

**Estrategias jurídicas para la aplicación de normas éticas y deontológicas
en el uso de las tecnologías de información y comunicación**

**Legal strategies for the application of ethical and deontological standards
in the use of ICTs**

*Stratégies juridiques pour l'application des normes éthiques et déontologiques
dans l'utilisation des technologies de l'information et de la communication*

**Estratégias legais para a aplicação de padrões éticos e deontológicos no uso de
tecnologias de informação e comunicação**

Ricardo M. Candanedo Yau

Universidad de Panamá, Centro Regional Universitario de Panamá Este, Panamá

ricardo.candanedo@up.ac.pa

 <https://orcid.org/0009-0002-5017-9830>

DOI: <https://doi.org/10.48204/contacto.v6n1.8888>

Recibido: 25/02/2026

Aceptado: 23/04/2026

RESUMEN

El objetivo de este estudio es identificar y analizar las estrategias jurídicas que respaldan la aplicación de normas éticas y deontológicas en el uso de las Tecnologías de Información y Comunicación (TIC). La descripción del estudio se centra en el examen de marcos normativos, políticas institucionales y prácticas de regulación ética implementadas en contextos educativos, administrativos y tecnológicos. La metodología utilizada corresponde a una revisión sistemática de carácter descriptivo, basada en la recopilación, clasificación y análisis de documentos académicos, legislaciones y estudios comparados publicados entre 2015 y 2025, complementada con tablas de porcentajes para visualizar la frecuencia de las estrategias analizadas. Los resultados evidencian que las acciones más recurrentes incluyen la actualización de marcos legales, la adopción de códigos de conducta, el fortalecimiento de mecanismos de supervisión y la promoción de programas de formación ética vinculados al uso responsable de las TIC. Asimismo, se observa un incremento de iniciativas orientadas a la privacidad de datos, la transparencia en el uso de algoritmos y la ciberseguridad. Se concluye que la aplicación eficaz de normas éticas y deontológicas en el ámbito digital exige estrategias jurídicas integrales, flexibles y coordinadas, capaces de responder a los desafíos derivados de la transformación tecnológica.

Palabras clave: ciberseguridad, códigos de conducta, ética profesional, legislación, tecnología de la información.

ABSTRACT

The objective of this study is to identify and analyze the legal strategies that support the effective application of ethical and deontological standards in the use of Information and Communication Technologies (ICT). The study describes existing regulatory frameworks, institutional policies, and ethical oversight practices implemented across educational, administrative, and technological contexts. The methodology consists of a descriptive systematic review based on the collection, classification, and analysis of academic documents, legislation, and comparative studies published between 2015 and 2025, supported by percentage tables that illustrate the frequency of the identified strategies. The findings show that the most recurrent measures include the modernization of legal frameworks, the adoption of sector-specific codes of conduct, the strengthening of monitoring mechanisms, and the promotion of ethical training related to responsible ICT use. Additionally, there is growing attention to data privacy, algorithmic transparency, and cybersecurity. The study concludes that the effective application of ethical and deontological norms in digital environments requires comprehensive, adaptable, and coordinated legal strategies capable of responding to ongoing technological transformation.

Keywords: codes of conduct, cybersecurity, information technology, legislation, professional ethics.

RÉSUMÉ

L'objectif de cette étude est d'identifier et d'analyser les stratégies juridiques favorisant l'application des normes éthiques et professionnelles dans l'utilisation des technologies de l'information et de la communication (TIC). L'étude porte sur l'examen des cadres réglementaires, des politiques institutionnelles et des pratiques de régulation éthique mises en œuvre dans les contextes éducatifs, administratifs et technologiques. La méthodologie employée est une revue systématique descriptive, fondée sur la collecte, la classification et l'analyse de documents académiques, de textes législatifs et d'études comparatives publiés entre 2015 et 2025, complétée par des tableaux de pourcentages permettant de visualiser la fréquence des stratégies analysées. Les résultats montrent que les actions les plus fréquentes consistent à actualiser les cadres juridiques, à adopter des codes de conduite, à renforcer les mécanismes de contrôle et à promouvoir des programmes de formation à l'éthique relatifs à l'utilisation responsable des TIC. Par ailleurs, on observe une augmentation des initiatives axées sur la protection des données, la transparence dans l'utilisation des algorithmes et la cybersécurité. Il apparaît donc que l'application effective des normes éthiques et professionnelles dans le domaine numérique exige des stratégies juridiques globales, flexibles et coordonnées, capables de répondre aux enjeux posés par la transformation technologique.

Mots-clés: cybersécurité, codes de conduite, déontologie professionnelle, législation, technologies de l'information.

RESUMO

O objetivo deste estudo é identificar e analisar as estratégias legais que apoiam a aplicação de padrões éticos e profissionais no uso das Tecnologias da Informação e Comunicação (TICs). O estudo concentra-se no exame de marcos regulatórios, políticas institucionais e práticas de regulação ética implementadas em contextos educacionais, administrativos e tecnológicos. A metodologia empregada é uma revisão sistemática descritiva, baseada na coleta, classificação e análise de documentos acadêmicos, legislação e estudos comparativos publicados entre 2015 e 2025, complementada por tabelas de porcentagem para visualizar a frequência das estratégias analisadas. Os resultados mostram que as ações mais recorrentes

incluem a atualização de marcos legais, a adoção de códigos de conduta, o fortalecimento de mecanismos de supervisão e a promoção de programas de formação ética relacionados ao uso responsável das TICs. Além disso, houve um aumento nas iniciativas focadas na privacidade de dados, na transparência no uso de algoritmos e na segurança cibernética. Conclui-se que a aplicação efetiva de padrões éticos e profissionais na esfera digital exige estratégias jurídicas abrangentes, flexíveis e coordenadas, capazes de responder aos desafios decorrentes da transformação tecnológica.

Palavras-chave: cibersegurança, códigos de conduta, ética profissional, legislação, tecnologia da informação.

