Un caso importante en la práctica nacional es el del algoritmo COMPAS en Estados Unidos. El sistema, con su nombre completo siendo *Correctional Offender Management Profiling for Alternative Sanctions* (en español, equivaldría a "Perfilado de Gestión Correccional de Delincuentes para Sanciones Alternativas") es una herramienta computacional popular en juzgados estadounidenses[271]. Esta se utiliza sobre todo para evaluar el riesgo de reincidencia a la hora de tomar decisiones cuantitativas como las de fianzas o sentencias, y tiene el objetivo de crear un sistema judicial "eficaz y acelerado"[272]. Sin embargo, COMPAS fue analizado en 2016 para descubrirse que tenía sesgos realizados en la práctica de señalar el nivel de reincidencia, dando tasas incorrectamente altas comparadas con la realidad a un mayor número de personas afroamericanas. Inversamente, daba una tasa falsamente baja a un mayor número de personas de raza blanca[273]. El análisis se hizo comparando la puntuación de COMPAS con la realidad de las personas puntuadas dos años después; el algoritmo acertó en un 61% de casos de reincidencia, pero solo en un 20% de reincidencia violenta. En esta última tasa, puntuada por separado, las personas afroamericanas tenían una probabilidad 77% más alta que las blancas de ser cualificadas para reincidencia violenta, siendo esto al controlar los factores en juego como la edad o el historial criminal[274].

El uso de COMPAS constituye, por lo tanto, un riesgo a la obligación de no discriminación a nivel estatal bajo el Derecho internacional. Aunque la invocación del mismo Derecho internacional es improbable en estos casos (ya que el uso de COMPAS es notable sobre todo a nivel de los condados en Estados Unidos y que se deberían primero agotar los recursos internos del territorio), sigue siendo un riesgo para dicho Estado. La función catalizadora de la IA continuará apoyando la propagación de sistemas como estos. Si no se

[271] N. Kartha y W.D. Young, *An Overview of Algorithmic Bias in Artificial Intelligence*, University of Texas at Austin, p. 4, https://hdl.handle.net/2152/86530 (última consulta: 14 de abril de 2025).
[272] Ídem.
[273] J. Larson et al., "How We Analyzed the COMPAS Recidivism Algorithm", ProPublica, 23 de mayo de 2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm (última consulta: 14 de abril de 2025).
[274] Ídem.

presta atención a la regulación y el ajuste de los datos utilizados, los sesgos se multiplicarán conllevando igualmente a un riesgo jurídico exponencial.

De la misma manera que aplica la función catalizadora de la IA en este apartado, vemos igualmente su función creadora por la facilitación brindada a sistemas que rompen los moldes de lo ya conocido. Un ejemplo notable es el sistema de puntuación social en China, el cual consiste en realidad en alrededor de 36 sistemas diferentes usados en varias regiones del país[275]. Estos tienen como objetivo colectivo puntuar el comportamiento de los ciudadanos[276], tras acciones diarias como la compra de gasolina o quebrantamientos menores y mayores de la ley[277]. La puntuación resultante da acceso o bien prioridad a servicios tal y como mejores cuidados médicos, conexiones web más rápidas, u oportunidades de inversión, entre otros[278]. Pese a que China no sea un Estado ejemplo para invocar la violación de obligaciones bajo el PIDCP, ya que firmó el Tratado en 1998 pero nunca lo ratificó, este algoritmo es un ejemplo perfecto para ilustrar las potencialidades de quebrantamiento de derechos humanos en un territorio. La IA permite, tras su función creadora, clasificar y discriminar a ciudadanos de una manera que no era posible antes.

Considerando estos ejemplos conjuntos con el resto de este Capítulo, es por lo tanto imprescindible que la regulación internacional preste especial atención a las funciones de la IA en la práctica. La comisión de HII no es novedosa en el comportamiento de los Estados, y pese a que la IA pueda apoyar a limitarla, se prevén igualmente varias situaciones donde esta tecnología podría presentar un riesgo de responsabilidad internacional de los Estados en su potencial comisión de HII.

[275] V. Agrawal, "Demystifying the Chinese Social Credit System: A Case Study on AI-Powered Control Systems in China", en *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, n.º 11, 2022, p. 13124.
[276] V. Vinayak, "The Human Rights Implications of China's Social Credit System", Oxford Human Rights Hub, 6 septiembre 2019, https://ohrh.law.ox.ac.uk/the-human-rights-implications-of-chinas-social-credit-system/ (última consulta: 14 de abril de 2025).
[277] V. Agrawal, "Demystifying the Chinese Social Credit System… *op. cit.*
[278] V. Vinayak, "The Human Rights Implications of China's Social Credit System... *op. cit.*

V. REGULACIÓN ACTUAL DE LA INTELIGENCIA ARTIFICIAL EN DERECHO INTERNACIONAL

Al haber expuesto así los usos de la IA para avanzar los intereses de los Estados, al igual que las funciones de aplicación negativa sobre las obligaciones de estos mismos, es indispensable recurrir al Derecho internacional existente para formar un análisis completo de la situación jurídica global actual. Para ello, se estudia a continuación las normas y regulación existentes tratando sobre la IA en particular, así como los desafíos y las limitaciones que presentan en vista a la práctica estatal con esta tecnología y los valores previamente expuestos.

Aunque las capacidades del Derecho internacional consuetudinario sean nulas en cuanto a implementaciones que apliquen directa y exclusivamente a las nuevas tecnologías, la generalidad de algunos principios (como los mencionados previamente) permite una aplicación *de facto* a nuevos desarrollos como la IA. Como avenida de cierre entre la *lex lata* y *lex ferenda* relevante a ello, existen desde los últimos años varias expresiones jurídicas internacionales que abordan la cuestión.

1. Normas y regulación existente

Pese a la relativamente "lenta" toma de decisiones a nivel de Derecho internacional[279] que menciona la literatura revisada sobre este tema, se presentan ya varias proposiciones jurídicas estatales y de parte de organizaciones internacionales para abordar la regulación de la IA. Revisaremos aquí los dos textos más importantes a nivel global, así como una generalidad de otras expresiones internacionales sobre el tema.

1.1. Reglamento de la Inteligencia Artificial de la Unión Europea

El primero de los dos textos más reconocidos, cronológicamente, es el *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024*[280] (abreviado aquí como Reglamento de la IA, o RIA[281]). Este Reglamento de la UE se convirtió en el primer texto vinculante sobre la IA a fecha de su entrada general en vigor en agosto de 2024. Su ámbito general es la institución de normas homogéneas para el desarrollo y uso, así como

[279] A. Hárs, "AI and international law – Legal personality… *op. cit.*, p. 321.
[280] Reglamento entrado en vigor el 1 de agosto de 2024, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 32024R1689).
[281] Otros textos en castellano se refieren igualmente a esta ley como *EU AI Act* por su nombre en inglés, véase por ejemplo M. Peguera Poch y B. Arribas Sánchez, *Perspectivas regulatorias de la inteligencia artificial en la Unión Europea*, 1ª ed., Reus, 2023.

presentación al mercado, de aplicaciones de IA en la UE[282]. Se trata por lo tanto de un instrumento sobre la seguridad de los productos de la IA, al igual que un intento "nominal" de destacar los derechos fundamentales frente a esta nueva tecnología[283].

El RIA es un texto clasificador; separa los sistemas de IA basados en su riesgo. Las visualizaciones del acto representan frecuentemente el RIA como una pirámide[284], con cuatro niveles: sistemas de riesgo mínimo (*e.g.* videojuegos o filtros de spam) en la base, despues riesgo limitado (*e.g. bots* y *deepfakes*), alto (*e.g.* IA utilizada en educación o juzgados), e inaceptable (*e.g.* puntuación social o reconocimiento facial) en la cima. Cada nivel de riesgo se acompaña de una obligación de regulación diferente, partiendo de simples códigos de conducta para riesgos mínimos a la prohibición total de riesgos inaceptables[285]. Estos últimos se prohibieron definitivamente en la región en febrero de 2025, siendo el primer paso en una aplicación a plazos, que concluirá 24 meses después de la entrada en vigor[286]. El RIA será por lo tanto aplicable en su totalidad a partir del 1 de agosto de 2026.

Este texto se dirige principalmente al uso de la IA en el sector público y para aplicaciones estatales[287]. El incumplimiento de las medidas del RIA y las aplicaciones que se les pide a los Estados miembros está recogido en el Artículo 99 del texto, y consiste en multas de varios millones de euros o cierto porcentaje del volumen de negocios anual total mundial del infractor, similar a la Ley de Protección de Datos de la UE[288]. Efectivamente, el RIA existe como una expansión de esta, trabajando en conjunto con las disposiciones existentes[289]

La revisión académica del RIA es generalmente positiva, con la literatura estando mayoritariamente de acuerdo que hay "mucho que aplaudir"[290] en lo que es el primer

[282] L. Edwards, *The EU AI Act: a summary of its significance and scope*, Ada Lovelace Institute, abril 2022, p. 4, https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf (última consulta: 16 de abril de 2025).
[283] M. Almada y N. Petit, "The EU AI Act : between the rock of product safety and the hard place of fundamental rights", en *Common market law review*, Vol. 62, No. 1, 2025, p. 119.
[284]S. González, "Claves del Reglamento Europeo de Inteligencia Artificial (RIA)", ITCL Centro Tecnológico, 14 marzo 2024, disponible en https://itcl.es/blog/reglamento-europeo-inteligencia-artificial/ (última consulta: 16 de abril de 2025).
[285] L. Edwards, *The EU AI Act: a summary of its significance and scope… op. cit.*, p. 9.
[286] Parlamento Europeo, *Ley de IA de la UE: primera normativa sobre inteligencia artificial*, 12 de junio de 2023, https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial#calendario-de-aplicacin-de-la-ley-de-ia-de-la-ue-6 (última consulta: 16 de abril de 2025).
[287] L. Edwards, *The EU AI Act: a summary of its significance and scope… op. cit.*, p. 4.
[288] *Ibid.*, p. 5.
[289] *Ibid.*, p. 4.
[290] C. Boine y D. Rolnick, *Why the AI Act Fails to Understand Generative AI*, publicado en *We Robot 2023 Conference, Boston University School of Law*, 30 de junio de 2023, p. 39, https://papers.ssrn.com/sol3/papers

mecanismo significativo a la hora de regular la IA a nivel internacional. Existen igualmente perspectivas de profesionales jurídicos que consideran el RIA un texto "visionario e innovador" que puede servir de modelo global a la hora de avanzar la legislación sobre la IA a nivel mundial[291].

Sin embargo, varios juristas consideran que el texto tiene lagunas significativas. Un análisis presentado en la conferencia "We Robot" 2023 en la Facultad de Derecho de la Universidad de Boston considera que el sistema cuatripartita de riesgos no es adecuado para regular la IA generativa[292]. La crítica observa que el RIA está construido con la perspectiva de otras regulaciones sobre la seguridad de productos comercializados en la UE, un punto de vista que limita el alcance de los requisitos al propósito previsto para las aplicaciones de la IA[293]. Por lo tanto, consideran que esto implica una "fuerte correlación positiva" entre el nivel de riesgo de una aplicación de la IA y su propósito previsto. Esto resulta problemático al no siempre ser cierto, y al no considerar los sistemas de IA que no tienen un propósito previsto en concreto[294]. Este análisis concluye entonces que el marco tradicional de clasificación de riesgos como presenta el RIA es "inadecuado" y que se ha de desechar el "enfoque de seguridad de los productos al estilo de la UE" a la hora de regular la IA[295].

