La Vigilancia Digital en la Protección de los Derechos Humanos en Colombia

Mayor Martínez Santos Edwin

Artículo para optar al título profesional:

Magister en Derechos Humanos y Derecho Internacional de los Conflictos Armados

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor Martínez Santos Edwin
Identificación	**:**	CC. 91521307
Programa académico	**:**	Maestría
Tutor metodológico	**:**	Dra. Claudia Patricia Garay Acevedo
Tutor temático	**:**	Carlos Arturo Martinez Forero
Fecha de entrega	**:**	26 de Octubre de 2024
Extensión	**:**	Palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-No Comercial-Sin Obras Derivadas.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

La Vigilancia Digital en la Protección de los Derechos Humanos en Colombia.

Digital Surveillance in the Protection of Human Rights in Colombia.

Martínez Santos Edwin [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La vigilancia digital se ha convertido en un tema crucial en el debate sobre derechos humanos, especialmente en el contexto de su implementación por parte de los Estados para fines de seguridad y seguimiento. En Colombia, un país con un pasado conflictivo y una realidad en constante evolución, la adopción de tecnologías de vigilancia enfrenta el desafío de equilibrar la seguridad con la protección de los derechos fundamentales. A pesar de contar con leyes como la Ley 1581 de 2012, que protege datos personales, la legislación vigente no aborda de manera exhaustiva los retos que presentan tecnologías emergentes como el reconocimiento facial y la inteligencia artificial. Este artículo investiga cómo la vigilancia digital impacta la garantía de los derechos humanos en Colombia, explorando tanto sus oportunidades en términos de seguridad y justicia como los

[1] Coronel del Ejército Nacional de Colombia. Candidato a magíster en derechos humanos y DICA, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: Edwin.martinez@esdeg.edu.co

riesgos para la privacidad y otras libertades fundamentales. La metodología empleada es cualitativa, con un enfoque analítico y un diseño no experimental. Se utiliza una revisión normativa y documental para ofrecer una comprensión profunda del fenómeno, integrando diversas fuentes de información para derivar conclusiones ajustadas a la realidad del contexto colombiano. La investigación se realiza mediante un estudio transversal, permitiendo observar y comparar eventos y contextos relevantes, y destaca la necesidad de un marco regulatorio robusto y específico para proteger los derechos humanos mientras se aprovechan las tecnologías de vigilancia.

Palabras clave: Colombia, Derechos, Normatividad, Vigilancia digital.

Abstract: Digital surveillance has become a crucial issue in the human rights debate, especially in the context of its implementation by States for security and monitoring purposes. In Colombia, a country with a conflictive past and a constantly evolving reality, the adoption of surveillance technologies faces the challenge of balancing security with the protection of fundamental rights. Despite having laws such as Law 1581 of 2012, which protects personal data, current legislation does not exhaustively address the challenges presented by emerging technologies such as facial recognition and artificial intelligence. This article investigates how digital surveillance impacts the guarantee of human rights in Colombia, exploring both its opportunities in terms of security and justice and the risks to privacy and other fundamental freedoms. The methodology used is qualitative, with an analytical approach and a non-experimental design. A normative and documentary review is used to offer a deep understanding of the phenomenon, integrating various sources of

information to derive conclusions adjusted to the reality of the Colombian context. The research is carried out through a cross-sectional study, allowing relevant events and contexts to be observed and compared, and highlights the need for a robust and specific regulatory framework to protect human rights while taking advantage of surveillance technologies.

Keywords: Colombia, Rights, Regulations, Digital surveillance.

Introducción

La vigilancia digital se ha transformado en un tema central en el debate global sobre los derechos humanos, especialmente en el contexto de su implementación por parte de los Estados para fines de seguridad y seguimiento; en un mundo cada vez más interconectado y digitalizado, la tecnología ofrece herramientas poderosas que pueden ser utilizadas para monitorear, proteger y, en algunos casos, facilitar la justicia, sin embargo, esta misma tecnología también plantea desafíos significativos en términos de privacidad, libertad de expresión y otros derechos fundamentales. En este contexto, Colombia, como Estado social de derecho, enfrenta un desafío particular: encontrar un equilibrio entre el uso de la vigilancia digital para garantizar la seguridad y la justicia, y la protección de los derechos humanos de sus ciudadanos (Ramió, 2019).

En Colombia, la implementación de tecnologías de vigilancia digital no ha sido un proceso sencillo ni lineal. Las dinámicas sociales y políticas del país, marcadas por un pasado conflictivo y un presente en constante evolución, han dificultado la adopción de un marco normativo claro y efectivo que regule el uso de estas tecnologías; a pesar de que el país cuenta con políticas y regulaciones sobre la protección de datos personales, estas normativas a menudo se quedan cortas frente al rápido avance tecnológico y las posibilidades que este ofrece en términos de vigilancia y control. La ausencia de una regulación robusta y específica sobre la vigilancia digital en el contexto de los derechos humanos deja un vacío legal que puede ser explotado, ya sea por el Estado o por actores privados, con consecuencias potencialmente negativas para la sociedad (Cano, 2023; Cano, 2012; Chaparro-López, 2021).