Introducción

La acelerada expansión de las Tecnologías de Información y Comunicación (TIC) ha generado transformaciones profundas en los ámbitos social, educativo, administrativo y jurídico, creando escenarios donde convergen oportunidades de innovación y desafíos éticos significativos. El uso intensivo de estas herramientas plantea interrogantes sobre la protección de derechos fundamentales, la gestión responsable de la información, la privacidad, la transparencia y la responsabilidad institucional. La incorporación de tecnologías emergentes, como la inteligencia artificial, el análisis masivo de datos, los algoritmos decisionales y los sistemas interconectados, ha intensificado tensiones entre los marcos normativos vigentes y las prácticas adoptadas por usuarios, organizaciones y gobiernos. Esta situación ha impulsado a organismos internacionales como UNESCO (2021, 2024), la Organización de las Naciones Unidas (United Nations, 2020), la OCDE (2019; OECD, 2023) y la Unión Europea (European Union, 2016; European Commission, 2021) han promovido lineamientos éticos orientados al uso responsable de tecnologías digitales, fundamentados en principios de equidad, justicia algorítmica, transparencia, seguridad digital y dignidad humana.

En paralelo, el desarrollo tecnológico ha ampliado la capacidad humana para acceder, procesar y difundir información, pero también ha generado retos jurídicos vinculados con la protección de derechos fundamentales, la responsabilidad civil y administrativa, y la ética profesional en entornos digitales. La deontología tecnológica, aunque respaldada por códigos de buenas prácticas como los establecidos por la Association for Computing Machinery (ACM, 2018) y el Institute of Electrical and Electronics Engineers (IEEE Global Initiative, 2019), resulta insuficiente sin un soporte legal que garantice su cumplimiento y que permita prevenir vulneraciones derivadas del uso indebido o irresponsable de tecnologías avanzadas. La rapidez con la que evolucionan los ecosistemas digitales supera con frecuencia la actualización de estos lineamientos, lo que genera vacíos regulatorios que pueden comprometer la privacidad, la igualdad, la no discriminación, la seguridad digital y la libertad de información.

La deontología profesional en el ámbito de las TIC se ha consolidado como un componente esencial para asegurar que el desarrollo y uso de estas herramientas se articulen conforme a principios éticos, jurídicos y sociales. En un entorno de creciente complejidad tecnológica, la deontología establece los deberes, valores y normas que orientan la conducta de los profesionales, con el propósito de garantizar la competencia técnica y la protección de derechos vinculados con la privacidad, la seguridad, la equidad

y el bienestar social. Las universidades han incorporado contenidos de ética, legislación informática y responsabilidad social en los planes de estudio, impulsando la formación de profesionales capaces de equilibrar innovación y valores humanos (Jiménez, 2024).

A nivel internacional, los códigos deontológicos de la ACM y del IEEE funcionan como marcos orientadores en situaciones donde la integridad, la transparencia, la justicia y la protección de datos deben prevalecer sobre intereses corporativos o presiones tecnológicas, aunque sus limitaciones exigen complementar estos instrumentos con una sólida cultura de ética digital y regulaciones que garanticen su observancia (Mittelstadt et al., 2016; Jobin et al., 2019). Este componente ético se extiende a roles especializados —como desarrolladores, analistas de datos, administradores de redes y expertos en ciberseguridad— que enfrentan dilemas cotidianos relacionados con la calidad del software, el manejo responsable de datos y la transparencia algorítmica. A ello se suma el enfoque de Responsabilidad Social Corporativa (RSC), que impulsa prácticas empresariales centradas en la sostenibilidad, la gobernanza tecnológica responsable y el manejo ético de datos e inteligencia artificial.

Desde el plano jurídico, los códigos deontológicos adquieren fuerza a través de la potestad de autorregulación conferida por el Estado a colegios y asociaciones profesionales, convirtiéndose en instrumentos obligatorios que pueden acarrear sanciones en caso de incumplimiento. Aunque contribuyen a prevenir malas prácticas, también presentan limitaciones, especialmente frente a desafíos emergentes como sesgos algorítmicos, vigilancia digital, recopilación excesiva de datos personales y falta de transparencia en sistemas basados en inteligencia artificial (Wachter et al., 2017; Veale & Zuiderveen Borgesius, 2021) y fortalecer la confianza pública, también pueden presentar desventajas, como rigidez normativa, complejidad en su diseño y dificultades para abordar situaciones éticamente ambiguas. En esencia, la deontología profesional en las TIC busca armonizar principios éticos, jurídicos y organizacionales para asegurar que el desarrollo tecnológico permanezca alineado con los valores de justicia, seguridad y bienestar social.

Las tecnologías emergentes (como la inteligencia artificial, el *Big Data*, la realidad virtual/aumentada y los sistemas biométricos) introducen riesgos legales significativos, incluyendo la discriminación algorítmica, la vigilancia masiva, la manipulación digital y la recopilación excesiva de datos sensibles. Estas problemáticas han motivado la actualización de legislaciones nacionales para regular aspectos esenciales de la vida digital, incluyendo la protección de datos personales. Entre estas normativas se encuentran el Reglamento General de Protección de Datos de la Unión Europea (European Union, 2016), la Ley Orgánica española (España, 2018), la Ley Federal mexicana (México, 2022) y la Ley panameña (Panamá, 2019).

Paralelamente, iniciativas regulatorias como el *Artificial Intelligence Act* (European Commission, 2021; Council of the European Union & European Parliament, 2024; European Parliament, 2023) han marcado tendencias globales. Todas estas normativas buscan fortalecer la gobernanza tecnológica y la supervisión de sistemas automatizados, lo cual demanda estrategias jurídicas eficaces que integren

principios constitucionales y estándares internacionales. Sin embargo, persiste una brecha entre la formulación normativa y su implementación efectiva, fenómeno que limita el alcance de estos marcos regulatorios para abordar dilemas éticos emergentes.

Frente a este escenario, surge la necesidad de analizar de manera sistemática cómo distintas regiones y sectores han articulado estrategias jurídicas para garantizar el cumplimiento de normas éticas y deontológicas en el uso de las TIC. Aunque la literatura científica y los documentos normativos producidos en la última década son abundantes, aún falta un estudio integrador que sintetice tendencias, identifique puntos de convergencia y describa, desde una perspectiva comparada, las estrategias jurídicas que han demostrado mayor coherencia y efectividad. Estudios recientes, como los de Dulima Zabala y Gómez Macfarland (2024), Floridi et al. (2018) o Flor-Unda et al. (2023), han aportado evidencia relevante, pero aún no existe una síntesis integradora de tendencias y convergencias normativas entre 2015 y 2025. Esta carencia limita la capacidad de legisladores, investigadores y organizaciones institucionales para comprender los enfoques regulatorios predominantes, evaluar su pertinencia y reconocer áreas donde persisten vacíos conceptuales o deficiencias de implementación.

