La Inteligencia Artificial en Seguridad Nacional: Marcos Regulatorios Internacionales y su Aplicabilidad normativa en Colombia

Leidy Lorena Espitia Rodríguez[1]

Resumen

La Inteligencia Artificial se ha convertido en la manera en que concebimos y organizamos nuestras sociedades, estableciendo nuevos paradigmas en la defensa, la ciberseguridad y la ética. Este escrito, de enfoque cualitativo y descriptivo, analiza los desafíos relacionados con su uso indebido y los diferentes impactos que conlleva. De igual manera, aborda los principales marcos regulatorios internacionales, incluyendo las disposiciones de organismos multilaterales como la ONU y la UNESCO, así como las normativas adoptadas por diversos países en materia de seguridad nacional. Finalmente, examina la viabilidad de adoptar aquellos marcos en el contexto normativo colombiano, verificando las políticas nacionales de Colombia y proponiendo lineamientos que equilibren la innovación tecnológica con el orden público y la protección de los derechos humanos.

Palabras clave: Inteligencia Artificial, Seguridad del Estado, Defensa, Ética, Derecho Internacional.

Abstract

Artificial Intelligence has become the way we conceive and organize our societies, establishing new paradigms in defense, cybersecurity, and ethics. This qualitative and descriptive paper analyzes the challenges related to its misuse and the various impacts it entails. It also addresses the main international regulatory frameworks, including the provisions of multilateral organizations such as the ONU and UNESCO, as well as the regulations adopted by various countries regarding national security. Finally, it examines the feasibility of adopting these frameworks in the Colombian regulatory context, reviewing Colombia's national policies and

[1] Universidad Colegio Mayor de Cundinamarca - Facultad de Derecho Estudiante de Derecho y de la Especialización en Derecho Internacional Público con Énfasis en Derechos Humanos.
Documento de trabajo resultado de la práctica investigativa dentro de la Especialización en Derecho Internacional Público.
Google Académico https://scholar.google.es/citations?view_op=new_articles&hl=es&imq=LEIDY+LORENA+ESPITIA+RODRIGUEZ#
CVLAC https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0002353580
ORCID https://orcid.org/0009-0001-5241-8

proposing guidelines that balance technological innovation with public order and the protection of human rights.

Keywords: Artificial Intelligence, State Security, Defense, Ethics, International Law.

Introducción

Durante muchos años, en el cine y la literatura se ha presentado un mundo donde las máquinas pueden razonar, comunicarse y tomar decisiones. Ejemplos icónicos incluyen: *Isaac Asimov con las leyes de la robótica, la visión futurista de Blade Runner dirigida por Ridley Scott* y la *inteligencia artificial HAL 9000 del 2001: una odisea en el espacio, obra de Clarke, Arthur C. y Kubrick Stanley*. Aunque esto parecía ser algo muy lejano de la realidad, hoy en día se ha vuelto en uno de los temas más debatidos a nivel mundial, con implicaciones profundas en diversos ámbitos de la sociedad.

Comúnmente las personas en general asocian la Inteligencia Artificial con el tema de sistemas, desarrollos de plataformas y herramientas que optimizan tareas, mejoran la productividad y facilitan la vida cotidiana. Esta percepción, se relaciona debido a que la especie humana siempre ha procurado crear herramientas que le faciliten su vida y realicen tareas operativas más sencillas, permitiendo enfocarse en otras cosas. Sin embargo, con una revisión exhaustiva nos damos cuenta que esta Inteligencia Artificial no solo es un instrumento tecnológico que puede ser adecuado para proteger las utilidades generales de la población, sino que también se ha convertido en un factor estratégico dentro de la seguridad nacional, pues su uso indebido puede comprometer infraestructuras críticas, afectar la defensa militar y poner en riesgo la soberanía de los países.

En este contexto, la IA se halla muy asociada con la seguridad nacional, especialmente en aspectos como la ética, la defensa y la ciberseguridad, pues no solo ponen en juego la estabilidad y el buen desarrollo de un Estado y su sociedad, sino que representa una transformación fundamental que requiere un enfoque equilibrado entre innovación, transparencia y responsabilidad.