Otras críticas rechazan la idea de utilizar el RIA como modelo para otras regulaciones en otras partes del mundo, como es el caso de un análisis de parte de juristas en la Facultad de Derecho de la Universidad de Emory. Opinan de tal manera que el Reglamento no se ha de considerar una perspectiva "*rights-driven*"[296] ni imperativa en su protección de derechos fundamentales frente a la IA, sino un producto de un contexto político con cultura e historia precisa[297]. Por lo tanto, argumentan claramente que "lo que funciona en Europa puede no funcionar en otro lugar"[298], un punto importante que considerar en este trabajo a la hora de presentar conclusiones sobre el futuro de la regulación global de la IA. Igualmente, otra crítica publicada por el Instituto Universitario Europeo indica que las referencias a los

.cfm?abstract_id=4644701 (última consulta: 16 de abril de 2025).
[291] T. Evas, "The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI", en *Journal of AI Law and Regulation*, Volume 1, Issue 1, 2024, p. 101.
[292] C. Boine y D. Rolnick, *Why the AI Act Fails… op. cit.*, p. 14.
[293] *Ibid*., p. 17.
[294] *Ibid*., p. 20.
[295] *Ibid*., p. 39.
[296] La traducción literal al castellano es "conducida por derechos", pero la traducción correcta sería "basada en derechos". Esta última sin embargo no transmite la totalidad de la idea emitida por el texto original, razón por la cual se opta por dejar el término en inglés.
[297] Y. Mei y M. Sag, *The Illusion of Rights based AI Regulation*, 27 de febrero de 2025, p. 3, https://doi.org/10.48550/arXiv.2503.05784 (última consulta: 16 de abril de 2025).
[298] *Ibid*, p. 59.

derechos fundamentales son "generales", y el RIA inadecuado en sí mismo para regularlos al ser un instrumento de seguridad frente a riesgos en productos[299]. Este último punto se resalta en el análisis de este trabajo a continuación, en relación con el percibido Estado de Derecho internacional y la contribución de la regulación de la IA en ello.

1.2. Tratado del Consejo de Europa

El segundo texto jurídico sobre la IA más relevante para el Derecho internacional a nivel global es el más reciente: el Tratado abierto a firma por el CdE, el llamado *Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y derechos humanos, democracia y Estado de derecho del 5 de septiembre de 2024*[300] (en adelante, TCdE, o bien Tratado del CdE). Este texto fue abierto a firma en Vilnius en septiembre de 2024, tras dos años de negociaciones del Comité de Inteligencia Artificial. Este último colaboró con 46 Estados miembros del CdE, la UE, y 11 Estados no miembros del CdE en su creación[301]. Unos meses después, a fecha de abril de 2025, tiene 14 Estados firmantes (incluyendo cuatro no miembros del CdE, Israel, Estados Unidos, Canadá y Japón) además de la UE.

El texto es breve, contenido en sólo 12 páginas (comparable con las 144 del RIA). Las consideraciones generales, recogidas en el título, están concentradas en el Capítulo II. En este, el Artículo 4 enfatiza la protección de los derechos humanos, y el Artículo 5 la integridad de los procesos democráticos y el respeto al Estado de Derecho. Ha de notarse entonces, que este Tratado intenta promover este concepto ya mencionado. A estos fines, el Capítulo III recoge algunos principios tecnológicos que han de gobernar la IA, siendo estos de naturaleza operacional (como Artículo 8 "Transparencia y supervisión", o Artículo 9 "Rendición de cuentas y responsabilidad") y ética (por ejemplo, Artículo 7 "Dignidad humana y autonomía individual", o Artículo 10 "Igualdad y no discriminación").

Al ser relativamente nuevo, el TCdE no goza de una crítica académica extensa sobre lo que es el Tratado realizado. La mayoría de los puntos de vista disponibles fuera del CdE analizan sobre todo los borradores, y la evolución de puntos claves como la enfatización de

[299] M. Almada y N. Petit, "The EU AI Act : between… *op. cit.*, p. 86.
[300] Tratado abierto a firma el 5 de septiembre de 2024, aún no entrado en vigor, publicado en la Colección de Tratados del Consejo de Europa (número de registro 225).
[301] Newsroom, "*Council of Europe adopts first international treaty on artificial intelligence*", 17 de mayo de 2024, publicado por el Consejo de Europa, disponible en https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence (última consulta: 31 de marzo de 2025).

los derechos humanos[302] o definiciones de la IA que coincidan con las del RIA[303]. Sobre este último punto, existen igualmente varias evaluaciones de ambos instrumentos. Algunas son de extensión simplemente informativas, como la de la Sociedad irlandesa de informática[304], mientras que algunas se adentran en la falta de mecanismos de aplicación "fuertes" comparado con el RIA[305]. Otras notan, como visto a continuación, la dificultad de aplicación del TCdE en comparación con el Reglamento por su necesidad de ser ratificado para entrar en vigor[306].

Más allá de su análisis académico, sin embargo, el texto del propio TCdE presenta dos limitaciones importantes en cuanto a su estado actual. Primero, cabe destacar que el Tratado no está abierto a firma globalmente. Su Artículo 30.1 requiere que la posibilidad de firma solo se presente a "los Estados no miembros que hayan participado en su elaboración", además de los miembros del CdE y la UE. El Artículo 31.1 provee la accesión (después de la entrada en vigor) de otros Estados ajenos al CdE solo tras invitación, necesitando el requisito tripartita de: consentimiento por unanimidad de las Partes del Tratado, mayoría de dos tercios en el Comité de Ministros del propio CdE, y unanimidad de los representantes de las Partes presentes en dicho Comité. Considerando los requisitos administrativos, y el número de Estados de influencia ausentes en la elaboración (como, por ejemplo, India, Brasil, o bien Corea del Sur), esta dificultad del ámbito global y de la libre participación al Tratado no se puede ignorar.

En segundo lugar, y con mayor notabilidad, el TCdE no ha entrado en vigor. A fecha de abril de 2025, ningún Estado ha ratificado el Tratado. Pese de haber sido firmado por un creciente número de países con distribución global, el Artículo 30(2) estipula que no entrará en vigor hasta que cinco (tres siendo miembros del CdE) lo ratifiquen. Sin ámbito de adentrarse en este trabajo en las razones por las cuales tantos Estados pueden haber firmado

[302] E. H. Morawska, *Council of Europe standards and activities related to AI: towards a Framework Convention on AI and human rights?*, en M. Balcerzak y J. Kapelańska-Pręgowska (eds.), *Artificial Intelligence and International Human Rights Law*, 2024, p. 36.
[303] *Ibid*., p. 37.
[304] Irish Computer Society, *Comparison of Council of Europe Framework Convention on Artificial Intelligence with the European Union Artificial Intelligence Act*, 29 de octubre de 2024, disponible en https://ics.ie/2024/10/29/comparison-of-council-of-europe-framework-convention-on-artificial-intelligence-with-the-european-union-artificial-intelligence-act/#:~:text=Legal%20Scope%20and%20binding%20nature,third%20countries%20around%20the%20world. (última consulta: 16 de abril de 2025).
[305] C. Chang, "The First Global AI Treaty: Analyzing the Framework Convention on Artificial Intelligence and the EU AI Act", en *University of Illinois Law Review (Online)*, 86, 2024, p. 97.
[306] J. Ziller, "The Council of Europe Framework Convention on Artificial Intelligence vs. the EU Regulation: two quite different legal instruments", en *Fascicolo 2/2024*, CERIDAP, 2024, p. 222.

pero aún no ratificado (al ser una realidad política), esto representa un evidente obstáculo para la efectividad global de las propuestas del TCdE.

1.3. Otras expresiones internacionales

Más allá de los textos de la UE o del CdE, varias organizaciones internacionales se han pronunciado sobre la IA en su ámbito. En marzo de 2024, la Asamblea General de la ONU aprobó su Resolución 78/265, titulada "Aprovechar las oportunidades de sistemas seguros y fiables de inteligencia artificial para el desarrollo sostenible"[307]. Esta reconoce las oportunidades que tiene la IA de promover la realización de los 17 Objetivos de Desarrollo Sostenible[308], pero que el uso negativo de la tecnología podría al contrario socavar el progreso[309]. La Resolución recomienda por lo tanto que los Estados dejen de usar IA que no se pueda considerar "en consonancia con el derecho internacional" o los derechos humanos, y la protección de estos mismos. Respalda que la manera de hacerlo es mediante la creación y aplicación de "marcos regulatorios y gobernantes nacionales", que se enfoquen entre otro la protección de los datos personales y la evaluación de riesgos[310]. En junio del mismo año, la Asamblea General coordinó igualmente un borrador de Resolución 78/L.86, para fomentar la cooperación internacional en la adopción de la IA y reducir brechas regionales[311].

La ONU formó igualmente en octubre de 2023 un Órgano Asesor de Alto Nivel para la IA, como parte de su Oficina de Tecnologías Digitales y Emergentes[312]. Este Órgano se encargó de la creación de un reporte llamado "Gobernar la IA para la Humanidad"[313], publicado en septiembre de 2024.

En 2022, la OECD publicó su reporte sobre el "Uso estratégico y responsable de la inteligencia artificial en el sector público, el cual provee a los Estados "[r]ecomendaciones para promover un enfoque de la IA responsable, fiable y centrado en el ser humano"[314]. Estas

---

[307] Asamblea General de las Naciones Unidas, Resolución 78/265, "Aprovechar las oportunidades de sistemas seguros, protegidos y fiables de inteligencia artificial para el desarrollo sostenible", Doc. A/RES/78/265 (2024).
[308] *Ibid.*, p. 2. Véase Organización de las Naciones Unidas, *United Nations Sustainable Development Goals*, disponible en https://www.un.org/sustainabledevelopment/ (última consulta: 17 de abril de 2025).
[309] *Ibid.,* p. 3.
[310] *Ibid.,* p. 5-6.
[311] Asamblea General de las Naciones Unidas, borrador de Resolución "Aumentar la cooperación internacional para la creación de capacidad en materia de inteligencia artificial", Doc. A/78/L.86 (2024).
[312] High-Level Advisory Body on Artificial Intelligence, *United Nations Office for Digital and Emerging Technologies*, disponible en https://www.un.org/digital-emerging-technologies/ai-advisory-body (última consulta: 16 de abril de 2025).
[313] United Nations AI Advisory Body, *Governing AI for Humanity: Final Report*, eISBN: 9789211067873 (2024).
[314] Organisation for Economic Co-operation and Development/CAF, *Uso estratégico y responsable de la inteligencia artificial… op. cit.*, p. 195.

incluyen varios conceptos previamente mencionados, como el desarrollo de un marco ético, la reducción de sesgos, o bien rendición de cuentas[315]. La OECD reafirmó en 2024 con otro reporte—esta vez enfocado en el desarrollo económico y del mercado laboral—que la IA presenta el riesgo de aumentar la desigualdad de desarrollo tecnológico entre regiones urbanas y rurales en los propios Estados, por lo que estos han de priorizar la "infraestructura digital" en su desarrollo[316]. Estos reportes se deben de considerar sobre la base de los principios establecidos por la misma OECD en su Recomendación del Consejo de IA[317], publicada en 2019 y revisada en 2024. Dichos principios, seguidos de recomendaciones para la implementación de una "administración responsable" de la IA, son cinco:

> "…i) crecimiento inclusivo, desarrollo sostenible y bienestar; ii) respeto del Estado de derecho, los derechos humanos y los valores democráticos, incluida la equidad y la privacidad; iii) transparencia y explicabilidad; iv) solidez, seguridad y protección; y v) rendición de cuentas.[318]"

Estos principios son igualmente la base de los principios sobre la IA adoptados por los líderes del G20 en junio de 2019. Estos últimos, publicados por el Ministerio de Asuntos Exteriores de Japón[319], son exactamente los mismos excepto el segundo, el cual cambia a ser "Valores centrados en el ser humano y equidad". Queda retirado de la mención titular del respeto al Estado de Derecho, pero reaparece en los detalles del propio principio, como elemento que los actores de la IA han de respetar e implementar mediante mecanismos apropiados y respaldos[320].