Con base en lo anterior, la investigación se orienta por preguntas clave: cuáles son las estrategias jurídicas más utilizadas a nivel nacional e internacional para promover la aplicación de normas éticas y deontológicas en el uso de las TIC; qué tendencias o enfoques comunes se observan en documentos académicos y normativos generados entre 2015 y 2025; qué desafíos permanecen en la ejecución de estas estrategias; y en qué medida las políticas y regulaciones analizadas responden a los retos derivados de la acelerada transformación digital. Estas interrogantes permiten abordar el fenómeno desde una perspectiva comparativa y global, orientando el análisis hacia los aspectos más críticos de la gobernanza tecnológica contemporánea.

El objetivo general de este estudio es analizar, mediante una revisión sistemática, las estrategias jurídicas implementadas para garantizar la aplicación de normas éticas y deontológicas en el uso de las TIC entre 2015 y 2025. Para ello, se busca identificar y clasificar documentos científicos, legislaciones y lineamientos institucionales sobre regulación ética y deontológica; describir las estrategias jurídicas predominantes; analizar tendencias, coincidencias y diferencias en su implementación; evaluar desafíos y oportunidades; y organizar los hallazgos mediante tablas comparativas que permitan visualizar la frecuencia y relevancia de cada estrategia.

Este estudio se sustenta en un marco teórico que integra la ética digital, la deontología profesional, la regulación jurídica de las TIC, la gobernanza digital y los desafíos emergentes vinculados con tecnologías avanzadas, todo ello en coherencia con estándares internacionales como los establecidos por UNESCO (2021, 2024), la OCDE (2019; OECD, 2023) y la Unión Europea (European Union, 2016). La ética y la deontología proporcionan los principios que orientan conductas responsables; el marco jurídico define límites y garantías esenciales para la convivencia digital; la gobernanza digital aporta modelos regulatorios y políticas públicas promovidas por organismos internacionales; y los desafíos emergentes,

como sesgos algorítmicos, vigilancia digital, vulnerabilidades sistémicas y falta de transparencia en aplicaciones basadas en inteligencia artificial, permiten contextualizar los riesgos que justifican la necesidad de fortalecer las estrategias jurídicas existentes.

En conjunto, estos elementos construyen una introducción sólida que justifica la pertinencia de la revisión sistemática, delimita el problema de estudio, establece los objetivos y ofrece el andamiaje conceptual necesario para interpretar los resultados que se desarrollarán en las siguientes secciones del artículo.

Materiales y métodos

El estudio se desarrolló mediante una revisión sistemática de carácter descriptivo orientada a identificar, analizar y sintetizar las estrategias jurídicas utilizadas para la aplicación de normas éticas y deontológicas en el uso de las Tecnologías de Información y Comunicación (TIC). Este enfoque permitió reunir información procedente de diversas fuentes doctrinales, normativas y académicas, compararlas e interpretar sus coincidencias y divergencias con el fin de ofrecer una visión integral y actualizada de las respuestas jurídicas frente a los retos éticos del entorno digital. Se adoptó un procedimiento estructurado que garantizó exhaustividad y transparencia en la búsqueda, selección y análisis de los documentos.

La recopilación del corpus documental se realizó entre enero y diciembre de 2025, mediante búsquedas en Scielo, RedALyC, Dialnet, Google Scholar y plataformas editoriales como Springer y Elsevier, limitando la selección a textos de acceso abierto publicados entre 2015 y 2025. Se incluyeron documentos en español e inglés para integrar perspectivas regionales e internacionales, así como lineamientos de organismos multilaterales como UNESCO (2021, 2024), la ONU (United Nations, 2020), la OCDE (2019; OECD, 2023) y la Unión Europea (European Union, 2016; European Commission, 2021).

Los criterios de inclusión abarcaron artículos científicos, legislaciones nacionales (España, 2018; México, 2022; Panamá, 2019), reglamentos, políticas públicas, lineamientos institucionales y documentos internacionales vinculados con regulación ética, deontología tecnológica, gobernanza digital, protección de datos, ciberseguridad y supervisión jurídica del uso de las TIC. Se excluyeron documentos duplicados, estudios centrados exclusivamente en aspectos técnicos sin dimensión ética o jurídica y materiales cuya disponibilidad impidiera la verificación de la información.

Las búsquedas emplearon combinaciones de palabras clave en español e inglés relacionadas con ética digital, deontología, legislación tecnológica, protección de datos y gobernanza algorítmica. Una vez reunido el corpus, se realizó una clasificación y codificación temática que permitió organizar la información según su naturaleza, región, enfoque normativo y estrategias jurídicas identificadas. Esta organización facilitó la elaboración de tablas porcentuales para cuantificar la frecuencia de estrategias tales como actualización legislativa, adopción de códigos de conducta (ACM, 2018; IEEE Global Initiative, 2019), mecanismos de supervisión, regulación de inteligencia artificial (European Commission,

2021; Council of the European Union & European Parliament, 2024; European Parliament, 2023), formación ética y lineamientos de transparencia algorítmica (Garrido et al., 2021; Wachter et al., 2017).

Una vez reunido el corpus documental, se aplicó un proceso de clasificación y codificación que permitió organizar la información según su naturaleza, país o región de procedencia, enfoque normativo, temática principal y estrategias jurídicas descritas. Esta clasificación se registró en matrices de análisis que facilitaron la identificación de patrones de recurrencia, coincidencias conceptuales y diferencias regulatorias. Posteriormente, se elaboraron tablas porcentuales para cuantificar la frecuencia con la que aparecían estrategias tales como la actualización legislativa, la adopción de códigos de conducta, el fortalecimiento de mecanismos de supervisión, la regulación de la inteligencia artificial, la instauración de programas de formación ética y el establecimiento de lineamientos de transparencia para el uso de datos y algoritmos. Los porcentajes y tendencias derivados de este proceso se basaron en el análisis comparativo de 24 fuentes verificadas del periodo 2015–2025, seleccionadas por su rigor académico, pertinencia y confiabilidad institucional, asegurando la validez de los patrones identificados.