Dando más profundidad a lo anterior, la IA no solo se limita a grandes empresas tecnológicas como lo es Google, Facebook, Apple o Microsoft, sino que es un elemento

importante que vas más allá en la evolución del cumplimiento de la ley, donde la protección de la sociedad es lo más importante para el estado. Ante ello, los gobiernos y organismos reconocen que existe un riesgo eminente en la vulneración de la seguridad, en la medida de que influyen delitos informáticos, investigación de temas militares, tratamiento de base de datos, información importante de los diferentes países e incluso ciberterrorismo, que han causado daños sociales y económicos. Por esto, han mejorado sus capacidades de ciberdefensa y seguridad de la información, dando el surgimiento de nuevas leyes y normas técnicas y dedicando más recursos a gestionar la seguridad en el ciberespacio y en otros aspectos sociales.

Por otro lado, dentro del contexto colombiano, existen algunas leyes de tratamiento y protección de datos y una estructura organizacional en materia de ciberdefensa en los niveles operacional, estratégico y táctico, pero en comparación con otros países se queda corto en el marco normativo de la IA, ya que carece de una regulación específica que establezca directrices claras sobre su desarrollo, uso y control en el ámbito de la seguridad nacional. Con todo este panorama es clave preguntarnos: ¿Cómo puede Colombia fortalecer su marco normativo en Inteligencia Artificial para garantizar un uso seguro y responsable en el ámbito de la seguridad nacional, tomando como referencia los marcos regulatorios internacionales?

Ante ello, es imprescindible que el Estado Colombiano primero tenga los recursos y mecanismos de control suficientes para dar paso a la estructura de un marco normativo. De igual modo, que tenga la capacidad de formar alianzas y desarrolle estrategias de cooperación internacional para mejorar la ciberseguridad nacional, la defensa estatal y proteger su infraestructura crítica, sin dejar atrás la soberanía digital del país, la ética y garantías individuales.

Metodología

El presente estudio se implementa por medio de un enfoque cualitativo con alcance descriptivo desde la metodología de Sampieri, ya que se dará la recolección de datos con evidencias de textos argumentativos, documentos científicos y artículos académicos, en donde analizará e interpretará el impacto de la IA en la defensa, la ciberseguridad y la ética, haciendo énfasis en la aplicabilidad normativa de los diferentes estándares internacionales y

dando una visión de lo establecido en Colombia, contribuyendo a la implementación de posibles soluciones.

Para ello, se examinarán documentos clave como el "Marco ético para la inteligencia artificial en Colombia" (Mintic,2020), la Política Nacional de Transformación Digital e Inteligencia Artificial (CONPES 3975 de 2019), y el Documento CONPES 3995 de 2020 sobre ciberseguridad y ciberdefensa. Asimismo, se revisarán normativas internacionales como los principios de la UNESCO, estrategias de seguridad y defensa en IA de potencias como EE.UU., la Unión Europea y China, lineamientos de organismos multilaterales como la ONU.

Resultados

Los beneficios de la IA son abundantes y ofrecen soluciones tecnológicas en varios campos de la sociedad. Sin embargo, hay riesgos éticos, de desarrollo, de ciberseguridad y de privacidad de datos como lo veremos a lo largo de este estudio.

En primer lugar, haremos alusión a la Seguridad Nacional, que ha sido un concepto que ha adoptado la mayoría de potencias globales, teniendo estrechamente relacionado los principios de responsabilidad, legalidad, transparencia, coordinación y cooperación respecto a los derechos humanos y el ámbito estatal. Si bien, ha hecho énfasis en la defensa nacional, en el terrorismo, en el crimen organizado, en la ciberseguridad y en la contrainteligencia, teniendo como misión la preservación de la soberanía y la seguridad del estado frente a las adversidades y/o peligros que confrontan todos los países. Uno de los problemas que más acarrea en la seguridad nacional es el manejo de la IA, pues su digitalización masiva y su perseverante evolución del software, el hardware y su integración con demás apps ocasionan vulnerabilidades de protección de datos importantes e información sensible que puede ser manipulada para desestabilizar naciones y que son utilizadas por los ciberdelincuentes.

Además, aquella seguridad nacional también se ve afectada en el ámbito ético, ya que la IA puede perjudicar la privacidad y los derechos individuales, incluso no tiene la idoneidad de comprender el contexto o el impacto de sus elecciones. Por lo que es importante que aquellos expertos que realizan algoritmos y desarrollan la IA incluyendo también los Estados

tengan la máxima responsabilidad de regular el uso de esos sistemas, manteniendo los principios éticos y legales.

Ahora bien, dentro del campo de la defensa se denota un desafío crucial en que se utilice esta inteligencia artificial con fines perjudiciales, como sucede con ataques terroristas que emplean ciber espionaje avanzado o la creación de armas autónomas. Adicionalmente, la IA no solo puede ser una tecnología de desequilibrio militar, sino también un elemento perturbador en el orden económico, industrial y social que puede afectar inmediatamente el contexto estratégico internacional.