El marco ético de la IA fue abordado también por la Recomendación sobre la Ética de la IA presentada por la UNESCO en 2022[321]. Esta se guía por diez principios, mencionando por lo tanto algunos conceptos adicionales que la OECD o el G20, como la proporcionalidad

---

[315] *Ibid*., p. 195-197.
[316] Organisation for Economic Co-operation and Development, *La IA generativa podría exacerbar las divisiones regionales en los países de la OCDE, según el primer análisis regional sobre su impacto en los mercados laborales locales*, 28 de noviembre de 2024, https://www.oecd.org/es/about/news/press-releases/2024/11/generative-ai-set-to-exacerbate-regional-divide-in-oecd-countries-says-first-regional-analysis-on-its-impact-on-local-job-markets.html (última consulta: 17 de abril de 2025).
[317] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence*, doc. OECD/LEGAL/0449 (adoptada el 22 de mayo de 2019, enmendada el 3 de mayo de 2024).
[318] *Ibid*., p. 4.
[319] Ministerio de Asuntos Exteriores de Japón, *Ministerial Statement on Trade and Digital Economy (Annex): G20 AI Principles*, disponible en https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf (última consulta: 17 de abril de 2025). Véase igualmente el documento completo publicado por la OECD en Organisation for Economic Co-operation and Development, *G20 Ministerial Statement on Trade and Digital Economy*, publicado el 9 de junio de 2019 en *OECD.AI Policy Observatory*, disponible en https://wp.oecd.ai/app/uploads/2021/06/G20-AI-Principles.pdf (última consulta: 17 de abril de 2025).
[320] *Ibid*., p. 1.
[321] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, doc. SHS/BIO/PI/2021/1 (2022).

y “Do No Harm”, la alfabetización, o bien la idea de colaboración global y el compartir de conocimientos[322] desarrollada después en la Resolución 78/L.86 de la Asamblea General de la ONU ya mencionada. El Estado de Derecho no está mencionado como principio ni valor, pero si es parte del Ámbito de Actuación número 2, el cual pide que los Estados aseguren el seguimiento y reparación de daños causados por IA[323]. La Recomendación pide igualmente “reforzar la capacidad del poder judicial” para asegurar *inter alia* dicho Estado de Derecho[324].

Mientras que este trabajo se enfoca en el Derecho internacional público, cabe mencionar que la IA ha sido ya enfoque de regulación en la ONU a nivel internacional privado. En julio de 2024, se aprobó la *Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Contratación Automatizada*[325]. Esta regulación es un modelo instrumental para el Derecho internacional privado, estableciendo un patrón de reglas para el reconocimiento jurídico de actuaciones de la IA en herramientas de contracción automática. La implementación de la Ley permite así tratar con las acciones y decisiones inesperadas de la IA en negocios a nivel internacional[326].

Finalmente, se ha de mencionar que el Derecho internacional no está solo en la regulación de la IA, ya que varios Estados han empezado a adoptar sus propias leyes o recomendaciones a nivel nacional. Este trabajo no se adentra en la análisis en profundidad de estas, al no ser de gran interés para modelar el Derecho internacional. Se estima que, por los intereses expuestos en el Capítulo I, los Estados priorizan sobre todo su propio desarrollo competitivo antes de la codificación de la colaboración internacional. Se puede considerar, por ejemplo, el caso de Corea del Sur con su proyecto de Ley Básica sobre el Desarrollo de la IA, que declara desde su Artículo 1 su propósito de “fortalecer la competitividad nacional”[327].

La influencia del Derecho internacional sobre la IA es sin embargo notable en la actualidad jurídica de varios países. El proyecto de ley de Brasil[328], por ejemplo, es muy

[322] *Ibid*., p. 20-23.
[323] *Ibid*., p. 27.
[324] *Ibid*., p. 28.
[325] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, *Ley Modelo sobre Contratación Automatizada*, aprobada el 11 de julio de 2024, doc. A/79/17, anexo IV.
[326] T. Rodríguez de las Heras Ballell, *Los riesgos de la inteligencia artificial en el comercio internacional*, presentación en el congreso “Los riesgos y los seguros en el comercio internacional – Jordana SEAIDA”, Universidad Complutense de Madrid, 22 abril 2025.
[327] Asamblea Nacional de Corea del Sur, *Proyecto de Ley Básica sobre el Desarrollo y la Creación de una Base de Confianza en la Inteligencia Artificial*, n.º 2206772 (2024).
[328] Senado Federal de Brasil, *Projeto de Lei n° 2338* (2023).

similar al Reglamento de la UE en su perspectiva de categorizar riesgos[329]. Las Recomendaciones para el uso de la IA de parte del Gobierno argentino hacia el ámbito público[330] citan los principios de la UNESCO y de la OECD, y les hacen eco. Por lo tanto, se observa la importancia del Derecho internacional en el condicionamiento de la legislación nacional, y la gran oportunidad de influencia efectiva y positiva.

2. Desafíos y limitaciones de la regulación internacional actual

Las regulaciones y recomendaciones presentadas son un conjunto remarcable, pero carecen de alcance sobre algunos puntos claves analizados en este trabajo. En particular, vemos una carencia potencialmente problemática de aplicabilidad al ámbito militar, de defensa, y de seguridad nacional. Adicionalmente, las menciones al Estado de Derecho varían, y presentan una perspectiva dudosa sobre el futuro de la regulación de la IA a este respecto.

2.1. Ámbito militar, de defensa, y seguridad nacional

Vemos en los textos analizados varias menciones a los usos de la IA en el ámbito militar, o bien para actividades que tengan que ver con la seguridad nacional o la defensa. Sin entrar en las definiciones de estos tres conceptos, se entiende una relación entre ellos por su propia naturaleza.

Ambos el TCdE y el RIA excluyen expresamente las aplicaciones al ámbito de defensa, o de seguridad nacional de su competencia en sus textos. El TCdE expresa en su Artículo 3(2) lo siguiente:

> "Una Parte no estará obligada a aplicar esta Convención a las actividades...relacionadas con la protección de sus intereses de seguridad nacional, con el entendimiento de que dichas actividades se llevarán a cabo de manera coherente con el Derecho internacional aplicable, incluidas las obligaciones en materia de derechos humanos internacionales, y con respeto a sus instituciones y procesos democráticos."

Reafirma así casi inmediatamente después en su Artículo 3(4) que tales "asuntos relacionados con la defensa nacional no entran dentro del ámbito de aplicación de esta Convención". Mientras que se puede argumentar semánticamente que el TCdE no excluye el ámbito

[329] J. Escudero Méndez, *Brasil: El Senado aprueba el Proyecto de Ley 2338/2023 sobre el uso de la inteligencia artificial*, Instituto Autor, 10 de enero de 2025, disponible en https://institutoautor.org/el-senado-de-brasil-aprueba-el-proyecto-de-ley-2338-2023-sobre-el-uso-de-la-inteligencia-artificial/ (última consulta: 17 de abril de 2025).
[330] Jefatura de Gabinete de Ministros de Argentina, Disposición 2/2023 "Recomendaciones para el uso de Inteligencia Artificial" (2023).

militar—ya no lo menciona literalmente en el texto, como hace el RIA a continuación— se sobreentiende que lo descarta de su alcance por las menciones de defensa y seguridad nacional.

El RIA define su alcance en su Artículo 2(3) excluyendo su aplicación a sistemas de IA "exclusivamente para fines militares, de defensa o de seguridad nacional". Consta aclarar que, en el caso del Reglamento, esta exclusión es en parte conforme con el *Tratado de la Unión Europea del 7 febrero de 1992*, el cual afirma en su Artículo 4(2) que la "seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro"[331]. Se puede destacar que el ámbito militar y la defensa no se señalan entonces como responsabilidad exclusiva, ya que el Tratado de la UE en sí establece una política común de seguridad y defensa para la UE, que pide además eventuales prestaciones militares de los Estados miembros, como en su Artículo 42(3). Sin embargo, el RIA se deshace de esos alcances igualmente, comentando en su preámbulo que "el Derecho internacional público…es el marco jurídico más adecuado para la regulación…en el contexto del uso de la fuerza letal y…de las actividades militares y de defensa".

El TCdE y el RIA consideran por lo tanto que estas aplicaciones no son de su competencia, sino que el Derecho internacional vigente es suficiente para abordar estas cuestiones. La Resolución 78/265 de la ONU previamente mencionada excluye también al ámbito militar de lo que considera en su texto como pautas para "sistemas seguros y fiables"[332]. Habiendo observado la práctica actual de la IA, y la escala de difusión y facilidad de comisión de HII que brinda su función catalizadora, así como innovación de prácticas ilícitas que ya ha permitido su función creadora, se podría poner en cuestión esta perspectiva.

2.2. Apoyo al Estado de Derecho internacional

Igualmente, las referencias en los textos mencionados al Estado de Derecho son inconsistentes e insuficientes para su protección efectiva a nivel internacional. El TCdE es sin duda el instrumento más vocal, haciendo referencia directa en su título. Carece sin embargo de mecanismos de aplicación robustos[333], por lo que el compromiso del posible Estado ratificante de este Tratado se puede considerar desestructurado en sus consecuencias si no se cumplen las obligaciones. Se enfatiza significativamente la responsabilidad de cada Parte de

[331] Tratado entrado en vigor el 1 de noviembre de 1993, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 12016M/TXT).
[332] Asamblea General de las Naciones Unidas, *Seizing the opportunities… op. cit.*, p. 2.
[333] C. Chang, "The First Global AI Treaty: Analyzing... *op. cit.*

ocuparse de la implementación, como en el Artículo 14 para los mecanismos de reparación, o bien el Artículo 26 para un mecanismo estatal que vigile la adherencia a las obligaciones. El Capítulo VII implementa una Conferencia de las Partes del Tratado, que se ha de reunir según el Artículo 23(2)(3) "cuando sea necesario", y las Partes han de entregar un reporte "periódicamente" después del primero (a remitir dos años después de su ratificación o accesión) según el Artículo 24(1). Estas disposiciones presentan por lo tanto un alto grado de generalidad, lo que es inconsistente con la enfatización del seguimiento de un Estado de Derecho internacional, el cual beneficiaría de unas pautas jurídicas más específicas y homogéneas.

Se puede argumentar que mecanismo de aplicación del RIA está más en línea con esta promoción del Estado de Derecho, el cual este texto menciona efectivamente desde su primera página, pero se ha de considerar de nuevo que un Reglamento de la UE es un instrumento jurídico de alcance regional y no global. Por lo tanto, las menciones del RIA acerca del Estado de Derecho se especifican en el contexto de la *Carta de los Derechos Fundamentales de la Unión Europea del 7 de diciembre de 2000*[334], y no en un sentido global.

Finalmente, vemos ya mencionada la petición directa de asegurar el Estado de Derecho en la Recomendación de la UNESCO[335]. Esta se puede comparar con la decisión del G20 de quitar la mención titular al Estado de Derecho en su segundo principio[336] en comparación con los originales de la OECD[337], la cual pese de poder ser una elección puramente editorial puede connotar una relegación de la idea.

[334] Tratado entrado en vigor el 1 de diciembre de 2009, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 12016P/TXT).
[335] UNESCO, *Recommendation on the Ethics of Artificial Intelligence… op. cit.*, p. 27-28.
[336] Ministerio de Asuntos Exteriores de Japón, *Ministerial Statement... op. cit.*, p. 1.
[337] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence… op. cit.*

VI. CONCLUSIONES

La IA es una dicotomía en Derecho internacional: presenta entonces una gran oportunidad de desarrollo estatal, pero conlleva un riesgo inminente por su falta de regulación. De lo expuesto, podemos así sacar las siguientes conclusiones:

I. Existen usos positivos de la IA para el seguimiento del Derecho internacional, por lo que se establece el valor de la tecnología desde la perspectiva de los Estados. La IA apoya el interés soberano de los Estados de proteger sus fronteras y no recibir injerencia ajena en sus asuntos, creando soluciones innovadoras para ello y mejorando defensas. Apoya igualmente la convivencia pacífica en la comunidad internacional, permitiendo medir usos potenciales de fuerza y detectar posibles conflictos antes de que estallen. Permite fomentar la diplomacia y la comunicación interestatal, al igual que da una oportunidad a los Estados de desarrollar varias de sus industrias. Al aplicar la función catalizadora y la función creadora de la IA positivamente, los Estados pueden mejorar el seguimiento de sus obligaciones internacionales, incluyendo los principios de la prohibición del uso de la fuerza y de la resolución pacífica de controversias. Por lo tanto, la IA es una tecnología con aspectos valorables en la práctica del Derecho internacional, y no un elemento puramente nocivo a la perspectiva jurídica.