El análisis de los datos se realizó mediante una síntesis narrativa que articuló los hallazgos documentales con los ejes del marco teórico, lo que permitió valorar la correspondencia entre los principios éticos, los marcos normativos y las políticas tecnológicas identificadas. Este procedimiento posibilitó una interpretación crítica del estado actual de la regulación ética de las TIC y de las tendencias emergentes que caracterizan la gobernanza digital contemporánea. Como limitación principal, se reconoce que la consulta se centró exclusivamente en documentos de acceso abierto, lo que pudo restringir la inclusión de informes técnicos especializados disponibles únicamente en repositorios cerrados.

En conjunto, la metodología empleada proporcionó un proceso sistemático, reproducible y orientado a ofrecer claridad sobre las estrategias jurídicas que predominan en el ámbito internacional para sustentar la aplicación de normas éticas y deontológicas en el uso de las tecnologías digitales.

Resultados

Los resultados de la revisión sistemática muestran que las estrategias jurídicas más utilizadas para promover la ética y la deontología digital se concentran en cuatro líneas principales: la actualización de marcos legales, la adopción institucional de códigos de conducta específicos para el uso de tecnologías, el fortalecimiento de mecanismos de supervisión y auditoría —especialmente en el ámbito algorítmico— y la incorporación de programas de formación ética orientados al uso responsable de las TIC. En los documentos revisados se observa una tendencia ascendente hacia regulaciones enfocadas en la privacidad de datos, la transparencia algorítmica y la ciberseguridad, lo que evidencia la urgencia de respuestas normativas frente a un ecosistema digital cada vez más complejo.

El análisis revela que estas estrategias se fundamentan en el concepto de Responsabilidad Digital, entendida como el uso seguro, ético y consciente de la tecnología, basado en la protección de datos

personales, el respeto a la privacidad y el cumplimiento de la propiedad intelectual. La ausencia de esta responsabilidad puede derivar en filtraciones de información, vulnerabilidades digitales, daños reputacionales y pérdida de confianza institucional. Este marco se articula con la noción de Ciudadanía Global, que promueve un uso tecnológico orientado al bien común, la defensa de los derechos humanos en línea y la construcción de sociedades más justas. La Ciudadanía Digital integra estos elementos al establecer los derechos —como la privacidad, la seguridad y la libertad de expresión— y los deberes —como el respeto, la protección de la información y la prohibición del plagio— que deben guiar el comportamiento en entornos virtuales, con especial énfasis en la gestión de la identidad y la reputación digital.

En relación con las tecnologías emergentes, los hallazgos muestran que persisten riesgos éticos significativos. En el caso del Big Data, se identifican amenazas vinculadas a la vigilancia masiva, la ausencia de consentimiento informado, la elaboración de perfiles y la discriminación algorítmica, particularmente en sectores como la educación. La inteligencia artificial presenta desafíos adicionales debido a la opacidad de determinados modelos, la toma de decisiones automatizadas sin suficiente supervisión humana y el potencial sesgo inherente a los algoritmos. También se detectan riesgos en el uso de tecnologías inmersivas, como la realidad virtual y la aumentada, las cuales recopilan datos biométricos altamente sensibles —entre ellos movimientos oculares y ritmo cardíaco— susceptibles de manipular la conducta y comprometer la integridad cognitiva. Estas problemáticas demandan con urgencia marcos legales especializados y protocolos avanzados de protección de datos.

Los hallazgos cuantitativos de la revisión se sintetizan en siete tablas que caracterizan el panorama regulatorio internacional. La Tabla 1 evidencia que América Latina y los organismos internacionales concentran la mayor parte de los documentos encontrados (37.5 % cada uno), mientras que la Unión Europea, aunque representa solo el 25 %, aporta normativas altamente influyentes como el RGPD y el AI Act.

Tabla 1

Distribución geográfica de las normativas y documentos éticos encontrados

Región / Tipo de organismo	Frecuencia	Porcentaje (%)
Unión Europea	2	25 %
América Latina	3	37.5 %
Organismos Internacionales (ONU, UNESCO, OCDE)	3	37.5 %

Fuente. Elaboración propia.

Se evidencia que América Latina y los organismos internacionales presentan una proporción equivalente en términos de documentos relevantes, mientras que la Unión Europea aporta normativas altamente influyentes, aunque menos numerosas. La tabla 2 clasifica los documentos revisados según su naturaleza jurídica. La legislación sobre protección de datos constituye la categoría predominante (37.5 %), lo que confirma el papel central de la privacidad en la regulación tecnológica.

Tabla 2*Tipología de documentos jurídicos y éticos identificados*

Tipo de documento	Frecuencia	Porcentaje (%)
Legislación sobre protección de datos	3	37.5 %
Marcos regulatorios sobre IA	2	25 %
Códigos de ética profesionales	1	12.5 %
Documentos éticos internacionales (orientaciones)	2	25 %

Fuente. Elaboración propia.

Los documentos sobre protección de datos conforman la categoría predominante, lo que confirma que este ámbito es el eje más consolidado de regulación ética y jurídica en torno a las TIC. Los principios éticos más recurrentes se sintetizan en la tabla 3. El principio de protección de datos y privacidad aparece en el 62.5 % de los documentos, seguido por transparencia, responsabilidad y no discriminación.

Tabla 3*Principios éticos recurrentes en las normativas revisadas*

Principio ético identificado	Documentos que lo incluyen	Porcentaje (%)
Protección de datos y privacidad	5	62.5 %
Transparencia	4	50 %
Responsabilidad y rendición de cuentas	4	50 %
No discriminación y equidad	3	37.5 %
Seguridad y mitigación de riesgos	3	37.5 %

Fuente. Análisis comparativo de las fuentes verificadas.

La prevalencia de la privacidad y la transparencia demuestra una fuerte orientación preventiva frente al uso de TIC, especialmente en ámbitos asociados al tratamiento automatizado de datos. La tabla 4 expone los ámbitos donde estas normativas tienen mayor presencia. La protección de datos personales en entornos digitales aparece como el sector más regulado (62.5 %), seguido por la inteligencia artificial (50 %).