El desafío radica en que, aunque la tecnología de vigilancia puede aportar significativamente a la seguridad y la justicia, su implementación sin un marco regulatorio claro y sin salvaguardas adecuadas puede llevar a la violación de derechos humanos fundamentales, la vigilancia digital, sin controles y equilibrios adecuados, puede convertirse en una herramienta de opresión, utilizada para suprimir la disidencia, invadir la privacidad y restringir la libertad de expresión. En un Estado social de derecho como Colombia, donde la protección de los derechos humanos es un principio fundamental, es crucial que cualquier avance tecnológico en el ámbito de la vigilancia esté acompañado de una reflexión profunda sobre sus implicaciones éticas y legales (García, 2022; Arroyo, 2023).

El panorama legal en Colombia refleja una cierta ambigüedad en cuanto a la regulación de la vigilancia digital. Existen leyes que protegen la privacidad y los datos personales, como la Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales, y la Constitución Política de Colombia, que garantiza el derecho a la intimidad. Sin embargo, estas leyes no abordan de manera exhaustiva los desafíos específicos que plantea la vigilancia digital, especialmente en lo que respecta al uso de tecnologías emergentes como el reconocimiento facial, los drones y las herramientas de inteligencia artificial; la falta de una legislación específica sobre estos temas deja un vacío que podría ser perjudicial para la garantía de los derechos humanos en el país (Dávila., & Monsalve, 2023).

En este contexto, la implementación de la vigilancia digital en Colombia enfrenta varios obstáculos; primero, la desconfianza generalizada en las instituciones del Estado, resultado de décadas de conflicto armado y corrupción, hace que cualquier intento de expandir la capacidad de vigilancia sea visto con sospecha; segundo, la falta de claridad y coherencia en el marco regulatorio crea incertidumbre tanto para las autoridades encargadas

de implementar estas tecnologías como para los ciudadanos que podrían verse afectados por ellas; tercero, las dinámicas sociales y políticas del país, que a menudo son volátiles e impredecibles, dificultan la creación de un consenso sobre cómo y cuándo se deben utilizar estas tecnologías (Liévano, 2024).

A pesar de estos desafíos, hay un reconocimiento creciente de la necesidad de abordar la cuestión de la vigilancia digital en Colombia; investigaciones recientes y debates académicos han subrayado la importancia de establecer un marco normativo que no solo permita el uso de tecnologías de vigilancia para fines legítimos de seguridad y justicia, sino que también garantice que su implementación respete los derechos humanos y las libertades fundamentales. Este documento busca explorar cómo la vigilancia digital afecta la garantía de los derechos humanos en Colombia, examinando tanto las oportunidades que ofrece en términos de seguridad y justicia, como los riesgos que plantea para la privacidad, la libertad de expresión y otros derechos fundamentales (Dencik, 2024; Buenadicha, et al, 2019).

El presente documento plantea como pregunta central: ¿Cómo afecta la vigilancia digital a la garantía de los derechos humanos en Colombia? Esta cuestión busca explorar si es posible alcanzar un equilibrio entre la necesidad de seguridad y la protección de los derechos humanos en el contexto de la vigilancia digital; la respuesta a esta pregunta es compleja y exige una reflexión profunda sobre el papel del Estado, el poder de la tecnología y los límites que deben establecerse para evitar que el avance tecnológico se convierta en una amenaza para las libertades fundamentales, la discusión sobre la vigilancia digital en Colombia no solo se centra en cuestiones de seguridad, sino que también plantea el tipo de sociedad que deseamos construir: una sociedad en la que la tecnología se utilice para

promover la justicia y la seguridad sin comprometer los derechos humanos que sustentan el Estado social de derecho.

Para abordar esta problemática, el objetivo general de este estudio es analizar cómo la vigilancia digital afecta la garantía de los derechos humanos en Colombia; de manera más específica, se busca identificar las medidas de protección de los derechos humanos en el país, con énfasis en la privacidad en el contexto de la vigilancia digital; describir el alcance de esta vigilancia y su impacto en los derechos fundamentales; y examinar las implicaciones legales y normativas que la vigilancia digital conlleva. Este enfoque permitirá desarrollar una comprensión integral de los desafíos que la vigilancia digital representa para la protección de los derechos humanos en Colombia.

Metodología

Este trabajo de investigación se desarrolla bajo un enfoque cualitativo con un alcance analítico, orientado a reconocer el impacto de las nuevas tecnologías en los procesos de vigilancia y su incidencia en los derechos humanos, a partir de la revisión normativa y documental, se adopta un diseño no experimental que permite realizar un análisis exhaustivo de la información, obteniendo así insumos suficientes para derivar conclusiones ajustadas a la realidad del fenómeno estudiado (Fernández, 2016).

El enfoque multimetodológico aplicado implica una interpretación profunda del objeto de estudio, lo que facilita una comprensión integral de la problemática planteada y permite analizar el impacto del fenómeno en cuestión (Arteaga et al., 2017; Meza et al., 2022).

La investigación se desarrolla como un estudio transversal, cuyo objetivo es observar y analizar cómo la vigilancia digital afecta la garantía de los derechos humanos en Colombia; este enfoque permite la comparación de diferentes eventos y contextos, proporcionando una aproximación eficiente al tema mediante la integración de diversas fuentes de información; las categorías abordadas para el desarrollo de la investigación incluyen tecnología, vigilancia y derechos humanos (Pacheco, 2019; Valle., Manrique., & Revilla, 2022; Borjas, 2020).