II. No obstante, los Estados tienen más oportunidades de evadir sus obligaciones existentes gracias a la IA. La función catalizadora de esta tecnología permite ejercer las mismas actividades ilícitas que los Estados realizaban antes de su aparición, pero facilitando el proceso y maximizando la escala o la magnitud de los resultados. Vemos así por ejemplo la vulneración de varios aspectos de *ius in bello* trás el uso de SAL, o del principio de soberanía cuando la IA se involucra en prácticas estatales ya ilícitas como la injerencia en elecciones. La facilitación de estos procesos mediante la IA bajará el requisito de recursos para los Estados en su comisión de HII, y la maximización de los resultados permitirá potenciales daños adicionales en la práctica ilícita. Ambas de estas consideraciones pueden entenderse como un riesgo para la comunidad internacional, resaltando la necesidad de regulación expresa por parte del Derecho internacional. Adicionalmente, la promoción de la colaboración global en la materia de la IA y la reducción de la brecha digital[338] ideada significan un proyectado acceso a más recursos para un mayor número de Estados,

[338] Véase Asamblea General de las Naciones Unidas, borrador de Resolución "Aumentar la cooperación... *op. cit.*, UNESCO, *Recommendation on the Ethics of Artificial Intelligence*… *op. cit.*

incrementando así la posibilidad de prácticas nocivas mediante la IA si no se crean obligaciones internacionales específicas a esta tecnología.

III. La función creadora de la IA expone el Derecho internacional a retos que no conocía hace 50 años, como es el caso reciente de los *bots* y los *deepfakes*, o bien el reconocimiento facial y los SAL. Existe por lo tanto el riesgo de aún más innovación dentro de actividades ya ilícitas, o bien de la creación de nuevas prácticas nocivas en la comunidad internacional inconcebibles en el presente. Por lo tanto, el conjunto de los Estados ha de actualizarse mediante la priorización de la regulación y vigilancia de estos nuevos riesgos ya en práctica. La creación en el ámbito del Derecho internacional privado de una Ley Modelo para combatir los riesgos de la nueva existencia de la contratación automatizada es un modelo pertinente; los Estados han de enfocarse en una regulación homogénea de los riesgos de la IA para el Derecho internacional público igualmente. La preocupación de nuevas amenazas aún no existentes ha de sin embargo no socavar la atención de la comunidad internacional; se ha de vigilar ante todo la función catalizadora de la IA en prácticas nocivas consideradas ya suficientemente englobadas en la regulación actual.

IV. Así, los usos de la IA para apoyar a los posibles HII expuestos en el Capítulo II son en sí mismo ya quebrantamientos de obligaciones existentes para los Estados que las contratan—por la propia definición de HII. Estos usos ilícitos de la IA son definidos como ilícitos justamente trás los varios tratados y principios mencionados. No obstante, el Derecho internacional se beneficiaría de repetir en nuevos instrumentos estas mismas obligaciones explícitamente en el contexto de la IA, y buscar obtener un máximo de apoyo de parte de la comunidad internacional. A través de sus dos funciones mencionadas, la IA representa una amenaza al seguimiento de obligaciones bajo el Derecho internacional vigente, pero existen oportunidades de remediación. Para las nuevas prácticas de armas generadas por la función creadora, como los SAL, vemos precedente en la comunidad internacional con respeto a la prohibición, como fue el caso la Convención sobre ciertas armas. Con respecto a la función catalizadora, como es el ejemplo del uso de datos privados mediante IA, la expansión de leyes actuales ha sido demostradamente posible, siendo este el caso del RIA con la Ley de Protección de Datos. El Derecho internacional es por lo tanto capaz, y ahora bajo presión expresa, de expandirse para incorporar específicamente obligaciones acerca de la IA. Esto es de nuevo igualmente importante en la consideración de la preparación para afrontar nuevas prácticas nocivas que impulsa la tecnología, y que la comunidad internacional aún no puede concebir.

V. La falta de aplicación al ámbito militar, de defensa, o de seguridad nacional de instrumentos de Derecho internacional como el RIA o el TCdE presenta un potencial riesgo a la hora del desarrollo de la IA para usos militares. Habiendo revisado varios usos de la tecnología en el ámbito de las armas y la práctica estatal en este respeto, incluyendo los SAL, los drones, o bien las armas nucleares, se puede observar el impacto de ambas funciones de la IA en el desarrollo de actividades potencialmente ilícitas. La deferencia del alcance de instrumentos como el RIA o el TCdE al resto del Derecho internacional implica una confianza total en la regulación actual para englobar estos casos. Mientras que principios establecidos, normas consuetudinarias, y otras fuentes del Derecho internacional puedan crear las obligaciones mínimas para que usos de la IA dañosos puedan constituir HII, las funciones de la IA crean la posibilidad de enfrentarse a más prácticas internacionales dañosas al entorno pacifico entre Estados. Este trabajo hace por lo tanto eco a iniciativas como el borrador de resolución A/C.1/79/L.77 de la Asamblea General de la ONU, en la necesidad de regular ciertas aplicaciones de la IA como los SAL más allá de lo ya recogido en Derecho internacional. La comunidad internacional necesita expresamente pronunciación jurídica sobre el uso de la IA en el ámbito militar, de defensa, o de seguridad nacional.

VI. Finalmente, se observan trás este análisis los riesgos que la IA presenta al fomento del Estado de Derecho internacional. Si bien el seguimiento de las obligaciones estatales que presenta la tecnología—junto con el interés intrínseco de los Estados en ella—es beneficioso, el impulso a HII presentado es una amenaza considerable. Si el Derecho internacional no es apto para regular la práctica, y los mecanismos de aplicación en la comunidad internacional insuficientes o inexistentes, la IA dominará la posibilidad de establecer dicho Estado de Derecho internacional. La literatura revisada apunta a la necesidad de crear regulación específica para el alcance de la IA[339], lo que se prevé como aún más relevante a la hora de establecer la importancia del seguimiento de regulaciones internacionales a nivel global. El futuro de la debatida existencia del Estado de Derecho internacional estaría en todo caso puesto en riesgo si la práctica actual y el desarrollo de la IA no son regulados apropiadamente. Este análisis siendo de envergadura limitada, se destaca por lo tanto la necesidad de abordar estas cuestiones académicamente en el desarrollo de la jurisprudencia relevante.

[339] Véase J.S. Viveros Álvarez, "La inteligencia artificial…" *op. cit.*, p. 101., B. Pino, *International Responsibility of States… op. cit.*, p. 43.,

1. Futuras perspectivas/proyectos relevantes

Considerando las conclusiones de este trabajo, es de nuevo vital para el desarrollo del Derecho internacional seguir atentamente la progresión de la IA puesta a disposición de la comunidad internacional. Esto incluye dos proyectos con esta tecnología que, pese de ser presentemente aún en parte ciencia ficción, tienen interés científico e investigativo notable. Con tal atención, se puede estimar que estos proyectos se han convertido ya en áreas de desarrollo a la cuales vigilar jurídicamente por sus posibles funciones en apoyo a la comisión de HII.

Primeramente, la IA general[340] se presenta como la forma plenamente realizada de las capacidades de esta tecnología; sería una forma hipotética de la IA capaz de emular o sobrepasar la inteligencia humana. Sus capacidades se presentarian efectivamente de forma *general*, al contrario de la IA llamada *estrecha* que se diseña para aplicaciones específicas[341] (como son todas las aplicaciones revisadas anteriormente en este trabajo). Esto revolucionaría industrias enteras, permitiendo tener un sistema inteligente que no presente las mismas necesidades biológicas que una persona, como un cierto tiempo de reposo, y pueda trabajar a una velocidad incomparable[342]. Sin embargo, al pensar y actuar autónomamente como lo haría una persona, la IA general vuelve a resurgir los problemas de personalidad jurídica mencionados en el Capítulo II de este trabajo, pero de manera aún más relevante. La IA general que podría trabajar para un Estado abre las puertas a una responsabilidad estatal confusa en su operación. Si esta IA fuera a tomar, por su cuenta, decisiones que fueran violaciones de una obligación del Estado, la aplicación de la atribución presentada en el Artículo 2 del PA 2001 se pondría efectivamente en cuestión. Adicionalmente, las funciones de la IA mencionadas serían también observadas en su cambio; es reto de ciencia ficción predecir efectivamente qué prácticas estatales ilícitas se catalizarían, y cuales se crearían desde cero, con la ayuda de una inteligencia suprahumana.

Asimismo, se ha de considerar la posibilidad de la IA cuántica (también conocida en inglés como *quantum machine learning*). Sin adentrar esta conclusión de Derecho internacional demasiado en la tecnología compleja de la computación cuántica, la

[340] Explícitamente diferente de la IA *generativa* ya existente, y mencionada previamente.
[341] S. Sonko *et al*., "A critical review towards artificial general intelligence: Challenges, ethical considerations, and the path forward", en *World Journal of Advanced Research and Reviews*, 21(03), 2024, p. 1262.
[342]IBM, "Getting ready for artificial general intelligence with examples", 18 de abril de 2024, disponible en https://www.ibm.com/think/topics/artificial-general-intelligence-examples (última consulta: 17 de abril de 2025).

investigación se basa en maneras de acelerar el funcionamiento de la IA mediante mejoras exponenciales en la rapidez de procesamiento y capacidad de recursos que tendrían los ordenadores[343]. Habiéndose considerado el concepto desde los años ochenta, el estudio de la posibilidad ha avanzado desde que se empezó a realizar, y que tiene gran potencial científico en varias áreas[344]. La significancia de ello para los Estados es de nuevo una explotación de las capacidades de la IA mencionadas en este trabajo; la función catalizadora se vería en si misma catalizada, y las oportunidades de comisión de HII mediante la IA llegarían a puntos inconcebibles. Mientras que no se espera que la comunidad internacional esté hoy preparada para abordar estas posibilidades jurídicamente, se resalta la importancia de preparación y evolución. Para estar a la altura de afrontar posibles desarrollos, es imprescindible que el Derecho internacional se adapte a la situación actual de la IA.

[343] A. Zeguendry, Z. Jarir y M. Quafafou, "Quantum Machine Learning: A Review and Case Studies", en *Entropy*, vol. 25, n.º 2, art. 287, 2023, p. 1.
[344] W. Lu et al., "Quantum machine learning: Classifications, challenges, and solutions", en *Journal of Industrial Information Integration*, vol. 42, art. 100736, 2024, p. 1-2.

ANEXOS

1. BIBLIOGRAFÍA CONSULTADA

1.1. LIBROS Y MONOGRAFÍAS

G. Álvarez Undurraga, *Metodología de la investigación jurídica: hacia una nueva perspectiva*, Universidad Central de Chile, Santiago, 2002.

W. Barfield y U. Pagallo, *Advanced Introduction to Law and Artificial Intelligence*, Elgar Advanced Introductions series, Edward Elgar, 2020.

P. de Miguel Asensio, *Conflict of Laws and the Internet*, *Elgar Information Law and Practice series*, Edward Elgar, 2020.

C.H. Gray, *AI, Sacred Violence, and War—The Case of Gaza*, Palgrave Macmillan, Cham, 2025.

J. Kenny, *Advanced Artificial Intelligence Techniques and the Principle of Non-Intervention in the Context of Electoral Interference*, Routledge, 2023.

R.L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression*, Oxford University Press, Nueva York, 1989.

M. Peguera Poch y B. Arribas Sánchez, *Perspectivas regulatorias de la inteligencia artificial en la Unión Europea*, 1ª ed., Reus, 2023.

J.I. Solar Cayón (ed.), *Dimensiones éticas y jurídicas de la inteligencia artificial en el marco del Estado de Derecho*, Universidad de Alcalá - Defensor del Pueblo (España), España, 2020.

1.2. CONTRIBUCIONES EN OBRAS COLECTIVAS

L. Arya, *et. al*., "Eyes in the Sky: Safeguarding Borders Security with AI-Powered Aerial Monitoring and IoT Integration", en *Proceedings of International Conference on Recent Innovations in Computing* (ICRIC 2023), vol. 2, en Z. Illés, *et. al.* (eds.), *Lecture Notes in Electrical Engineering*, vol. 1195, Springer, Singapur, 2024, p. 863-873.

F. Bolici *et al*., "Unpopular Policies, Ineffective Bans: Lessons Learned from ChatGPT Prohibition in Italy", en *ECIS 2024 Proceedings European Conference on Information Systems (ECIS)*, Università di Cassino e del Lazio Meridionale, junio 2024, p. 1-15.

K. Bontcheva et al., *"EUvsDisinfo: A Dataset for Multilingual Detection of Pro-Kremlin Disinformation"*, en *Proceedings of the 31st ACM International Conference on Information & Knowledge Management (CIKM '22)*, 2022, p. 5380-5384.

E. H. Morawska, *Council of Europe standards and activities related to AI: towards a Framework Convention on AI and human rights?*, en M. Balcerzak y J. Kapelańska-Pręgowska (eds.), *Artificial Intelligence and International Human Rights Law*, 2024, p. 25-44.