Tabla 4*Ámbitos de aplicación más frecuentes y sectores regulados por las normas analizadas*

Ámbito de aplicación	Frecuencia	Porcentaje (%)
Protección de datos personales en entornos digitales	5	62.5 %
Inteligencia artificial aplicada	4	50 %
Servicios públicos y gobierno digital	3	37.5 %
Educación y uso académico de TIC	2	25 %
Comercio electrónico	2	25 %

Fuente. Elaboración propia.

El sector más cubierto es el de protección de datos, seguido de la inteligencia artificial, demostrando la relevancia de ambos campos en la formulación de marcos éticos y jurídicos actuales. Estos resultados muestran que la estrategia predominante consiste en la actualización de marcos legales con el fin de alinearlos a los desafíos tecnológicos contemporáneos. Muchas de estas reformas toman como referencia modelos europeos, incorporando principios de transparencia, explicabilidad y mitigación de sesgos en las regulaciones sobre inteligencia artificial. Paralelamente, se ha fortalecido el reconocimiento de derechos digitales como la portabilidad de datos, el acceso a información transparente y la neutralidad tecnológica. Otra tendencia relevante es la incorporación de códigos de conducta institucionales con fuerza vinculante, lo que permite a organizaciones y centros educativos normar el uso de datos y sistemas automatizados mediante reglamentos internos.

El fortalecimiento de las capacidades institucionales también es una estrategia común. Entre los organismos más citados destacan las autoridades de protección de datos, los comités de auditoría algorítmica y las unidades de ética digital, encargadas de supervisar el cumplimiento normativo y gestionar los riesgos tecnológicos. A ello se suma la creciente inclusión de programas de formación jurídica y ética dirigidos a fortalecer el cumplimiento normativo, especialmente en ámbitos académicos y profesionales donde el uso intensivo de datos requiere competencias claras sobre privacidad y transparencia. Las políticas de transparencia y privacidad también adquieren un papel central, expresadas en la exigencia del consentimiento informado reforzado, la regulación de datos biométricos y la implementación de evaluaciones de impacto algorítmico.

La tabla 5 resume las estrategias jurídicas identificadas en los documentos analizados. La regulación obligatoria aparece como la estrategia más frecuente (62.5 %), seguida por mecanismos de supervisión y auditoría (50 %), lo cual refleja un enfoque normativo que combina obligatoriedad y vigilancia permanente.

Tabla 5

Estrategias jurídicas predominantes identificadas para garantizar el uso ético de TIC

Estrategia jurídica	Frecuencia	Porcentaje (%)
Regulaciones obligatorias (leyes, reglamentos)	5	62.5 %
Mecanismos de supervisión y auditoría	4	50 %
Sanciones administrativas	3	37.5 %
Guías y recomendaciones éticas no vinculantes	3	37.5 %
Principios para diseño responsable (IA y TIC)	2	25 %

Fuente. Elaboración propia con base en la comparación normativa internacional.

En cuanto a los riesgos jurídicos, los documentos revisados muestran preocupación por fenómenos como los *deepfakes*, que representan amenazas tanto para la integridad de la información como para la seguridad financiera y política. Casos recientes, como el fraude de 25 millones de dólares en Hong Kong mediante el uso de videos generados por inteligencia artificial, evidencian la urgencia de mecanismos robustos de autenticación, detección automatizada y marcas digitales de verificación.

Antes de presentar la siguiente tabla, es importante destacar que las estrategias jurídicas identificadas en la revisión sistemática revelan un patrón global orientado a fortalecer la protección de derechos fundamentales ante el avance acelerado de las tecnologías digitales. Estas estrategias se centran principalmente en actualizar marcos legales, institucionalizar la supervisión digital, reforzar códigos de conducta y promover la formación ética. La tabla 6 resume las cinco categorías más representativas encontradas en las fuentes analizadas.

Tabla 6

Estrategias jurídicas predominantes para promover la ética en el entorno digital

Estrategia jurídica identificada	Descripción sintética	Frecuencia
Actualización legislativa en protección de datos y derechos digitales	Reformas inspiradas en el RGPD, leyes de privacidad, normas sobre transparencia algorítmica	Alta
Códigos de conducta y lineamientos institucionales	Instrumentos internos que orientan el uso responsable de TIC en organizaciones y centros educativos	Media
Creación de organismos de supervisión tecnológica	Autoridades de datos, comités de ética digital y unidades de auditoría algorítmica	Media-Alta
Formación jurídica y ética en ciudadanía digital	Programas formativos sobre derechos, deberes, privacidad, transparencia y uso responsable	Media
Políticas de transparencia, consentimiento y protección biométrica	Regulación de datos sensibles, evaluaciones de impacto y consentimiento informado reforzado	Alta

Fuente. Elaboración propia.

Se muestra que las estrategias más consolidadas se concentran en la protección de datos personales y en la supervisión del uso de tecnologías avanzadas, especialmente aquellas vinculadas con la inteligencia artificial. Este énfasis responde a la necesidad de garantizar la transparencia y la no discriminación en sistemas automatizados. También se observa una tendencia creciente a institucionalizar prácticas éticas mediante códigos internos y programas de formación, lo que demuestra que la regulación jurídica se complementa con mecanismos de autorregulación y educación digital.

Conviene señalar que el ecosistema digital actual no solo enfrenta desafíos normativos, sino también riesgos complejos derivados del Big Data, la inteligencia artificial, las tecnologías inmersivas y el uso de datos biométricos. Estos riesgos afectan derechos fundamentales como la privacidad, la igualdad, la reputación y la autonomía personal. La tabla 7 clasifica los riesgos éticos y jurídicos más recurrentes detectados en la revisión.

Tabla 7*Principales riesgos éticos y jurídicos asociados a tecnologías emergentes*

Tecnología o ámbito	Tipo de riesgo identificado	Impacto jurídico-potencial	Frecuencia
Big Data y vigilancia digital	Pérdida de anonimato, perfiles invasivos, vigilancia masiva	Vulneración de privacidad y derechos civiles	Alta
Inteligencia artificial	Sesgo algorítmico, falta de explicabilidad, decisiones automatizadas	Discriminación, desigualdad y responsabilidad difusa	Alta
Realidad virtual y aumentada	Recolección de datos biométricos, manipulación cognitiva	Riesgos para integridad cognitiva y datos sensibles	Media
Deepfakes y manipulación digital	Falsificación audiovisual, desinformación, fraude	Afectación a la honra, seguridad jurídica y derechos penales	Media-Alta
Reconocimiento facial y biometría	Identificación involuntaria, falta de consentimiento	Amenazas a libertades civiles y derecho a la intimidad	Alta

Fuente. Elaboración propia.