Por ello, estos desafíos requieren de una creación de marcos regulatorios adecuados y cooperación internacional para asegurar su uso responsable. Si bien, la implementación de la IA, está conectada con las mayores potencias del mundo y a su vez con organismos multilaterales en lo que respecta a políticas de defensa e implementación de planes estratégicos normativos hacia el futuro como, por ejemplo:

Dentro de la ONU, el Consejo de Seguridad ha hecho mención a ciertos riesgos del uso de la IA con propósitos violentos y/o revolucionarios, dando en argumento las diversas ciberdelincuencias que están direccionando a las instalaciones críticas, intervenciones humanitarias y consolidación de la paz. Por ello esta organización, recomienda actuar con celeridad en la regulación de dicha tecnología, estableciendo el llamamiento de algunos países que se consolidan, con el objetivo de establecer un nuevo organismo de la ONU que defienda los proyectos comunitarios para dirigir estas nuevas tecnologías, desarrollando métodos de prueba para evaluar sus capacidades y posibles fallas de seguridad.

Del mismo modo, en el año 2021, la organización UNESCO desarrollo los principios universales sobre la integridad de la IA, enfocándose en la protección de los derechos fundamentales y la dignidad, teniendo como fundamento las bases principales como son: transparencia e imparcialidad, rememorando la transcendencia del control de las personas en los sistemas de la IA.

En el caso de EE.UU., su eventual estrategia de Seguridad Nacional destaca la tecnología y la IA como elemento esencial de la actual competición internacional. En 2023, la ordenación de la IA en Estados Unidos alcanzó un hito con una jerarquía diligente de Joe

Biden, que establece estándares de seguridad nacional y promueve el liderazgo estadounidense globalmente. Dentro de ella, se establecen diversas acciones sobre la inteligencia artificial, en donde varias agencias, buscarán comentarios del público y evaluarán riesgos y beneficios de modelos de IA. Esta orden ejecutiva guía a los líderes de las agencias a crear directrices sobre el uso responsable de la IA, como por ejemplo las colisiones negativas de la IA en los trabajadores, estrategias de salud con la IA, desarrollo de políticas y recursos en la enseñanza y el aprendizaje, la utilización de la IA en el método de equidad disciplinaria, y entre otras cosas. De igual forma, se instaura una Junta de I.A de la Casa Blanca, en donde se encuentra comités especializados en IA y un grupo de trabajo que conlleve las operaciones gubernamentales con el uso de la IA.

China, por el contrario, contiene una seguridad nacional con un método de cesión proyectado para conformar el ámbito civilizado y marcial bajo distintas etapas de indagación y crecimiento con disposiciones militares de IA. De igual manera, enuncia una ley que introduce aspectos como el progreso y fomentación de la IA, la custodia de derechos, responsabilidades de protección, inspección y diligencia, cooperación internacional y responsabilidades legales. Su estrategia normativa más reciente se ha basado en que los sistemas de IA deben considerar los valores marxistas primordiales, la integralidad comunitaria y la moral profesionista, dejando en prohibición la generación de contenidos que vulneren la seguridad nacional, la estabilidad social, la unidad territorial o los derechos e intereses colectivos.

En esa misma línea, la Gestión Europea en el año 2019 constituyo el orden técnico de alto grado sobre IA, en donde se presentaron directrices de moralidad para la IA de confianza, que establece ciertos requisitos fundamentales: supervisión humana, la transparencia, la no discriminación, el vigor técnico y de seguridad, el bienestar social y la privacidad y gobernanza de datos. Su principal enfoque es que el ciudadano sea un elemento esencial en la implementación de la IA. Además, cabe decir, que la UE dentro de su política común de seguridad y defensa (PCSD), integrada en la Politica Exterior y de Seguridad Comun (PESC), busca fortalecer la capacidad para gestionar crisis, garantizar la seguridad de sus ciudadanos y desarrollar capacidades militares.

Por otra parte, dentro del contexto colombiano desde hace aproximadamente dos décadas, se ha empezado a considerar e incluso a implementar la I.A como un instrumento de desarrollo para afrontar los desafíos de la IV revolución industrial. No obstante, el legislador no ha mostrado un interés significativo en establecer políticas adecuadas para su gestión ni en desarrollar regulaciones que aborden los posibles problemas derivados de su uso. Aunque, existen algunas leyes importantes que han dado los primeros pasos respecto a la protección y manejo de datos, así como también el tema de la ciberseguridad aún se ve un vacío normativo para regular distintos aspectos de la Inteligencia Artificial.