S. Powers, *Towards Information Sovereignty*, en W. J. Drake y M. Price (eds.), *Beyond Netmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem*, University of Pennsylvania, agosto 2014, p. 90-98.

1.3. ARTÍCULOS EN REVISTAS CIENTÍFICAS ESPECIALIZADAS

M. Ahmad *et al*., "Leveraging Blockchain and Machine Learning to Promote Child Labor-Free Sustainable Development", en *Distrib. Ledger Technol.*, 4, 1, Article 7, March 2025, p. 1-33.

V. Agrawal, "Demystifying the Chinese Social Credit System: A Case Study on AI-Powered Control Systems in China", en *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, n.º 11, 2022, p. 13124-13125.

M. Almada y N. Petit, "The EU AI Act : between the rock of product safety and the hard place of fundamental rights", en *Common market law review*, Vol. 62, No. 1, 2025, p. 85-120.

A. Andreou, "e-Securing the EU Borders: AI in European Integrated Border Management", en *Journal of Politics and Ethics in New Technologies and AI*, vol. 2, n.º 1, 2023, p. 1-20.

I. Artíñano Ortiz, M. Balcerzak y J. Kapelańska-Pręgowska, Eds. 2024., "Artificial Intelligence and International Human Rights Law. Developing Standards for a Changing World", en *Deusto Journal of Human Rights*, n.º 14, diciembre 2024, p. 377-384.

J. Beim, "Enforcing a Prohibition on International Espionage", en *Chicago Journal of International Law*, vol. 18, n.º 2, art. 6, 2018, p. 647-672.

L. Bence Márquez y T. Diéguez La O, "Soberanía e inmunidad del Estado. Reflexiones a la luz del Derecho Internacional", en *Política Internacional*, vol. 6, núm. 1, 2024, Instituto Superior de Relaciones Internacionales "Raúl Roa García", Cuba, p. 144-156.

A. Bin Rashid, M.D. Ashfakul Karim Kausik, "AI Revolutionizing Industries Worldwide: A Comprehensive Overview of Its Diverse Applications", en *Hybrid Advances*, vol. 7, 2024, 100277, p. 134.

E. Blanco Niyitunga, "Armed drones and international humanitarian law", en *Digital Policy Studies*, vol. 1, n.º 2, University of Johannesburg, 2023, p. 18-39.

B. Boutin, "State responsibility in relation to military applications of artificial intelligence", en *Leiden Journal of International Law*, vol. 36, n.º 1, 2023, p. 133-150.

C. Chang, "The First Global AI Treaty: Analyzing the Framework Convention on Artificial Intelligence and the EU AI Act", en *University of Illinois Law Review (Online)*, 86, 2024, p. 86-99.

G. Dimitrov, “A Brief History of Cyber Intelligence: How Did Computer Data Evolve to Be Used for Intelligence Operations”, en *American Intelligence Journal*, vol. 37, n.º 1, 2020, p. 107-114.

A. Dulka, “The Use of Artificial Intelligence in International Human Rights Law”, en *Stanford Technology Law Review*, vol. 26, n.º 2, 2023, p. 316-366.

A. Etzioni, “Sovereignty as Responsibility”, en *Orbis*, vol. 50, n.º 1, invierno 2006, p. 71-85.

T. Evas, “The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI”, en *Journal of AI Law and Regulation*, Volume 1, Issue 1, 2024, p. 98-101.

M. Giovanardi, “AI for Peace: Mitigating the Risks and Enhancing Opportunities”, en *Data & Policy*, vol. 6, e41, 2024, p. 1-12..

F. Gualdi y A. Cordella, “Theorizing the Regulation of Generative AI: Lessons Learned from Italy's Ban on ChatGPT”, en *Proceedings of the 57th Hawaii International Conference on System Sciences*, 2024, p. 2023-2032.

H. Gusterson, “It's all Lavender in Gaza”, en *Anthropology Today*, vol. 40, 2024, p. 1-2.

H. Ha y P. Min-Hye, “The Threat of AI and Our Response: The AI Charter of Ethics in South Korea”, en *Asian Journal of Innovation and Policy*, vol. 9, no. 1, 2020, p. 56-78.

A. Hárs, ‘AI and international law – Legal personality and avenues for regulation*”*, en *Hungarian Journal of Legal Studies*, vol. 62, n.º 4, 2022, p. 320-244.

R. de la C. Hernández Rodríguez, “El amparo constitucional. Herramienta catalizadora de la función judicial en la nueva Constitución cubana”, en *Cadernos de Dereito Actual*, n.º 12, 2019, p. 194-226.

M. Herrera, “La Intersección entre Inteligencia Artificial y Armas Nucleares: Riesgos, Beneficios y Recomendaciones”, en *Revista UNISCI / UNISCI Journal*, n.º 67, enero 2025, p. 87-109.

R. Herrero, “Política exterior de España e intereses nacionales”, en *UNISCI Discussion Papers*, n.º 27, octubre 2011, p. 87-99.

E. Hunter Christie *et al.*, "Regulating lethal autonomous weapon systems: exploring the challenges of explainability and traceability", en *AI and Ethics*, vol. 4, 2024, p. 229-245.

R. K. Jha y M. Jha, *"*Optimizing E-Government Cybersecurity through Artificial Intelligence Integration*"*, en *Journal of Trends in Computer Science and Smart Technology*, vol. 6, n.º 1, 2024, p. 67-87.

C. Kuner et al., “The GDPR as a Chance to Break Down Borders”, en *International Data Privacy Law*, vol. 7, n.º 4, 2017, p. 231-232.

S. Leal W, “Los Sistemas de Armas Letales Autónomos”, en *Frónesis. Revista de Filosofía Jurídica, Social y Política*, vol. 31, n.º 1, Universidad del Zulia, 2023, p. 52-66.

L.A. López Marcos, “Colaboración internacional en el ámbito de los recursos espaciales: sobre la necesidad de crear un instrumento internacional que regule la explotación y apropiación de los recursos espaciales en la Luna y otros cuerpos celestes”, en *Revista Española de Derecho Aeronáutico y Espacial*, n.º 2022, Asociación Española de Derecho Aeronáutico y Espacial (AEDAE)/ATELIER, Madrid, 2022, p. 495-563.

A. G. López Martín, “La protección internacional de los derechos de los trabajadores en el marco de la centenaria OIT: una breve referencia a la situación de España como miembro de la misma”, en *Anuario de los Cursos de Derechos Humanos de Donostia-San Sebastián: Donostiako Giza Eskubideei Buruzko Ikastaroen Urtekaria*, n.º 21, 2021, p. 155-198.

A.G. López Martín, “Principios y reglas de solución aplicables a las controversias territoriales a la luz de la jurisprudencia de la Corte Internacional de Justicia”, en *Anuario Colombiano de Derecho Internacional,* Vol. 6, 2013, p. 15-45.

W. Lu et al., “Quantum machine learning: Classifications, challenges, and solutions”, en *Journal of Industrial Information Integration*, vol. 42, art. 100736, 2024, p. 1-12.

C. E. Marinică, “Artificial intelligence – A possible key for better results on tackling climate change”, en *Law Review*, vol. XII, núm. 1, Union of Jurists of Romania, 2022, p. 83-93.

N. Md Nor, *et. al*., "Leveraging Artificial Intelligence (AI) Technology for Enhanced Border Surveillance at the Malaysia-Thailand Land Border", en *e-Bangi: Journal of Social Sciences & Humanities*, vol. 21, n.º 4, 2024, p. 54-65.

I. Moll Santa-Isabel, “El desarrollo normativo, ético y tecnológico de los Sistemas Autónomos Letales”, en *Araucaria*, vol. 26, n.º 57, 2024, p. 37-66.

C. R. Moran, J. Burton y G. Christou, “The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying”, en *Journal of Global Security Studies*, vol. 8, n.º 2, 2023, p. 1-18.

M. Pacholska, “Military Artificial Intelligence and the Principle of Distinction: A State Responsibility Perspective”, *Israel Law Review*, vol. 56, n.º 1, 2023, p. 3-23.

F. Palmiotto y N. Menéndez González, “Facial Recognition Technology, Democracy and Human Rights”, *Computer Law & Security Review*, vol. 50, 105857, 2023, p. 1-6.

J. A. Perea Unceta, ″Reflexiones sobre las restricciones a la soberanía del Estado en el Derecho Internacional contemporáneo″, en *Anuario Jurídico y Económico Escurialense*, vol. XXXVII, 2004, p. 95-129.

B. Ram y P. Verma, “Artificial intelligence AI-based Chatbot study of ChatGPT, Google AI Bard and Baidu AI”, en *World Journal of Advanced Engineering Technology and Sciences*, vol. 08, n.º 01, 2023, p. 258-261.

D. Ramírez Plascencia *et. al*., “Digital Partisans: An Inquiry on the Use of Bots for Political Propaganda in Mexico”, en *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, avance en línea, 2025, p. 1-9.

H. M. Roff, “Lethal Autonomous Weapons and Jus Ad Bellum Proportionality”, en *Case Western Reserve Journal of International Law*, vol. 47, 2015, n.º 1, p. 37-52.

W.R.W. Rosli, “Waging Warfare Against States: The Deployment of Artificial Intelligence in Cyber Espionage”, en *AI and Ethics*, vol. 5, 2025, p. 47-53.

F. Safraoui, "Security Challenges and Air Sovereignty: Between Escalating Threats and the Need for Fortification", en *Qədim Diyar Beynəlxalq Elmi Jurnal*, vol. 7, n.º 2, 2025, p. 408-419.

M. Sánchez Zorrilla, “La metodología en la investigación jurídica: características peculiares y pautas generales para investigar en el derecho”, en *Revista Telemática de Filosofía del Derecho*, n.º 14, 2011, p. 317-358.

Y. Shen y X. Zhang., “The impact of artificial intelligence on employment: the role of virtual agglomeration”, en *Humanit Soc Sci Commun* 11, 122, 2024, p. 1-14.

S. Sonko *et al*., “A critical review towards artificial general intelligence: Challenges, ethical considerations, and the path forward”, en *World Journal of Advanced Research and Reviews*, 21(03), 2024, p. 1262-1268.

A. Spain, “Sovereignty and the Promotion of Peace in Non-International Armed Conflict”, 106 *Am. Soc'y Int'l L. Proc*. 78 (2012), p. 78-80.

I. Szabadföldi, “Artificial intelligence in military application – opportunities and challenges”, en *Land Forces Academy Review*, vol. XXVI, n.º 2(102), 2021, p. 157-165.

M.H. Tessler, et al., “AI can help humans find common ground in democratic deliberation”, en *Science*, vol. 386, núm. 6719, octubre 2024, p. 1-9.

A. D. Vanberg, “Informational Privacy Post GDPR – End of the Road or the Start of a Long Journey?”, en *The International Journal of Human Rights*, 25(1), 2020, p. 1-27.

M.T. Veber., "International Organizations and AI-Supported Humanitarian Aid: Navigating through the Applicable (Data Protection) Legal Regimes.", en *International and Comparative Law Review*, vol. 24, no. 2, Sciendo, 2024, p. 54-83.

J.S. Viveros Álvarez, “La inteligencia artificial y la responsabilidad internacional de los Estados”, en *Revista Estudios en Derecho a la Información*, n.º 14, julio-diciembre de 2022, p. 83-105.

K. Vold, "Human-AI cognitive teaming: using AI to support state-level decision making on the resort to force", en *Australian Journal of International Affairs*, vol. 78, n.º 2, 2024, p. 229-236.

O. E. Wetter, “Imaging in Airport Security: Past, Present, Future, and the Link to Forensic and Clinical Radiology”, en *Journal of Forensic Radiology and Imaging*, vol. 1, n.º 4, 2013, p. 152-160.

A. Zeguendry, Z. Jarir y M. Quafafou, “Quantum Machine Learning: A Review and Case Studies”, en *Entropy*, vol. 25, n.º 2, art. 287, 2023, p. 1-41.

J. Ziller, “The Council of Europe Framework Convention on Artificial Intelligence vs. the EU Regulation: two quite different legal instruments”, en *Fascicolo 2/2024*, CERIDAP, 2024, p. 202-227.