Se deja en evidencia que los riesgos más críticos se concentran en áreas donde el tratamiento automatizado de datos afecta de manera directa derechos fundamentales. Big Data, inteligencia artificial y tecnologías biométricas representan los escenarios de mayor preocupación global, debido a la combinación de opacidad técnica y capacidad para tomar decisiones de alto impacto. Adicionalmente, fenómenos como los deepfakes generan nuevos desafíos penales y de seguridad, destacándose la necesidad de mecanismos avanzados de autenticación y detección automática.

Finalmente, en el ámbito educativo se identifican riesgos particulares derivados de la implementación acelerada de plataformas digitales y sistemas algorítmicos de evaluación y analítica del aprendizaje. Entre los problemas más señalados se encuentran la recopilación excesiva de datos estudiantiles, la discriminación derivada de modelos predictivos y la falta de transparencia sobre los algoritmos que gestionan procesos pedagógicos y administrativos. Aunque algunas instituciones han comenzado a generar políticas internas, persiste la necesidad de marcos legales específicos, supervisión externa y estándares comunes para garantizar la protección de los estudiantes y la equidad en los procesos formativos.

En conjunto, los resultados muestran un panorama regulatorio robusto, caracterizado por la consolidación de principios éticos como privacidad, transparencia y responsabilidad, y por la creciente influencia de organismos internacionales y modelos regulatorios de referencia como los desarrollados en Europa. El análisis evidencia también riesgos significativos asociados a las tecnologías emergentes, los cuales requieren estrategias jurídicas cada vez más especializadas y mecanismos de supervisión adaptados al ritmo del cambio tecnológico.

Paralelamente, el entorno digital exige una respuesta jurídica multifacética que combine regulación estricta, supervisión institucional, educación ética y tecnologías de seguridad avanzada. Mientras que se destaca estrategias orientadas a prevenir y gestionar riesgos mediante marcos regulatorios y formación, subrayando las amenazas reales derivadas de tecnologías emergentes que pueden comprometer derechos fundamentales. Estos hallazgos confirman la necesidad urgente de reforzar la gobernanza tecnológica, especialmente frente a la inteligencia artificial, los datos biométricos y la manipulación digital, consolidando un ecosistema digital seguro, transparente y respetuoso de la dignidad humana.

Discusión

Los hallazgos de esta revisión evidencian que la regulación ética y jurídica del uso de las Tecnologías de Información y Comunicación se encuentra en una fase de consolidación global, aunque avanza a ritmos diferenciados según las regiones y los niveles institucionales. La distribución geográfica de los documentos muestra que América Latina y los organismos internacionales constituyen las fuentes más prolíficas, mientras que la Unión Europea, aunque menos representada en volumen, continúa liderando la producción de marcos regulatorios tecnológicamente avanzados, como el Reglamento General de Protección de Datos y el reciente AI Act. Este fenómeno sugiere que el liderazgo jurídico no depende de la cantidad de instrumentos, sino de su alcance, rigor conceptual y capacidad de convertirse en estándares de referencia internacional.

La predominancia de leyes de protección de datos como tipo documental más frecuente confirma que la privacidad sigue siendo el eje articulador de la ética digital contemporánea. Este énfasis responde al crecimiento exponencial del flujo informativo, al uso intensivo de plataformas digitales y al avance de sistemas basados en el procesamiento automatizado de datos. Sin embargo, la presencia creciente de marcos regulatorios orientados específicamente a la inteligencia artificial revela un desplazamiento hacia un escenario más complejo, en el cual la protección de datos se articula con otros principios como la transparencia algorítmica, la mitigación de sesgos y la responsabilidad jurídica frente a decisiones computacionales de alto impacto. Los resultados indican una tendencia progresiva hacia normativas más amplias que buscan abarcar no solo la privacidad, sino también dimensiones éticas vinculadas a la equidad, la explicabilidad y la supervisión del comportamiento automatizado.

La coincidencia entre regiones respecto a principios éticos fundamentales permite identificar un movimiento hacia la estandarización global de valores mínimos para la gobernanza digital, una tendencia ampliamente reconocida en investigaciones comparativas sobre marcos éticos internacionales (Jobin et al., 2019). La privacidad, la transparencia y la responsabilidad emergen como principios transversales presentes en marcos nacionales e internacionales, lo que demuestra un consenso inicial sobre los límites éticos de la tecnología contemporánea. No obstante, la menor presencia relativa de principios asociados a la no discriminación y a la equidad revela un desafío pendiente: el fortalecimiento de marcos normativos que aborden explícitamente los riesgos sociales derivados de algoritmos entrenados en contextos con desigualdades estructurales. La persistencia de sesgos algorítmicos y discriminación automatizada,

ampliamente documentada en la literatura, refuerza la necesidad de instrumentos vinculantes que garanticen equidad y trato justo (Mittelstadt et al., 2016).

El análisis de los ámbitos de aplicación confirma que la regulación ética se ha concentrado principalmente en los entornos digitales generales y en tecnologías de inteligencia artificial. Esto coincide con el acelerado desarrollo de sistemas automatizados en sectores como gobierno digital, comercio electrónico y educación. La presencia de marcos regulatorios aplicados al ámbito educativo, aunque reducida, es significativa porque señala un reconocimiento emergente del impacto de las TIC y la IA en procesos formativos. La revisión evidencia la necesidad de orientar políticas específicas que aborden el tratamiento de datos estudiantiles, la analítica del aprendizaje y los riesgos de decisiones automatizadas en contextos pedagógicos.

Los resultados también muestran que las estrategias jurídicas predominantes combinan regulaciones obligatorias con mecanismos de supervisión institucional. Esto indica un enfoque que privilegia la exigibilidad, la responsabilidad y el control, elementos indispensables para limitar prácticas tecnológicas que puedan vulnerar derechos fundamentales. Sin embargo, la coexistencia de instrumentos no vinculantes, como lineamientos éticos o recomendaciones internacionales, revela que los Estados y organismos multilaterales buscan equilibrar la flexibilidad adaptativa con la coerción legal. Esta dualidad responde a una realidad estructural: la tecnología avanza más rápido que los ciclos legislativos, por lo que los marcos orientativos funcionan como herramientas temporales que permiten guiar el desarrollo tecnológico mientras se consolidan regulaciones más robustas.