En el proceso de análisis y comprensión del fenómeno, se emplean herramientas metodológicas que permiten un acercamiento riguroso a la realidad mediante el análisis normativo y la recolección bibliográfica, es decir, la consulta de fuentes secundarias como artículos, libros, informes y normas (Flores, Franco, Ricalde, Garduño, & Apáez, 2013).

Estas fuentes proporcionan la información necesaria para abordar de manera eficiente cada una de las categorías y dimensiones del estudio, asegurando que el análisis responda a los objetivos de la investigación y permita la presentación de conclusiones lógicas, teóricas y recomendaciones pertinentes (Echeverría, 2005).

La metodología cualitativa de revisión y análisis documental y normativo utilizada en este estudio no solo permite un análisis crítico y contextualizado de las fuentes, sino que también facilita la identificación de patrones y tendencias en la aplicación de la normativa relacionada con la vigilancia y los derechos humanos. Esta aproximación metodológica, al centrarse en la interpretación de datos cualitativos, permite una mayor flexibilidad en el análisis y una mejor adaptación a la complejidad del fenómeno investigado (Miras., & Requena, 2014; Neubauer, 2022).

Marco Teórico

La vigilancia digital se ha convertido en un tema central en el debate global sobre los derechos humanos, especialmente en un contexto donde los Estados recurren a herramientas tecnológicas avanzadas para garantizar la seguridad y el seguimiento de sus ciudadanos; en un mundo cada vez más interconectado y digitalizado, la tecnología ofrece poderosos instrumentos que pueden ser utilizados no solo para monitorear y proteger, sino también para facilitar la justicia. Sin embargo, esta misma tecnología plantea desafíos significativos en términos de privacidad, libertad de expresión y otros derechos fundamentales, en este contexto, Colombia, como Estado social de derecho, enfrenta un desafío particular: encontrar el equilibrio adecuado entre el uso de la vigilancia digital para garantizar la seguridad y la justicia, y la protección de los derechos humanos de sus ciudadanos (Gómez, 2010; Bolaño, 2022).

La Teoría del Control Social, tal como fue desarrollada por Travis Hirschi (2003), Talcott Parsons (2012) y Émile Durkheim (1966, 2002), ofrece un marco conceptual útil para entender cómo las sociedades regulan el comportamiento a través de mecanismos formales e informales; en el contexto colombiano, la vigilancia digital puede ser vista como una extensión moderna de estos mecanismos de control. Hirschi argumentaba que la conformidad de los individuos con las normas sociales depende de los vínculos que estos tienen con la sociedad, como el apego a las instituciones y el compromiso con las normas establecida, en este sentido, la vigilancia digital refuerza estos vínculos al generar un sentido de autocontrol, dado que los ciudadanos saben que su comportamiento puede estar bajo constante monitoreo.

Sin embargo, esta capacidad de control plantea interrogantes sobre la capacidad del Estado para garantizar que el monitoreo no se convierta en una forma de represión.

Por su parte, Talcott Parsons (2012), con su visión funcionalista de la sociedad como un sistema en el que las instituciones regulan el comportamiento para mantener el equilibrio, ofrece un análisis que se puede aplicar al contexto colombiano, la vigilancia digital se convierte en un subsistema que regula de manera eficiente el comportamiento de los individuos, pero que también puede fallar en su objetivo si no está acompañado de un marco normativo claro y de salvaguardias que limiten su uso excesivo. En un Estado donde las instituciones aún luchan por consolidar la confianza ciudadana, la vigilancia digital sin la adecuada regulación puede generar exclusión y opresión, en lugar de garantizar la seguridad y el orden.

Emile Durkheim (1966, 2002), con su concepto de anomia, introduce una perspectiva valiosa para analizar las deficiencias en la regulación de la vigilancia digital en Colombia; la falta de un marco normativo claro para el uso de tecnologías emergentes, como el reconocimiento facial y los drones, puede generar una situación de anomia digital, donde la ausencia de normas claras fomenta el abuso de poder y la desconfianza en las instituciones. Este vacío normativo podría resultar perjudicial no solo para la garantía de los derechos fundamentales, sino también para la cohesión social, ya que los ciudadanos, al no sentir que sus derechos están protegidos, podrían volverse más reacios a cooperar con el Estado y a respetar sus leyes.

Por otro lado, la Teoría del Panóptico, desarrollada inicialmente por Jeremy Bentham (2011) y más tarde reinterpretada por Michel Foucault (2020) y Zygmunt Bauman (2015), ofrece una metáfora poderosa para comprender los mecanismos de vigilancia en las

sociedades modernas. Bentham concibió el panóptico como una estructura donde los individuos son vigilados de manera constante sin saber si realmente están siendo observados, lo que les lleva a autocensurarse y conformarse con las normas. Este concepto es fácilmente aplicable a la vigilancia digital contemporánea. Las tecnologías que permiten la vigilancia masiva, como las cámaras de seguridad y el análisis de grandes volúmenes de datos, generan un entorno donde los ciudadanos pueden sentir que están siendo observados en todo momento, lo que les lleva a moderar su comportamiento de manera anticipada. Aunque este efecto puede ser útil para mantener el orden, también plantea riesgos para las libertades individuales, ya que la vigilancia constante puede coartar derechos fundamentales como la libertad de expresión y la privacidad (Pérez-Fernández, 2024)).