(Imagen #1: regulación normativa en Colombia – Elaboración propia)

De acuerdo a lo anterior, podemos evidenciar que no hay una ley u norma específica en Colombia que regule la IA en seguridad nacional, gracias a que existen desafíos que dificultan su implementación.

Entre estos desafíos se encuentra la brecha tecnológica, en donde las fuerzas de seguridad y las instituciones colombianas carecen en muchos casos de los recursos necesarios para implementar soluciones avanzadas de IA, lo que limita su efectividad frente a las amenazas. Además, la regulación de los derechos de las personas, es un aspecto crítico, pues el uso de la IA en vigilancia y monitoreo genera preocupaciones sobre la privacidad de los ciudadanos colombianos, haciendo imprescindible garantizar que su aplicación no infrinja los principios básicos. Asimismo, la desigualdad regional representa un obstáculo, ya que la infraestructura tecnológica en algunas zonas rurales de Colombia sigue siendo limitada, lo que dificulta la implementación uniforme de tecnologías de IA en todo el país.

Por consiguiente, para que Colombia pueda aplicar los estándares internacionales de manera efectiva, es necesario implementar reformas y fortalecer la regulación en varios frentes como, por ejemplo: el desarrollo de un marco legal específico sobre IA**,** puesto que Colombia debe trabajar en la instauración de leyes que regulen específicamente el uso de la IA en sectores sensibles como la seguridad nacional, alineándose con los principios internacionales de ética y derechos humanos, en donde defina límites de uso, supervisión y sanciones; establecer un órgano de supervisión independiente que evalúe el uso de IA en defensa y seguridad; una colaboración internacional, en vista de que Colombia debería intensificar la cooperación con organismos internacionales, para intercambiar experiencias y mejorar las alternativas del uso de IA en seguridad nacional; la capacitación y recursos, debido a que es fundamental aumentar la capacitación en IA para las fuerzas de seguridad y los operadores públicos, y destinar recursos adecuados para el desarrollo de infraestructura tecnológica en todo el país.

Conclusión

La IA está transformando profundamente la seguridad nacional a nivel global, ofreciendo nuevas capacidades para la defensa, la ética y la ciberseguridad. Sin embargo, su implementación plantea desafíos significativos, especialmente en términos legales y éticos. Colombia, al igual que otros países, debe adaptar su marco normativo para aprovechar los beneficios que trae consigo la inteligencia artificial mientras protege lo principios básicos de sus ciudadanos. A medida que la tecnología avanza, es crucial que se adopten políticas y regulaciones que promuevan una implementación responsable y transparente de la IA en la seguridad nacional con el desarrollo de una nueva ley nacional, colaboración internacional para intercambiar experiencias y mejorar el uso de IA en la protección nacional, capacitación y recursos adecuados para el desarrollo de infraestructura tecnológica en todo el país.

Referencias

Documentos CONPES. (2024). https://goo.su/kMvEP6v

Garat, J. (2024) *La inteligencia artificial como factor de transformación de las operaciones militares en el nivel operacional.* https://goo.su/pZFZ

Global Affairs and Strategic Studies (2023). *El reto de la inteligencia artificial para la seguridad y defensa.* https://goo.su/nNAB0t

Guío, A. (2020) *Marco ético para la inteligencia artificial en Colombia.* https://www.usergioarboleda.edu.co/wp-content/uploads/2021/11/Marco-etico-para-lainteligencia- artificial-en-Colombia-Maestria-en-Inteligencia-artificial.pdf

Irribarren, A. (2023) *Análisis comparativo de la regulación de la inteligencia artificial en la unión europea y estados unidos* https://ddd.uab.cat/pub/tfg/2023/303428/TFG_alluisiribarren.pdf

Ley 1266 de 2008 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1273 de 2009 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Morandin, (2023). *Principios normativos para una ética de la inteligencia artificial". Consejo de ciencia y tecnología del estado de puebla.* https://philpapers.org/archive/MORIUE-2.pdf

ONU (2024) *Inteligencia Artificial: Un cambio revolucionario para el desarrollo sostenible*. https://goo.su/uHVd2

Romero, G (2019) *Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados*. Revista de la Escuela Superior de Guerra Naval. https://portal.amelica.org/ameli/journal/262/2621457007/html/index.html

Valls, M. (2018) *La inteligencia artificial y su encaje en las Estrategias de Seguridad Nacional.* Instituto español de estudios estratégicos. https://goo.su/Ym1m5T