En este contexto, la relación entre ética, derecho y tecnologías emergentes se vuelve central. El derecho tiene la función de traducir principios éticos en mecanismos vinculantes, verificables y exigibles, capaces de proteger derechos aun cuando los sistemas tecnológicos operen con niveles crecientes de autonomía y complejidad. Para ello, la normativa debe ser flexible, actualizable y diseñada para anticipar riesgos derivados de aplicaciones innovadoras. Esta exigencia es especialmente relevante en ámbitos donde las decisiones automatizadas pueden tener consecuencias significativas sobre la vida social, laboral, financiera o educativa de las personas.

De forma complementaria, la construcción de estrategias jurídicas integrales se fundamenta en la articulación de leyes coherentes con estándares internacionales, mecanismos sancionadores efectivos, auditorías tecnológicas y programas de formación continua en derecho digital. Un sistema jurídico que aspire a regular tecnologías emergentes debe incorporar prácticas como la auditoría algorítmica, que permite identificar sesgos, validar la transparencia de los procesos automatizados y garantizar que las decisiones informadas por inteligencia artificial respeten criterios de equidad y justicia.

Asimismo, la promoción de la educación y de la ciudadanía digital se posiciona como una medida preventiva crucial. La alfabetización jurídica y ética facilita que estudiantes, docentes y profesionales comprendan sus derechos digitales, los límites del tratamiento de datos y los riesgos de los sistemas

tecnológicos contemporáneos. El fortalecimiento de la formación ciudadana en temas digitales resulta indispensable para construir sociedades capaces de ejercer un uso crítico, informado y seguro de las tecnologías.

Los desafíos futuros identificados en la revisión exigen particular atención. Entre ellos destacan los riesgos asociados a los deepfakes, la autonomía creciente de sistemas de inteligencia artificial, el impacto laboral de la automatización y la persistente brecha digital que limita el acceso equitativo a los beneficios tecnológicos. La complejidad de estos retos evidencia que la gobernanza tecnológica debe ser anticipatoria, precisa y multidisciplinaria, articulando perspectivas éticas, jurídicas, técnicas y educativas.

Finalmente, las tendencias regulatorias recientes muestran un avance hacia marcos jurídicos más integrales, que incluyen normas sobre gobernanza de datos, responsabilidad algorítmica y auditorías obligatorias, junto con políticas emergentes relacionadas con la sostenibilidad digital y la certificación ética de sistemas tecnológicos. Estos esfuerzos reflejan una preocupación creciente por equilibrar la innovación con la defensa de la dignidad humana, la justicia social y la equidad. En conjunto, la discusión sugiere que, aunque el ecosistema jurídico-ético se encuentra en expansión y presenta un avance significativo hacia la armonización global, persisten desafíos relacionados con la actualización permanente de marcos legales, la consolidación de principios amplios de justicia digital y el fortalecimiento institucional necesario para implementar mecanismos de supervisión efectivos. Asimismo, se identifica la necesidad de investigaciones futuras que evalúen el cumplimiento real de estas normativas y su impacto sobre las prácticas tecnológicas emergentes, particularmente en regiones en desarrollo donde las vulnerabilidades son más agudas.

Conclusiones

La revisión sistemática desarrollada permitió identificar un conjunto significativo de estrategias jurídicas y orientaciones éticas destinadas a regular el uso de las Tecnologías de Información y Comunicación en distintos contextos y regiones. Los hallazgos confirman que, a pesar de la diversidad de enfoques normativos existentes, los instrumentos tienden a converger en principios fundamentales como la protección de datos, la transparencia, la responsabilidad y la rendición de cuentas. Estos principios, presentes tanto en marcos internacionales como en legislaciones nacionales, se erigen como pilares esenciales para garantizar un uso ético y socialmente responsable de las tecnologías digitales.

El estudio evidencia que las estrategias jurídicas constituyen un componente indispensable para asegurar la aplicación efectiva de normas éticas y deontológicas en el ámbito tecnológico. Los marcos regulatorios deben ser integrales, coherentes y dinámicos, de modo que puedan responder a los retos emergentes de un ecosistema digital en constante transformación. La protección de la dignidad humana, la justicia, la transparencia algorítmica y los derechos digitales se consolidan, así, como elementos esenciales para garantizar entornos tecnológicos seguros, responsables y alineados con los principios del Estado de Derecho.

Los resultados también muestran el papel estratégico que desempeñan los organismos internacionales en la consolidación de estándares globales, al articular recomendaciones que, aunque no siempre vinculantes, orientan decisivamente el desarrollo de políticas públicas. La Unión Europea destaca en este ámbito por la profundidad, rigurosidad y alcance de sus normativas, influyendo en la formulación de marcos similares en otras regiones, especialmente en América Latina. Paralelamente, la expansión de regulaciones vinculadas a la inteligencia artificial revela una ampliación de la agenda ética más allá de la protección de datos personales. Esta tendencia responde al reconocimiento de nuevos riesgos, entre ellos los sesgos algorítmicos, la opacidad de los sistemas automatizados y las desigualdades que pueden derivarse de la distribución inequitativa de sus beneficios.

La integración de normas éticas y deontológicas en el uso de tecnologías digitales requiere estrategias jurídicas robustas, flexibles y orientadas a la protección de los derechos fundamentales. La actualización permanente de leyes, el fortalecimiento de instituciones de supervisión, la adopción de códigos de conducta vinculantes, la formación jurídica continua y la implementación de mecanismos de transparencia tecnológica constituyen pilares esenciales para la construcción de un entorno digital seguro, justo y responsable. No obstante, persisten desafíos significativos, como el fortalecimiento de los mecanismos de supervisión institucional, la mejora en la capacidad de implementación normativa y la necesidad de ampliar los marcos éticos hacia principios que integren la equidad, la justicia digital y la protección de grupos vulnerables. Igualmente, se observa una brecha entre la producción normativa y su aplicación práctica, lo que exige estudios futuros orientados a evaluar el impacto real de estas regulaciones en contextos tecnológicos dinámicos.