Foucault (2020), en su análisis del poder y la vigilancia, sostiene que las sociedades modernas han adoptado estructuras panópticas en todas las esferas de la vida, no solo en las cárceles, sino también en las escuelas, hospitales y espacios de trabajo. En el caso de Colombia, la implementación de tecnologías de vigilancia digital sin un marco regulador adecuado puede ser vista como un mecanismo de control estatal que no solo disciplina a los ciudadanos, sino que también limita la posibilidad de cuestionar el poder y de expresar disidencia. Esto es especialmente preocupante en un país donde la vigilancia ha sido históricamente utilizada como una herramienta para controlar a grupos vulnerables o críticos del gobierno.

Zygmunt Bauman (2015), en su análisis de la modernidad líquida, lleva el concepto del panóptico un paso más allá, argumentando que en el mundo contemporáneo, la vigilancia ya no se limita a un espacio físico, sino que es difusa, líquida y omnipresente. La vigilancia digital es un ejemplo claro de esta vigilancia líquida, donde tanto el Estado como los actores

privados tienen acceso a herramientas tecnológicas que les permiten recolectar grandes cantidades de datos personales. En Colombia, esta vigilancia líquida puede aumentar la capacidad de control tanto del Estado como de las empresas privadas, lo que plantea serias dudas sobre el uso que se le da a estos datos y sobre la protección de los derechos humanos en un entorno donde la vigilancia es omnipresente.

El dilema de la vigilancia digital en Colombia se sitúa, entonces, en la tensión entre la necesidad de seguridad y la protección de los derechos humanos; la implementación de tecnologías de vigilancia puede ser fundamental para mejorar la seguridad, especialmente en un país con un pasado conflictivo y una situación de seguridad aún inestable. Sin embargo, como advierte la teoría del panóptico, la vigilancia sin límites ni salvaguardias puede derivar en un régimen autoritario, donde el Estado utiliza estas tecnologías no para proteger a los ciudadanos, sino para controlar y reprimir; la falta de un marco regulatorio específico que contemple el uso de tecnologías emergentes en Colombia deja un vacío legal que podría ser explotado, tanto por el Estado como por actores privados, con consecuencias potencialmente graves para los derechos fundamentales (Yupanqui, 2017).

Además, la desconfianza en las instituciones del Estado, resultado de décadas de conflicto armado y corrupción, agrava el problema. Los ciudadanos son cada vez más escépticos respecto a las intenciones del gobierno cuando se trata de implementar tecnologías de vigilancia. Desde la perspectiva de la teoría del control social, la debilidad en los vínculos entre los ciudadanos y el Estado puede generar una situación de anomia, donde el uso de la vigilancia digital, lejos de fortalecer el orden social, provoca resistencia y desconfianza (Saavedra, 2014).

En conclusión, la vigilancia digital en Colombia plantea una serie de desafíos éticos y normativos que requieren una reflexión profunda. Si bien estas tecnologías pueden contribuir a mejorar la seguridad y la justicia, su implementación sin un marco regulador claro puede llevar a la violación de derechos humanos fundamentales. Es necesario que el Estado colombiano desarrolle un marco normativo que garantice que la vigilancia digital se utilice de manera transparente y respetuosa de los derechos humanos. De lo contrario, la tecnología, en lugar de ser un instrumento para promover la justicia, podría convertirse en una herramienta de represión y control social.

La protección de los derechos humanos en la vigilancia digital.

La protección de los derechos humanos en el contexto de la vigilancia digital es un desafío crucial en la era moderna, donde la tecnología se ha integrado profundamente en casi todos los aspectos de la vida cotidiana; aunque la vigilancia digital puede ser una herramienta poderosa para mantener el orden público y prevenir delitos, también presenta serios riesgos para los derechos fundamentales, como la privacidad, la libertad de expresión y la libertad de reunión. Por ello, es esencial que existan marcos legales sólidos que protejan estos derechos contra posibles abusos por parte del Estado o de entidades privadas (Bartolomé, 2021; Valdez, 2019).

La vigilancia digital ha experimentado una evolución significativa a lo largo de los años, implementándose de manera continua y adaptativa en diferentes países alrededor del mundo. En América Latina, esta tendencia no ha sido la excepción, destacándose países como Brasil, Ecuador y Colombia, que han adoptado tecnologías de vigilancia digital de manera eficiente para mejorar la seguridad pública y la gestión de la información; estas naciones han

implementado sistemas avanzados, como cámaras de reconocimiento facial, drones y plataformas de análisis de datos, con el objetivo de fortalecer el control social y la prevención del delito, aunque no sin generar preocupaciones sobre el equilibrio entre seguridad y derechos humanos (Bartolomé, 2021; Véliz, 2021).

En Ecuador, la vigilancia digital ha adquirido mayor relevancia, especialmente tras el mayor hackeo de datos en la historia del país y el controvertido caso de Ola Bini, un activista de derechos digitales. Estos eventos han subrayado la urgente necesidad de fortalecer la protección de los derechos humanos en el ámbito digital. La vigilancia masiva sin salvaguardias adecuadas puede llevar a graves violaciones de la privacidad y otros derechos fundamentales, erosionando la confianza de los ciudadanos en las instituciones y limitando su libertad de expresión y de reunión (Valdez, 2019).