1.4. OTRAS PUBLICACIONES

Y. Abraham, “'Lavender': The AI machine directing Israel’s bombing spree in Gaza”, *+972 Magazine*, 3 de abril de 2024, disponible en https://www.972mag.com/lavender-ai-israeli-army-gaza/ (última consulta: 23 de marzo de 2025).

*"*AKPS will ensure smooth, efficient border control, says DPM Fadillah*"*, *The Sun Daily*, 2 de febrero de 2025, disponible en https://thesun.my/malaysia-news/akps-will-ensure-smooth-efficient-border-control-says-dpm-fadillah-HE13605507 (última consulta: 18 de febrero de 2025).

Australian Electoral Commission, *AI & Elections*, última actualización: 10 de febrero de 2025, disponible en https://www.aec.gov.au/Elections/electoral-advertising/ai-and-elections.htm (última consulta: 21 de febrero de 2025).

N. Bashir et al., *"The Climate and Sustainability Implications of Generative AI"*, en *An MIT Exploration of Generative AI*, marzo de 2024, disponible en https://doi.org/10.21428/e4baedd9.9070dfe7 (última consulta: 23 de febrero de 2025).

A. Blanchard y M. Taddeo, “Predictability, Distinction & Due Care in the use of Lethal Autonomous Weapon Systems,” 3 de mayo de 2022, SSRN, http://dx.doi.org/10.2139/ssrn.4099394 (última consulta: 25 de marzo de 2025).

C. Boine y D. Rolnick, *Why the AI Act Fails to Understand Generative AI*, publicado en *We Robot 2023 Conference, Boston University School of Law*, 30 de junio de 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4644701 (última consulta: 16 de abril de 2025).

R. J. Buchan, “The International Legal Regulation of Cyber Espionage”, en A.-M. Osula y H. Rõigas (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn, 2016, p. 1, disponible en https://eprints.whiterose.ac.uk/id/eprint/98791/10/Russell_The%20International%20Legal%20Regulatio (última consulta: 5 de abril de 2025).

Capgemini Research Institute, *Climate AI: How artificial intelligence can power your climate action strategy*, disponible en https://www.capgemini.com/wp-content/uploads/2021/05/Report-Climate-AI-4.pdf, p. 2 (última consulta: 17 de marzo de 2025).

S. Cheung, *“A Hong Kong University Launched the World’s First Large-Scale AI Model Earth Observation Satellite”*, *The Diplomat*, 21 de octubre de 2024, disponible en https://thediplomat.com/2024/10/a-hong-kong-university-launched-the-worlds-first-large-scale-ai-model-earth-observation-satellite/ (última consulta: 3 de febrero de 2025)

Colorado State University Global, "How Does AI Actually Work?", blog post, 9 de agosto de 2021, disponible en https://csuglobal.edu/blog/how-does-ai-actually-work#:~:text=AI%20systems%20work%20by%20combining,performance%20and%20develops%20additional%20expertise (última consulta: 15 de marzo de 2025).

Comité Internacional de la Cruz Roja, *Autonomy, artificial intelligence and robotics: Technical aspects of human control*, Ginebra, agosto 2019, https://www.icrc.org/sites/default/files/document/file_list/autonomy_artificial_intelligence_and_robotics.pdf (última consulta: 25 de marzo de 2025).

Comité Internacional de la Cruz Roja (ICRC) y Geneva Academy, *Expert Consultation Report on AI and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts*, Ginebra, Comité Internacional de la Cruz Roja, marzo de 2024, p. 8, disponible en https://www.geneva-academy.ch/joomlatools-files/docman-files/Artificial%20Intelligence%20And%20Related%20Technologies%20In%20Military%20Decision-Making.pdf (última consulta: 16 de abril de 2025).

CORDIS, *Periodic Reporting for Period 2 - AI-ARC (Artificial Intelligence based Virtual Control Room for the Arctic (AI-ARC))*, periodo de reporte: 2022-09-01 a 2024-02-29, disponible en https://cordis.europa.eu/project/id/101021271/reporting (última consulta: 18 de febrero de 2025).

CORDIS, *The Next Generation of Maritime Awareness and Surveillance*, disponible en https://cordis.europa.eu/article/id/452691-the-next-generation-of-maritime-awareness-and-surveillance (última consulta: 18 de febrero de 2025).

CUHK Communications and Public Relations Office, *"The Chinese University of Hong Kong satellite was successfully launched into space orbit to celebrate the 75th anniversary of the founding of New China"*, comunicado de prensa, 24 de septiembre de 2024, disponible en https://www.cpr.cuhk.edu.hk/tc/press/%E9%A6%99%E6%B8%AF%E4%B8%AD%E6%96%87%E5%A4%A7%E5%AD%B8%E8%A1%9E%E6%98%9F%E6%88%90%E5%8A%9F%E7%99%BC%E5%B0%84%E9%80%B2%E5%85%A5%E5%A4%AA%E7%A9%BA%E8%BB%8C%E9%81%93-%E7%8D%BB%E7%A6%AE%E6%96%B0%E4%B8%AD/ (última consulta: 3 de febrero de 2025).

Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, *Consolidated Risk in Focus: Gen AI and Elections*, 18 de enero de 2024, disponible en https://www.cisa.gov/sites/default/files/2024-05/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf (última consulta: 20 de abril de 2025).

E. Dans, "Facial recognition is here to stay, but can we control its use?", disponible en https://www.forbes.com/sites/enriquedans/2020/06/11/facial-recognition-is-here-to-stay-but-can-we-control-itsuse/ (última consulta: 3 de febrero de 2025).

J. Dastin, "Google rebrands Bard chatbot as Gemini, rolls out paid subscription", *Reuters*, 8 de febrero de 2024, disponible en https://www.reuters.com/technology/google-rebrands-bard-chatbot-gemini-rolls-out-paid-subscription-2024-02-08/ (última consulta: 17 de marzo de 2025).

N. Davison, “A legal perspective: Autonomous weapon systems under international humanitarian law”, en *UNODA Occasional Papers No. 30, November 2017*, enero 2018, p. 5-18.

Declaración, *"ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform: OTPLink"*, declaración del 24 de mayo de 2023. Publicado por la Corte Penal Internacional, disponible en https://www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink (última consulta: 31 de marzo de 2025).

Departamento de Seguridad Nacional de los Estados Unidos, *Artificial Intelligence Roadmap*, 15 de marzo de 2024, disponible en https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf (última consulta: 18 de febrero de 2025).

N. de Rivière, “Russia Continues to Blatantly Violate International Humanitarian Law”, declaración ante el Consejo de Seguridad, Misión Permanente de Francia ante las Naciones Unidas en Nueva York, 9 de octubre de 2023, disponible en https://onu.delegfrance.org/russia-continues-to-blatantly-violate-international-humanitarian-law (última consulta: 5 de abril de 2025).

C. Dumbrava, *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues*, Member’s Research Service, p. 10, disponible en https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf (última consulta: 27 de abril de 2025).

L. Edwards, *The EU AI Act: a summary of its significance and scope*, Ada Lovelace Institute, abril 2022, p. 4, disponible en https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf (última consulta: 16 de abril de 2025).

Electoral Commission, *"Information about Cyber Attack on Electoral Commission Systems"*, última actualización: 30 de julio de 2024, disponible en https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems/information-about-cyber-attack (última consulta: 21 de febrero de 2025).

J. Escudero Méndez, *Brasil: El Senado aprueba el Proyecto de Ley 2338/2023 sobre el uso de la inteligencia artificial*, Instituto Autor, 10 de enero de 2025, disponible en https://institutoautor.org/el-senado-de-brasil-aprueba-el-proyecto-de-ley-2338-2023-sobre-el-uso-de-la-inteligencia-artificial/ (última consulta: 17 de abril de 2025).

European Agency for Safety and Health at Work, *Integrating artificial intelligence at work: automation of tasks*, 27 de junio de 2024, https://healthy-workplaces.osha.europa.eu/en/media-centre/news/integrating-artificial-intelligence-work-automation-tasks (última consulta: 18 de marzo de 2025).

European Space Agency, *New satellite to show how AI advances Earth observation*, 2 de julio de 2024, disponible en https://www.esa.int/Applications/Observing_the_Earth/Phsat-2/New_satellite_to_show_how_AI_advances_Earth_observation (última consulta: 3 de febrero de 2025).

Forbes, *AI 50 List*, ed. Kenrick Cai, 11 de abril de 2024, disponible en https://www.forbes.com/lists/ai50/ (última consulta: 17 de marzo de 2025).

Frontex, *Industry Day on Artificial Intelligence Tools for Seamless Border Checks at European Border Crossing Points*, 23 de enero de 2025, disponible en https://www.frontex.europa.eu/innovation/announcements/industry-day-on-artificial-intelligence-tools-for-seamless-border-checks-at-european-border-crossing-points-lUTEhX (última consulta: 18 de febrero de 2025).

Garante per la protezione dei dati personali, "Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori", 31 de marzo de 2023, disponible en https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847 (última consulta: 14 de abril de 2025).

R. A. Gati, M. Rizki y R. Y. Posumah, *"Artificial Intelligence and Indonesia Government Cyber Security Strategies"*, en *International Conference on Public Organization*, 2020.

S. González, "Claves del Reglamento Europeo de Inteligencia Artificial (RIA)", ITCL Centro Tecnológico, 14 marzo 2024, disponible en https://itcl.es/blog/reglamento-europeo-inteligencia-artificial/ (última consulta: 16 de abril de 2025).

Grand View Research, *AI in Retail Market Analysis Report*, disponible en https://www.grandviewresearch.com/industry-analysis/ai-retail-market-report (última consulta: 17 de marzo de 2025).

A. Guterres, "Davos 2024: Special Address by António Guterres, Secretary-General of the United Nations", *World Economic Forum*, 17 de enero de 2024, disponible en https://www.weforum.org/stories/2024/01/davos-2024-special-address-by-antonio-guterres-secretary-general-of-the-united-nations/ (última consulta: 15 de marzo de 2025).

G. Hardesty, "Foreign Election Interference Has a Long History", University of Southern California – Sol Price School of Public Policy, 1 de noviembre de 2024, disponible en https://priceschool.usc.edu/news/foreign-election-interference-has-a-long-history/ (última consulta: 6 de abril de 2025).

C. Hernandez-Roy, R. Bledsoe y G. Marma-Gutierrez, "Ensuring Information Integrity in Electoral Processes in the Americas", Center for Strategic & International Studies, 28 de julio de 2023, disponible en https://www.csis.org/analysis/ensuring-information-integrity-electoral-processes-americas (última consulta: 5 de abril de 2025).

M. Hewes, *"*Cómo la inteligencia artificial cambiará la seguridad informática y la seguridad física de la información en el mundo nuclear*"*, *Boletín del OIEA*, junio de 2023, p. 14. Publicado por el Organismo Internacional de Energía Atómica, disponible en https://www.iaea.org/sites/default/files/6421415es.pdf (última consulta: 31 de marzo de 2025).

F. Hicks, *AI in Military Drones: Redefining National Defense Strategies*, Aegis Softtech, disponible en https://www.aegissofttech.com/insights/ai-in-military-drones/#:~:text=AI%20

in%20Drone%20Navigation&text=By%20integrating%20AI%20algorithms%20with,in%20planning%20their%20routes%20dynamically (última consulta: 25 de marzo de 2025).

High-Level Advisory Body on Artificial Intelligence, *United Nations Office for Digital and Emerging Technologies*, disponible en https://www.un.org/digital-emerging-technologies/ai-advisory-body (última consulta: 16 de abril de 2025).

Human Rights Watch, "Questions and Answers: Israeli Military's Use of Digital Tools in Gaza", 10 de septiembre de 2024, disponible en http://hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza#:~:text=Another%2C%20which%20the%20military%20calls,labeling%20them%20as%20military%20targets. (última consulta: 25 de marzo de 2025).

IBM, "Getting ready for artificial general intelligence with examples", 18 de abril de 2024, disponible en https://www.ibm.com/think/topics/artificial-general-intelligence-examples (última consulta: 17 de abril de 2025).

IBM, "What are large language models (LLMs)?", 2 de noviembre de 2023, disponible en https://www.ibm.com/think/topics/large-language-models (última consulta: 15 de marzo de 2025).

IBM. "What is machine learning?" *IBM*, 2025, https://www.ibm.com/think/topics/machine-learning. (última consulta: 18 de marzo de 2025).