En síntesis, la revisión confirma que las estrategias jurídicas y éticas para el uso de las TIC se encuentran en un proceso de consolidación y expansión. Su evolución dependerá de la capacidad de los Estados, instituciones y organismos internacionales para mantener enfoques actualizados, inclusivos y coherentes ante las transformaciones aceleradas de la innovación digital contemporánea. La aplicación eficaz de normas éticas en el ámbito tecnológico exige marcos normativos que aborden las áreas de mayor riesgo social, como la privacidad de los datos biométricos en entornos de realidad virtual y aumentada, la mitigación de sesgos algorítmicos en sistemas de inteligencia artificial y Big Data, y la ciberseguridad frente a amenazas avanzadas como los *deepfakes* (Flor-Unda et al., 2023). La deontología profesional en las TIC debe reforzarse mediante prácticas de responsabilidad social corporativa y un modelo de ciudadanía digital global que promueva la justicia social, el respeto y la defensa de los derechos humanos en el ciberespacio. En este proceso, universidades y centros educativos desempeñan un papel crucial al fomentar la formación ética y la actualización normativa que asegure que el desarrollo tecnológico avance bajo principios de equidad, seguridad y bienestar social.

A partir de los hallazgos obtenidos, se recomienda impulsar procesos de armonización normativa regional que faciliten la coherencia regulatoria y el intercambio de buenas prácticas; fortalecer las capacidades institucionales mediante programas permanentes de formación en ética digital y auditoría tecnológica; desarrollar marcos jurídicos específicos para el uso responsable de la inteligencia artificial

en sectores como educación, salud y servicios públicos; e incentivar investigaciones aplicadas que permitan evaluar la eficacia de los marcos legales existentes, particularmente en contextos de países en desarrollo. Asimismo, se sugiere integrar de manera explícita principios de equidad, justicia social y protección de grupos vulnerables en las regulaciones sobre tecnologías digitales, con el fin de asegurar que su implementación contribuya a un desarrollo tecnológico ético, inclusivo y sostenible.

Referencias

- Association for Computing Machinery (ACM). (2018). *ACM Code of Ethics and Professional Conduct* (revised 2018). ACM. <https://www.acm.org/code-of-ethics>
- Comisión Europea. (2023). Comisión celebra el acuerdo político sobre el Acta de IA [Comunicado de prensa]. European Commission Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473
- Council of the European Union & European Parliament. (2024). *Proposal and consolidated drafts for the Artificial Intelligence Act* (Final Draft 21 January 2024). <https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AIA-Final-Draft-21-January-2024.pdf>
- Dulima Zabala Leal, T., & Gómez Macfarland, C. A. (2024). La responsabilidad civil y la ética en la inteligencia artificial: una revisión sistemática de las ideas del período 2018–2023. *Revista IUSTA*, (60), 66–93. <https://doi.org/10.15332/25005286.9964>
- España. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). *Boletín Oficial del Estado*. <https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf>
- European Commission. (2021). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021)206 final. European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:206:FIN>
- European Parliament. (2023, 6 de diciembre). Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI [Press release]. <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>
- European Union. (2016). Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR). *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Minds & Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America. *Informatics*, 10(3), 71. <https://doi.org/10.3390/informatics10030071>
- Garrido, R., Lapostol, J. P., & Hermosilla, M. P. (2021). *Transparencia algorítmica en el sector público*. GobLab (Universidad Adolfo Ibáñez) y Consejo para la Transparencia. <https://goblab.uai.cl/wp-content/uploads/2021/10/ESTUDIO-TRANSPARENCIA-ALGORITMICA-EN-EL-SECTOR-PUBLICO-GOBLAB-CPLT-final....pdf>
- IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. (2019). *Ethically Aligned Design (EAD), Version II* (for public discussion). IEEE. https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf

- Jiménez, Y. (2024). Deontología en el uso de la inteligencia artificial: hacia un futuro responsable. *Dialógica. Revista Multidisciplinaria*, 21(1), 66–83. <https://doi.org/10.56219/dialgica.v21i1.2935>
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–399. <https://doi.org/10.1038/s42256-019-0088-2>
- México. (2022). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Cámara de Diputados. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2). <https://doi.org/10.1177/2053951716679679>
- OECD. (2019). *Scoping the OECD AI principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)* (OECD Digital Economy Papers No. 291). OECD Publishing. <https://doi.org/10.1787/d62f618a-en>
- Organisation for Economic Co-operation and Development (OECD). (2023). *The state of implementation of the OECD AI Principles: Four years on* (implementación y seguimiento). OECD. <https://oecd.ai/en/consultations/state-of-implementation>
- Panamá. (2019). Ley 81 de 26 de marzo de 2019 — Sobre Protección de Datos Personales. *Gaceta Oficial*. <https://antai.gob.pa/ley-81-de-proteccion-de-datos-personales-entra-en-vigencia-en-panama/>
- UNESCO. (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa
- UNESCO. (2024). *Artificial intelligence and democracy* (Report / regional analysis building on the Recommendation). UNESCO. <https://www.unesco.org/en/articles/artificial-intelligence-and-democracy>
- United Nations. (2020). *Secretary-General's Roadmap for Digital Cooperation* (A/74/821). United Nations. <https://undocs.org/en/A/74/821>
- Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/cr-2021-220402>
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ix005>

Declaración de Autoría

Conceptualización: Ricardo M. Candanedo Yau; **Investigación:** Ricardo M. Candanedo Yau; **Metodología:** Ricardo M. Candanedo Yau; **Redacción – Borrador orogianal:** Ricardo M. Candanedo Yau; **Redacción – revisión y edición:** Ricardo M. Candanedo Yau; **Autor de correspondencia:** Ricardo M. Candanedo Yau.

Conflicto de interés

El autor de este manuscrito certifica que no existen conflictos de interés de ningún tipo, ni financieros ni personales, académicos o políticos, que pudieran haber influido de manera inapropiada en la realización, análisis o interpretación de los resultados de esta investigación.

Información adicional

La correspondencia y las solicitudes de materiales sobre este escrito deben dirigirse al autor de correspondencia al correo electrónico proporcionado, en la afiliación.