La vigilancia digital puede ser ejercida tanto por las autoridades (surveillance) como por la ciudadanía; mientras que la primera suele ser más intrusiva y cuenta con mayores recursos tecnológicos, la segunda es una respuesta de la sociedad para monitorear a quienes los vigilan. Sin embargo, la sousveillance está tecnológicamente limitada y no siempre es suficiente para equilibrar el poder entre vigilantes y vigilados. Por lo tanto, es crucial que las autoridades sean transparentes y rindan cuentas sobre el uso de tecnologías de vigilancia para evitar abusos (Perez, 2017; García, 2016).

El reconocimiento facial es un claro ejemplo de cómo la vigilancia digital puede amenazar los derechos humanos. En Estados Unidos, esta tecnología ha sido utilizada por diversas agencias para identificar a sospechosos en disturbios y protestas, generando preocupación sobre su uso indiscriminado (Sanabria., Roa., & Lee, 2022). En Rusia y China, la situación es aún más alarmante, ya que el reconocimiento facial ha sido empleado para

reprimir a activistas y manifestantes pacíficos, evidenciando la falta de un marco jurídico que proteja adecuadamente los derechos fundamentales (Cebul., & Pinckney, 2021; Daucé, 2014).

En Hong Kong, los manifestantes recurrieron al uso de láseres para evadir las cámaras de reconocimiento facial, demostrando cómo la tecnología puede ser empleada tanto para la represión como para la resistencia (Redacción IFOBAE; 2019). Sin embargo, cuando el Estado ejerce un control exhaustivo sobre la vigilancia, las posibilidades de proteger los derechos humanos se ven significativamente reducidas; por ello, la vigilancia digital debe ser regulada con un enfoque que priorice la protección de los derechos fundamentales (Quinn, et al, 2002).

En Colombia, se han implementado tecnologías de vigilancia como circuitos cerrados de televisión (CCTV), BodyCams, drones y software enfocado en el almacenamiento de información sobre protestas, manifestaciones y movilizaciones; la obtención de información sobre estas prácticas fue posible gracias a un exhaustivo trabajo de investigación que incluyó solicitudes de derechos de petición a las principales entidades estatales y distritales encargadas de la seguridad ciudadana, así como la revisión de noticias y la consulta de procedimientos regulados en el país (Villalobos, 2020; Duarte, et al, 2021).

Adicionalmente, la vigilancia digital en el país ha sido impulsada como parte de políticas públicas orientadas a fortalecer la seguridad nacional, según lo reiterado por el Ministerio de Defensa, la Policía Nacional es la institución encargada de utilizar medios tecnológicos para acompañar manifestaciones públicas pacíficas y gestionar disturbios o alteraciones del orden público.

No obstante, este enfoque ha sido objeto de cuestionamientos por parte de académicos, quienes han señalado posibles inconsistencias legales en algunos de los sistemas utilizados por las autoridades; Carmina (2023) destaca que, bajo la "Política de Defensa y Seguridad. Todos por un Nuevo País," se ha priorizado el uso de la tecnología, como las cámaras de vigilancia, con el objetivo de ampliar los sistemas de monitoreo y combatir la criminalidad, estos desarrollos han puesto en primer plano la necesidad de evaluar cuidadosamente las implicaciones legales y éticas de la vigilancia digital en el país.

En conclusión, la protección de los derechos humanos en el contexto de la vigilancia digital es un desafío que requiere un equilibrio delicado entre seguridad y libertad, a medida que las tecnologías de vigilancia se expanden y se implementan de manera más eficiente en diferentes países, incluyendo varias naciones en América Latina, se hace evidente la necesidad de marcos legales sólidos y transparentes que regulen su uso. Estas regulaciones son esenciales para evitar que la vigilancia digital, que puede ser una herramienta valiosa para el control social y la prevención del delito, se convierta en un medio de represión que socave derechos fundamentales como la privacidad, la libertad de expresión y la libertad de reunión. Los casos en Ecuador, Rusia, China, y Colombia demuestran que, sin salvaguardias adecuadas, la vigilancia digital puede tener graves consecuencias para los derechos humanos, haciendo imperativo un enfoque regulatorio que priorice la protección de estos derechos en todos los contextos (Borboa, 2023).

El alcance de la vigilancia digital en Colombia

El alcance de la vigilancia digital en Colombia es un asunto complejo y multifacético que involucra diversas dimensiones legales, tecnológicas y de derechos humanos. Este tema

ha cobrado relevancia en los últimos años, a medida que el avance tecnológico ha permitido el desarrollo y la implementación de nuevos sistemas de monitoreo que, aunque pueden ser efectivos para garantizar la seguridad pública, también generan preocupaciones significativas en cuanto a la protección de la privacidad y otros derechos fundamentales (Gerlero., Lezcano., & Liceda, 2019).

En Colombia, el marco legal y normativo que regula la vigilancia digital se ha desarrollado con el objetivo de equilibrar la necesidad de seguridad con la protección de los derechos individuales; la Ley 1581 de 2012, también conocida como la Ley de Protección de Datos Personales, establece las bases para la recolección, almacenamiento y uso de datos personales por parte de entidades públicas y privadas. Esta ley es fundamental para la protección de la privacidad de los ciudadanos, ya que regula el tratamiento de la información personal y establece obligaciones para quienes manejan estos datos. Sin embargo, la Ley 1581 de 2012 se enfoca principalmente en la protección de datos personales en general y no aborda de manera específica las tecnologías de vigilancia digital, lo que deja ciertos aspectos desregulados (Cano, 2018; Chaparro-López, 2021).