International Association of Privacy Professionals, *Global AI Law and Policy Tracker*, noviembre de 2024, disponible en https://iapp.org/resources/article/global-ai-legislation-tracker/ (última consulta: 27 de abril de 2025).

International Committee for Robot Arms Control, *Berlin Statement*, octubre 2010, disponible en https://www.icrac.net/statements/? (última consulta: 23 de abril de 2025).

International Labour Organization (ILO) and UNICEF. *Executive Summary: Child Labour. Global Estimates 2020, Trends and the Road Forward*. 2020. https://www.ilo.org/media/384736/download. (última consulta: 18 de marzo de 2025).

Irish Computer Society, *Comparison of Council of Europe Framework Convention on Artificial Intelligence with the European Union Artificial Intelligence Act*, 29 de octubre de 2024, disponible en https://ics.ie/2024/10/29/comparison-of-council-of-europe-framework-convention-on-artificial-intelligence-with-the-european-union-artificial-intelligence-act/#:~:text=Legal%20Scope%20and%20binding%20nature,third%20countries%20around%20the%20world. (última consulta: 16 de abril de 2025).

N. Kartha y W.D. Young, *An Overview of Algorithmic Bias in Artificial Intelligence*, University of Texas at Austin, p. 4, https://hdl.handle.net/2152/86530 (última consulta: 14 de abril de 2025).

D. Kelly, *A Modern-Day Space Race: Artificial Intelligence is the New Frontier*, disponible en https://americanedgeproject.org/a-modern-day-space-race- artificial-intelligence-is-the-new-frontier/ (última consulta: 27 de enero de 2025).

H.-K. Kim, “Sentry Robots in Action: Ethical and Legal Issues of Automated Weapon in South Korea,” en *ICRES 2022: 7th International Conference on Robot Ethics and Standards*, Seúl, Corea del Sur, 18-19 de julio de 2022, p. 41-44.

T. Krupiy, *"What role artificial intelligence could play in evaluating the compliance of military operations with international humanitarian law: The case study of the conduct of hostilities in Ukraine"*, en *EJIL:Talk!, Blog of the European Journal of International Law*, 23 de febrero de 2024, disponible en https://www.ejiltalk.org/what-role-artificial-intelligence-could-play-in-evaluating-the-compliance-of-military-operations-with-international-humanitarian-law-the-case-study-of-the-conduct-of-hostilities-in-ukraine/#:~:text=It%20is%20put%20forward%20that,spreading%20terror%20among%20the%20civilian (última consulta: 23 de abril de 2025).

J. Larson et al., “How We Analyzed the COMPAS Recidivism Algorithm”, ProPublica, 23 de mayo de 2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm (última consulta: 14 de abril de 2025).

J. Mackay Stanhope, “Opposing Inherent Immorality in Autonomous Weapons Systems”, *The Forge*, Australian Defence College, 6 de abril de 2021, https://theforge.defence.gov.au/article/opposing-inherent-immorality-autonomous-weapons-systems (última consulta: 25 de marzo de 2025).

N. Mäki, *Between Peace and Technology – A Case Study on Opportunities and Responsible Design of Artificial Intelligence in Peace Technology*, Laurea University of Applied Science, Vantaa, 2020.

"Malaysia streamlines border control and protection forces", *Vietnam+*, 3 de febrero de 2025, disponible en https://en.vietnamplus.vn/malaysia-streamlines-border-control-and-protection-forces-post309212.vnp (última consulta: 18 de febrero de 2025).

B. McKernan and H. Davies, “‘The machine did it coldly’: Israel used AI to identify 37,000 Hamas targets”, *The Guardian*, 3 de abril de 2024, disponible en https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes (última consulta: 23 de marzo de 2025).

Y. Mei y M. Sag, *The Illusion of Rights based AI Regulation*, 27 de febrero de 2025, p. 3, https://doi.org/10.48550/arXiv.2503.05784 (última consulta: 16 de abril de 2025).

C. Metz y M. Tobin, “How Chinese A.I. Start-Up DeepSeek Is Competing With Silicon Valley Giants,” *The New York Times*, 23 de enero de 2025, disponible en https://www.nytimes.com/2025/01/23/technology/deepseek-china-ai-chips.html (última consulta: 15 de marzo de 2025).

Organisation for Economic Co-operation and Development, *G20 Ministerial Statement on Trade and Digital Economy*, publicado el 9 de junio de 2019 en *OECD.AI Policy Observatory*, disponible en https://wp.oecd.ai/app/uploads/2021/06/G20-AI-Principles.pdf (última consulta: 17 de abril de 2025).

Microsoft y UNFCCC, *UNFCCC partners with Microsoft to use AI and advanced data technology to track global carbon emissions and assess progress under the Paris Agreement*, Microsoft News Center, 29 de noviembre de 2023, disponible en https://news.microsoft.com/2023/11/29/unfccc-partners-with-microsoft-to-use-ai-and-advanced-data-technology-to-track-global-carbon-emissions-and-assess-progress-under-the-paris-agreement/ (última consulta: 23 de abril de 2025).

Ministerio de Asuntos Exteriores de Japón, *Ministerial Statement on Trade and Digital Economy (Annex): G20 AI Principles*, disponible en https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf (última consulta: 17 de abril de 2025).

National Aeronautics and Space Administration, *"2024 AI Use Cases"*, 7 de enero de 2025, disponible en https://www.nasa.gov/general/2024-ai-use-cases/ (última consulta: 3 de febrero de 2025).

National Cyber Security Centre, *The Near-Term Impact of AI on the Cyber Threat*, 24 de enero de 2024, disponible en https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat (última consulta: 21 de febrero de 2025).

Newsroom, "*Council of Europe adopts first international treaty on artificial intelligence*", 17 de mayo de 2024, publicado por el Consejo de Europa, disponible en https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence (última consulta: 31 de marzo de 2025).

Organisation for Economic Co-operation and Development, *La IA generativa podría exacerbar las divisiones regionales en los países de la OCDE, según el primer análisis regional sobre su impacto en los mercados laborales locales*, 28 de noviembre de 2024, https://www.oecd.org/es/about/news/press-releases/2024/11/generative-ai-set-to-exacerbate-regional-divide-in-oecd-countries-says-first-regional-analysis-on-its-impact-on-local-job-markets.html (última consulta: 17 de abril de 2025).

Organisation for Economic Co-operation and Development/CAF, *Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe*, en *Estudios de la OECD sobre Gobernanza Pública*, OECD Publishing, Paris, 2022, https://doi.org/10.1787/5b189cb4-es (última consulta: 17 de abril de 2025).

OpenAI, "Introducing ChatGPT", 30 de noviembre de 2022, disponible en https://openai.com/index/chatgpt/ (última consulta: 14 de abril de 2025).

Organización de las Naciones Unidas, *United Nations Sustainable Development Goals*, disponible en https://www.un.org/sustainabledevelopment/ (última consulta: 17 de abril de 2025).

Parlamento Europeo, *Ley de IA de la UE: primera normativa sobre inteligencia artificial*, 12 de junio de 2023, https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial#calendario-de-aplicacin-de-la-ley-de-ia-de-la-ue-6 (última consulta: 16 de abril de 2025).

M.K. Pasupuleti., “AI’s Role in Global Stability, Diplomacy, and Peacebuilding”, en *AI-Powered Diplomacy and Conflict Resolutions*, National Education Services, febrero de 2025, p. 1-11.

B. Pino, *International Responsibility of States and Artificial Intelligence*, CEI, Centro Adscrito a la Universitat de Barcelona, 8 de mayo de 2020, disponible en https://diposit.ub.edu/dspace/bitstream/2445/170430/1/TFM_Beatriz_Pino.pdf (última consulta: 20 de abril de 2025).

A.P. Pokharel, “AI in Warfare: The Rise of Autonomous Weapons and the Future of Global Security,” *LinkedIn*, 10 de marzo de 2025, disponible en https://www.linkedin.com/pulse/ai-warfare-rise-autonomous-weapons-future-global-adrian-pokharel-zg3ee/ (última consulta: 25 de marzo de 2025).

Programa de las Naciones Unidas para el Medio Ambiente, ″La IA plantea problemas ambientales. Esto es lo que el mundo puede hacer al respecto.″, 21 de septiembre de 2024, disponible en https://www.unep.org/es/noticias-y-reportajes/reportajes/la-ia-plantea-problemas-ambientales-esto-es-lo-que-el-mundo-puede (última consulta: 21 de febrero de 2025).

PwC, *AI Analysis: Sizing the Prize Report*, PwC, p. 4., disponible en https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf (última consulta: 17 de marzo de 2025).

I. Reynolds y B. Jensen, “Machine Learning Meets War Termination: Using AI to Explore Peace Scenarios in Ukraine”, *Center for Strategic and International Studies*, febrero 2025, disponible en https://www.csis.org/analysis/machine-learning-meets-war-termination-using-ai-explore-peace-scenarios-ukraine (última consulta: 15 de marzo de 2025).

L. Romero, “US-China Cold War Is AI-Centric: Can OpenAI’s Stargate Settle It?”, *Forbes*, 23 de enero de 2025, disponible en https://www.forbes.com/sites/luisromero/2025/01/23/us-china-cold-war-is-ai-centric-can-openais-stargate-settle-it/ (última consulta: 17 de marzo de 2025).

J. Ruiz Valerio, *El Estado de derecho internacional. Una aproximación cartográfica a su definición*, Repositorio Universitario - Jurídicas de la UNAM, disponible en http://ru.juridicas.unam.mx:80/xmlui/handle/123456789/32432 (última consulta: 15 de marzo de 2025).

A. Saltini, "To avoid nuclear instability, a moratorium on integrating AI into nuclear decision-making is urgently needed: The NPT PrepCom can serve as a springboard", *European Leadership Network*, 28 de julio de 2023, disponible en https://europeanleadershipnetwork.org/commentary/to-avoid-nuclear-instability-a-moratorium-on-integrating-ai-into-nuclear-decision-making-is-urgently-needed-the-npt-prepcom-can-serve-as-a-springboard/ (última consulta: 31 de marzo de 2025).

I. Sánchez y G. Verdi, *Engaños digitales: Cómo un Escudo Europeo de la Democracia puede ayudar a hacer frente a la desinformación rusa*, 6 de junio de 2024, publicado por European Council on Foreign Relations, disponible en https://ecfr.eu/madrid/article/enganos-digitales-

como-un-escudo-europeo-de-la-democracia-puede-ayudar-a-hacer-frente-a-la-desinformacion-rusa/ (última consulta: 31 de marzo de 2025).

J. A. Sandhu, "What are LLMs and generative AI? A beginner's guide to the technology turning heads", Schwartz Reisman Institute for Technology and Society, 25 de enero de 2024, [en línea], disponible en https://srinstitute.utoronto.ca/news/gen-ai-llms-explainer#:~:text=While%20LLMs%20represent%20just%20one,%2C%20computer%20code%2C%20and%20more. (Última consulta: 18 de marzo de 2025).

J. Saura, *Implications of the use of drones in international law*, International Catalan Institute for Peace, disponible en https://www.icip.cat/perlapau/en/article/implications-of-the-use-of-drones-in-international-law/ (última consulta: 25 de marzo de 2025).

Senate Select Committee on Intelligence, *Report of the Select Committee on Intelligence on Russian Active Measures* (vol. 5), disponible en https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf (última consulta: 21 de febrero de 2025).

E. Shayotovich, "Everything we know about Samsung's machine gun robots", *SlashGear*, 1 de febrero de 2023, https://www.slashgear.com/825074/everything-we-know-about-samsungs-machine-gun-robots/ (última consulta: 23 de marzo de 2025).

Statista Research Department, *Artificial Intelligence (AI) in Finance*, Statista, 5 de abril de 2024, disponible en https://www.statista.com/topics/7083/artificial-intelligence-ai-in-finance/#topicOverview (última consulta: 17 de marzo de 2025).

The White House, "Putting America First in International Environmental Agreements" 23 de enero de 2025, disponible en https://www.whitehouse.gov/presidential-actions/2025/01/putting-america-first-in-international-environmental-agreements/ (última consulta: 17 de marzo de 2025).

R. ul Khaliq, "South deploys AI-powered systems to 'better monitor' North Korea," *Anadolu Agency*, 23 mayo 2024, disponible en https://www.aa.com.tr/en/artificial-intelligence/south-deploys-ai-powered-systems-to-better-monitor-north-korea/3228037 (última consulta: 25 de marzo de 2025).