Además de la Ley 1581 de 2012, el Código Nacional de Policía y Convivencia (Ley 1801 de 2016) es otra pieza clave del marco normativo en Colombia; esta ley otorga a las autoridades facultades para utilizar tecnologías de vigilancia en el contexto de la seguridad pública, con el fin de prevenir y controlar actividades delictivas (Bernal, 2022; Ochoa, 2017).

Este marco legal permite el uso de cámaras de vigilancia, drones y otros dispositivos de monitoreo en áreas públicas, particularmente en ciudades y zonas con alta criminalidad; el objetivo principal de estas tecnologías es reforzar la seguridad pública y mejorar la capacidad de respuesta de las autoridades ante situaciones de emergencia; sin embargo, la

implementación de estas tecnologías también ha suscitado preocupaciones sobre el impacto que pueden tener en la privacidad de las personas, especialmente cuando se utilizan de manera masiva y sin una regulación específica (Parra, 2018).

Uno de los avances tecnológicos más destacados en el ámbito de la vigilancia digital en Colombia es el uso del reconocimiento facial, aunque esta tecnología tiene el potencial de mejorar la eficiencia en la identificación de sospechosos y en la prevención del delito, su implementación ha sido objeto de debate debido a la ausencia de una regulación clara que establezca los límites y condiciones para su uso, la Policía Nacional y otras entidades de seguridad han comenzado a utilizar sistemas de reconocimiento facial en ciertos contextos, pero la falta de un marco regulatorio específico deja un vacío legal que podría permitir abusos o un uso excesivo de esta tecnología. La preocupación principal radica en que el reconocimiento facial puede facilitar la vigilancia masiva e indiscriminada, lo que podría resultar en una erosión del derecho a la privacidad y otros derechos fundamentales (Gómez-Córdoba, et al, 2020; Aliaga, 2023; Carbajal, 2024).

El derecho a la privacidad es uno de los principales desafíos que plantea la expansión de la vigilancia digital en Colombia; la Constitución Política de Colombia garantiza el derecho a la intimidad y a la protección de los datos personales, pero la creciente utilización de tecnologías avanzadas como la inteligencia artificial y el análisis de grandes volúmenes de datos (Big Data) está poniendo a prueba estas garantías constitucionales, la falta de una regulación específica sobre el uso de tecnologías como el reconocimiento facial y la inteligencia artificial en el contexto de la vigilancia digital deja a los ciudadanos en una situación vulnerable, ya que no existen mecanismos claros para prevenir o remediar posibles violaciones a su privacidad (Arce, 2022; Rivero-Ortega, 2023).

La supervisión y el control del uso de tecnologías de vigilancia en Colombia están a cargo de varias entidades, siendo la Superintendencia de Industria y Comercio (SIC) una de las más relevantes en el ámbito de la protección de datos personales. La SIC tiene la responsabilidad de vigilar el cumplimiento de la Ley 1581 de 2012 y de sancionar a quienes incumplan con las disposiciones establecidas en esta ley, no obstante, el control sobre tecnologías específicas de vigilancia, como los drones o los sistemas de reconocimiento facial, es aún limitado; esto se debe en parte a la falta de un marco normativo que regule de manera detallada el uso de estas tecnologías, lo que dificulta la labor de supervisión y control por parte de las autoridades competentes (Gómez., & Botero, 2016; Pérez, 2018).

En cuanto a los avances y perspectivas futuras, Colombia se encuentra en un punto crítico en relación con la vigilancia digital, el desarrollo de tecnologías más avanzadas, como la inteligencia artificial y el análisis de grandes volúmenes de datos, está ampliando el alcance y la capacidad de la vigilancia digital en el país; estas tecnologías ofrecen oportunidades significativas para mejorar la seguridad pública y la eficiencia en la gestión de recursos, pero también plantean nuevos desafíos éticos y legales que deben ser abordados de manera oportuna (Velásquez., Martínez., & Palma, 2020; Aguilar, 2016; Barragán-Huamán., et al, 2023).

La inteligencia artificial, por ejemplo, puede ser utilizada para predecir patrones de comportamiento y anticipar delitos, lo que podría ser una herramienta valiosa para las autoridades. Sin embargo, el uso de estas tecnologías también podría dar lugar a la discriminación o la vigilancia masiva sin un control adecuado, lo que subraya la necesidad de un marco regulatorio más específico (Chaure, 2021; Borges., & Pérez, 2024).

El desarrollo de un marco regulatorio que aborde de manera integral los riesgos y beneficios de las tecnologías de vigilancia digital es una tarea pendiente en Colombia. Aunque existen leyes y normas que regulan ciertos aspectos de la vigilancia, estas no son suficientes para enfrentar los desafíos que plantea el avance tecnológico. Es necesario que el legislador colombiano desarrolle una normativa más específica y detallada que establezca claramente los límites y condiciones para el uso de tecnologías de vigilancia, garantizando un equilibrio entre la seguridad pública y la protección de los derechos humanos. Este marco regulatorio debería incluir disposiciones sobre la transparencia en el uso de estas tecnologías, el consentimiento informado de los ciudadanos, y mecanismos efectivos de supervisión y control por parte de las autoridades (Muñiz, 2020; Morato., & Quintero, 2022).

En resumen, el alcance de la vigilancia digital en Colombia está en expansión, impulsado por el crecimiento en el uso de nuevas tecnologías de monitoreo que, aunque potencialmente útiles para la seguridad pública, plantean importantes desafíos en términos de privacidad y derechos humanos; la falta de una regulación específica y detallada sobre el uso de tecnologías como el reconocimiento facial, los drones y la inteligencia artificial deja a los ciudadanos en una situación de vulnerabilidad frente a posibles abusos o un uso excesivo de estas herramientas; para enfrentar estos desafíos, es fundamental que Colombia desarrolle un marco regulatorio más robusto que garantice un equilibrio adecuado entre la necesidad de seguridad y la protección de los derechos fundamentales, asegurando que el avance tecnológico no se traduzca en una erosión de las libertades individuales.

Implicaciones legales y normativa de la vigilancia digital en Colombia

Las implicaciones legales y normativas de la vigilancia digital en Colombia constituyen un tema complejo que abarca múltiples aspectos del derecho a la privacidad, la protección de datos personales, y el uso de tecnologías avanzadas como cámaras de seguridad, drones y sistemas de reconocimiento facial; la protección de la privacidad en Colombia está amparada por un marco legal que, aunque robusto en ciertos aspectos, presenta vacíos significativos, especialmente en lo que respecta a la regulación de tecnologías emergentes que podrían afectar los derechos fundamentales de los ciudadanos (Bernal, 2022; Arroyo, 2023).

En primer lugar, es crucial señalar que el derecho a la privacidad en Colombia está garantizado por la Constitución de 1991; este derecho, consagrado en el artículo 15, protege la intimidad, la honra y la reputación de las personas, y establece el derecho al habeas data, que permite a los individuos conocer, actualizar y rectificar la información que se ha recopilado sobre ellos en bases de datos. La Corte Constitucional, en su jurisprudencia, ha subrayado la importancia de este derecho, aunque ha reconocido que no es absoluto. En ciertas circunstancias, como la necesidad de preservar el orden público o garantizar la seguridad nacional, este derecho puede ser limitado. No obstante, cualquier restricción debe ser proporcional y estar respaldada por un marco legal claro y preciso, lo que garantiza un equilibrio entre la protección de la privacidad y otras necesidades colectivas (Salcedo, 2003; Santiago, 2014; Arévalo, 2018).

En cuanto a la protección de datos personales, la Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales, establece un régimen general para la recolección,

almacenamiento, uso, circulación y supresión de datos personales en Colombia; esta ley es fundamental para cualquier sistema de vigilancia que implique el tratamiento de datos personales, ya que exige el consentimiento informado del titular de los datos y establece una serie de derechos y garantías para los ciudadanos. Además, el Decreto 1377 de 2013 reglamenta parcialmente esta ley, imponiendo obligaciones adicionales a los responsables del tratamiento de datos, como la adopción de medidas de seguridad y la implementación de políticas de privacidad, estas normativas buscan proteger a los ciudadanos de posibles abusos en el manejo de su información personal, aunque en la práctica se presentan desafíos significativos, especialmente cuando se trata de tecnologías avanzadas de vigilancia (Cano, 2012; Cabezas, 2023; Gómez, 2017; Vargas., & Montealegre, 2021).

El uso de tecnologías de vigilancia en Colombia, particularmente cámaras de seguridad en espacios públicos, es otro aspecto crucial, aunque existen normativas a nivel local y nacional que regulan el uso de estas tecnologías, el panorama se complica cuando se introducen sistemas avanzados como el reconocimiento facial; a pesar de su potencial para mejorar la seguridad pública, la falta de una regulación específica sobre el uso de estas tecnologías plantea serias preocupaciones sobre la invasión de la privacidad y el posible mal uso de la información recogida. De manera similar, el uso de drones con fines de vigilancia está regulado por la Aeronáutica Civil de Colombia, que ha establecido normas para el uso de vehículos aéreos no tripulados, sin embargo, estas regulaciones no abordan de manera específica las implicaciones en términos de privacidad y protección de datos personales cuando estos drones se utilizan con fines de seguridad pública (Abril., & Pizarro, 2014; Jasso., & Jasso, 2021).

Uno de los principales desafíos que enfrenta Colombia en este contexto es la regulación de tecnologías emergentes, como el reconocimiento facial y la inteligencia artificial; a pesar de los avances tecnológicos, el país aún no cuenta con un marco regulatorio específico que aborde las particularidades de estas tecnologías, lo que genera una serie de preocupaciones sobre posibles violaciones de derechos fundamentales. La ausencia de regulaciones claras también crea incertidumbre sobre los límites y alcances del uso de estas tecnologías en la seguridad pública, lo que podría dar lugar a conflictos entre el derecho a la privacidad y la necesidad de mantener el orden público (Oliver, 2021; Victoria-Díaz., Rosero-García., & Prías-Caicedo, 2016).

Además de los desafíos internos, Colombia también debe cumplir con sus obligaciones internacionales en materia de derechos humanos; como la Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, el país está obligado a asegurar que sus prácticas de vigilancia digital se alineen con los estándares internacionales. Estos tratados protegen derechos fundamentales como la privacidad y la libertad de expresión, y cualquier desviación de estas normas podría resultar en sanciones o recomendaciones por parte de organismos internacionales (Ramírez-Huertas, 2017; Ramelli, 2004).