UNESCO, "Shaping the future of justice in Rwanda: training of Judiciary on AI, Data Protection and the Rule of Law", 22 de abril de 2025, disponible en https://www.unesco.org/en/articles/shaping-future-justice-rwanda-training-judiciary-ai-data-protection-and-rule-law (última consulta: 24 de abril de 2025).

United Nations, "Artificial Intelligence (AI)", en *Global Issues*, disponible en https://www.un.org/en/global-issues/artificial-intelligence (última consulta: 17 de abril de 2025).

United Nations Climate Change Technology Executive Committee, *Artificial Intelligence for Climate Action in Developing Countries: Opportunities, Challenges and Risks*, p. 17, disponible en https://unfccc.int/ttclear/misc_/StaticFiles/gnwoerk_static/AI4climateaction/28da5d97d7824d16b7f68a225c0e3493/a4553e8f70f74be3bc37c929b73d9974.pdf (última consulta: 17 de marzo de 2025).

United Nations Department for General Assembly and Conference Management, *Definition of AI*, disponible en https://unterm.un.org/unterm2/es/view/49e80eb5-7736-4861-8f62-ffacfde67208 (última consulta: 17 de abril de 2025).

United Nations Office for Disarmament Affairs, *Lethal Autonomous Weapon Systems (LAWS)*, disponible en https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/ (última consulta: 18 de marzo de 2025).

United Nations Office for Disarmament Affairs, *The Convention on Certain Conventional Weapons*, disponible en https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/ (última consulta: 26 de abril de 2025).

United Nations University Centre for Policy Research, *Artificial Intelligence: Addressing or Distorting the Modern Slavery Challenge?*, octubre 2023, p. 3, disponible en https://unu.edu/sites/default/files/2023-10/AI%20addressing%20or%20distorting%20modern%20slavery%20challenge.pdf (última consulta: 18 de marzo de 2025).

United Nations y World Bank, *Pathways for Peace: Inclusive Approaches to Preventing Violent Conflict*, Washington DC, United States: World Bank, 2018.

Universidad Nacional Autónoma de México, *Teoría Tridimensional del Derecho*, disponible en https://repositorio-uapa.cuaed.unam.mx/repositorio/moodle/pluginfile.php/1466/mod_resource/content/4/contenido/index.html (última consulta: 7 de abril de 2025).

U.S. National Security Commission on Artificial Intelligence, *Final Report - National Security Commission on Artificial Intelligence*, 2021, p. 10, disponible en https://assets.foleon.com/eu-central-1/de-uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf (última consulta: 29 de marzo de 2025).

V. Van Roy *et al*, "AI Watch - National strategies on Artificial Intelligence: A European perspective"*, Publications Office of the European Union,* 2022, p. 139, https://publications.jrc.ec.europa.eu/repository/handle/JRC129123 (última consulta: 27 de abril de 2025).

V. Vinayak, "The Human Rights Implications of China's Social Credit System", Oxford Human Rights Hub, 6 septiembre 2019, https://ohrh.law.ox.ac.uk/the-human-rights-implications-of-chinas-social-credit-system/ (última consulta: 14 de abril de 2025).

A. Vinci, "The Coming Revolution in Intelligence Affairs: How Artificial Intelligence and Autonomous Systems Will Transform Espionage", *Foreign Affairs*, 31 de agosto de 2020, disponible en https://www.foreignaffairs.com/articles/united-states/2020-08-31/coming-revolution-intelligence-affairs (última consulta: 3 de abril de 2025).

E. Washabaugh, "The Robot, the Targeter and the Future of U.S. National Security", *The Cipher Brief*, 8 de marzo de 2021, disponible en https://www.thecipherbrief.com/the-robot-the-targeter-and-the-future-of-u-s-national-security (última consulta: 4 de abril de 2025).

World Economic Forum, "9 ways AI is helping tackle climate change," *World Economic Forum*, 12 de febrero de 2024, disponible en https://www.weforum.org/stories/2024/02/ai-combat-climate-change/#:~:text=

The%20use%20of%20artificial%20intelligence,the%20World%20Economic%20Forum%20says (última consulta: 17 de marzo de 2025).

A. Younger, "MI6 'C' speech on fourth generation espionage", publicado por *Foreign & Commonwealth Office, Secret Intelligence Service*, 3 de diciembre de 2018, disponible en https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage (última consulta: 3 de abril de 2025).

2. JURISPRUDENCIA

STEDH de 13 de diciembre de 2022, *Asunto de Glukhin v. Rusia* (Aplicación no. 11519/20).

3. TRATADOS

Acuerdo de París del 12 de diciembre de 2015, entrado en vigor el 4 de noviembre de 2016, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 54113).

Acuerdo que debe regir las actividades de los Estados en la Luna y otros cuerpos celestes de 5 de diciembre de 1979, entrado en vigor el 11 de julio de 1984, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 23002).

Carta de las Naciones Unidas del 26 de junio de 1945, entrado en vigor el 24 de octubre de 1945, publicado en la Colección de Tratados de las Naciones Unidas (registro s/n).

Carta de los Derechos Fundamentales de la Unión Europea del 7 de diciembre de 2000, entrado en vigor el 1 de diciembre de 2009, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 12016P/TXT).

Convención de Viena sobre Relaciones Consulares del 24 de abril de 1963, entrado en vigor el 19 de marzo de 1967, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 8638).

Convención de Viena sobre Relaciones Diplomáticas del 18 de abril de 1961, entrado en vigor el 24 de abril de 1964, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 7310).

Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial del 21 de diciembre de 1965, entrado en vigor el 4 de enero de 1969, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 9464).

Convención Marco de las Naciones Unidas sobre el Cambio Climático del 9 de mayo de 1992, entrado en vigor el 21 de marzo de 1994, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 30822).

Convención sobre los Derechos del Niño del 20 de noviembre de 1989, entrado en vigor el 2 de septiembre de 1990, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 27531).

Convención sobre Derechos y Deberes de los Estados del 26 de diciembre de 1933, entrado en vigor el 26 de diciembre de 1934, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 3802).

Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados del 10 de octubre de 1980, entrado en vigor el 2 de diciembre de 1983, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 22495).

Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y derechos humanos, democracia y Estado de derecho del 5 de septiembre de 2024, abierto a firma el 5 de septiembre de 2024, aún no entrado en vigor, publicado en la Colección de Tratados del Consejo de Europa (número de registro 225).

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales del 4 de noviembre de 1950, entrado en vigor el 3 de septiembre de 1953, publicado en la Colección de Tratados del Consejo de Europa (número de registro ETS No. 005).

Convenios de Ginebra del 12 agosto de 1949, entrados en vigor el 21 de octubre de 1950, publicados en la Colección de Tratados de las Naciones Unidas (números de registro 970-973).

Convenios de Ginebra del 12 agosto de 1949, Protocolos Adicional I y II, adoptados el 8 de junio de 1977, entrados en vigor el 7 de diciembre de 1978, publicados en la Colección de Tratados de las Naciones Unidas (número de registro 17512 y 17513).

Convenios de Ginebra del 12 agosto de 1949, Protocolo Adicional III, adoptado el 8 de diciembre de 2005, entrado en vigor el 14 de enero de 2007, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 43425).

Estatuto de Roma de la Corte Penal Internacional del 17 de julio de 1998, entrado en vigor el 1 de julio de 2002, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 38544).

Pacto Internacional de Derechos Civiles y Políticos del 16 de diciembre de 1966, entrado en vigor el 23 de marzo de 1976, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 14668).

Tratado de la Unión Europea del 7 febrero de 1992, entrado en vigor el 1 de noviembre de 1993, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 12016M/TXT).

Tratado del Funcionamiento de la Unión Europea del 13 de diciembre de 2007, entrado en vigor el 1 de diciembre de 2009, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 12016ME/TXT).

Tratado de No Proliferación Nuclear del 1 de julio de 1968, entrado en vigor el 5 de marzo de 1950, publicado en la Colección de Tratados de las Naciones Unidas (número de registro 10485).

4. DOCUMENTACIÓN

Asamblea General de las Naciones Unidas, borrador de Resolución “Aumentar la cooperación internacional para la creación de capacidad en materia de inteligencia artificial”, Doc. A/78/L.86 (2024).

Asamblea General de las Naciones Unidas, borrador de Resolución “Sistemas de armas autónomos letales”, Doc. A/C.1/79/L.77 (2024).

Asamblea General de las Naciones Unidas, Resolución 2625 (XXV), "Declaración sobre los principios de Derecho Internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas" (1970).

Asamblea General de las Naciones Unidas, Resolución 3314 (XXIX), Doc. A/RES/3314 (1974).

Asamblea General de las Naciones Unidas, Resolución 68/167, "El derecho a la privacidad en la era digital", Doc. A/RES/68/167 (2013).

Asamblea General de las Naciones Unidas, Resolución 78/265, “Aprovechar las oportunidades de sistemas seguros, protegidos y fiables de inteligencia artificial para el desarrollo sostenible”, Doc. A/RES/78/265 (2024).

Asamblea Nacional de Corea del Sur, *Proyecto de Ley Básica sobre el Desarrollo y la Creación de una Base de Confianza en la Inteligencia Artificial*, n.º 2206772 (2024).

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, *Ley Modelo sobre Contratación Automatizada*, aprobada el 11 de julio de 2024, doc. A/79/17, anexo IV.

Comisión de Derecho Internacional, *Proyecto de Artículos sobre la responsabilidad del Estado por Hechos Internacionalmente Ilícitos* (2001).

Comité de Derechos Humanos, Observación general núm. 16 (32º período de sesiones, 1994), doc. ONU HRI/GEN/1/Rev.1, (1994).

Consejo de Derechos Humanos de las Naciones Unidas, Informe A/HRC/44/24*, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, (2020).

Grupo de Expertos Gubernamentales sobre Sistemas de Armas Letales Autónomas, *Non-exhaustive compilation of definitions and characterizations*, CCW/GGE.1/2023/CRP.1, 2023.

Jefatura de Gabinete de Ministros de Argentina, Disposición 2/2023 “Recomendaciones para el uso de Inteligencia Artificial” (2023).

Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence*, doc. OECD/LEGAL/0449 (adoptada el 22 de mayo de 2019, enmendada el 3 de mayo de 2024).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, entrado en vigor el 25 de mayo de 2018, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 32016R0679).

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, entrado en vigor el 1 de agosto de 2024, publicado en la base de datos de la Unión Europea, EUR-Lex (documento no. 32024R1689).

S. 321, "Decoupling America's Artificial Intelligence Capabilities from China Act of 2025", 119º Congreso de EE. UU., presentado por Sen. Josh Hawley, 29 de enero de 2025.

Senado Federal de Brasil, *Projeto de Lei n° 2338* (2023).

United Nations AI Advisory Body, *Governing AI for Humanity: Final Report*, eISBN: 9789211067873 (2024).

UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, doc. SHS/BIO/PI/2021/1 (2022).

5. PÁGINAS WEB CONSULTADAS

EUR-Lex: https://eur-lex.europa.eu/homepage.html

Consejo de Europa: https://www.coe.int/en/web/portal/home

DeepSeek: https://www.deepseek.com/

OpenAI: https://openai.com/

Organización de las Naciones Unidas: https://www.un.org/es

Unión Europea: https://european-union.europa.eu/index_en

6. CLASES, CURSOS ACADÉMICOS Y PONENCIAS

J. B. Cartes Rodríguez, "*Clase sobre los Hechos Internacionalmente Ilícito*s", en *El Ordenamiento Jurídico Internacional: Sujetos y Normas*, Máster en Derecho internacional 2024-2025, Universidad Complutense de Madrid, 29 de octubre de 2024.

T. Rodríguez de las Heras Ballell, *Los riesgos de la inteligencia artificial en el comercio internacional*, presentación en el congreso "Los riesgos y los seguros en el comercio internacional – Jordana SEAIDA", Universidad Complutense de Madrid, 22 abril 2025.

Universidad Complutense de Madrid, *Certificado en Inteligencia Artificial en las Ciencias Sociales y Jurídicas · 4ª edición*, disponible en https://empowertalent.com/ucm/inteligencia-artificial/ (última consulta: 15 de marzo de 2025).