A pesar de los esfuerzos legislativos y regulatorios en Colombia, el país enfrenta vacíos y desafíos significativos en la regulación de la vigilancia digital; estos vacíos se hacen más evidentes con el rápido avance de tecnologías emergentes que, si bien pueden ser herramientas poderosas para garantizar la seguridad pública, también plantean riesgos importantes para los derechos fundamentales. La falta de un marco normativo específico que regule el uso de tecnologías como el reconocimiento facial o la inteligencia artificial crea un

terreno fértil para posibles abusos y violaciones de la privacidad, lo que subraya la necesidad urgente de desarrollar y adoptar regulaciones más claras y robustas.

En conclusión, las implicaciones legales y normativas de la vigilancia digital en Colombia reflejan un equilibrio delicado entre la necesidad de seguridad pública y el respeto por los derechos fundamentales, en particular el derecho a la privacidad; a medida que las tecnologías de vigilancia continúan evolucionando, se hace evidente la necesidad de un marco regulatorio más claro y robusto que garantice que estas tecnologías se utilicen de manera que sean compatibles con los derechos humanos. Colombia, como muchos otros países, se encuentra en una encrucijada donde debe decidir cómo avanzar en la regulación de estas tecnologías, asegurando que la protección de la privacidad y otros derechos fundamentales no se sacrifiquen en nombre de la seguridad pública.

Conclusiones

En conclusión, la vigilancia digital en Colombia presenta un desafío crítico en la garantía de los derechos humanos, en un contexto donde la tecnología juega un papel cada vez más dominante en la vida cotidiana, la integración de sistemas avanzados de vigilancia, como cámaras de reconocimiento facial y drones, ha sido impulsada por políticas públicas orientadas a mejorar la seguridad y el orden público. Sin embargo, este avance tecnológico conlleva riesgos significativos para derechos fundamentales como la privacidad, la libertad de expresión y la libertad de reunión.

Aunque la legislación colombiana, incluyendo la Ley 1581 de 2012 y el Código Nacional de Policía y Convivencia, proporciona un marco para la protección de datos personales y el uso de tecnologías de vigilancia, estas normativas resultan insuficientes para

abordar los desafíos emergentes asociados con tecnologías avanzadas, la falta de regulaciones específicas para tecnologías como el reconocimiento facial y la inteligencia artificial expone a los ciudadanos a riesgos considerables de invasión de privacidad y posibles abusos, dada la existencia de vacíos legales y la ausencia de un marco detallado que contemple las particularidades de estas herramientas (Pinto., León., & Serna, 2024).

Este panorama revela la necesidad urgente de un enfoque regulatorio más robusto y específico en Colombia, para garantizar que la vigilancia digital no se convierta en un instrumento de represión que socave derechos fundamentales, es imperativo desarrollar una normativa integral que equilibre la seguridad pública con la protección de las libertades individuales; un marco legal claro y detallado no solo permitirá enfrentar los retos de la vigilancia digital de manera efectiva, sino que también asegurará que el progreso tecnológico respete los derechos humanos y preserve la privacidad y otras libertades esenciales. En resumen, Colombia se encuentra en un momento crucial donde debe equilibrar la innovación tecnológica con la protección de los derechos fundamentales, asegurando que la seguridad no se logre a expensas de la libertad y la dignidad de sus ciudadanos.

Referencias

Abril, P., & Pizarro, E. (2014). La intimidad europea frente a la privacidad americana. *Revista para el Análisis del Derecho: Indret*, *1*, 1-62.

Aguilar, L. (2016). *Big Data, Análisis de grandes volúmenes de datos en organizaciones*. Alfaomega Grupo Editor.

Aliaga, A. (2023). El impacto de la tecnología del reconocimiento facial en la prevención del delito de robo agravado en Lima 2022.

Arce, C. (2022). Desafíos para la ciudadanía y el sistema de derechos fundamentales en la era digital. *Derechos y Libertades: 46, 1, 2022*, 241-272.

Arévalo, D. (2018). *Análisis jurídico-crítico sobre los derechos que se afectan al divulgar información personal por parte de las instituciones financiera en el cantón Otavalo* (Bachelor's thesis).

Arroyo, C. (2023). *Revolución digital y Constitución*. Palestra Editores.

Arroyo, C. (2023). *Revolución digital y Constitución*. Palestra Editores.

Barragán-Huamán, H., et al. (2023). La inteligencia artificial y la video-vigilancia en la predicción y detección de delitos en espacio-tiempo: una revisión sistemática. *Revista Criminalidad, 65*(1), 11-25.

Bartolomé, M. (2021). Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. *RESI: Revista de estudios en seguridad internacional*, *7*(2), 167-185.

Bauman, Z. (2015). *Modernidad líquida*. Fondo de cultura económica.

Bentham, J. (2011) Panóptico (trad. David Cruz Acevedo). Madrid: Círculo de Bellas Artes.

Bernal, D. (2022). Transformación del concepto de la ciudad inteligente: estado del arte. Ci en el ordenamiento jurídico colombiano: perspectiva holística e integral de la CI como construcción social, que impacta los desafíos multinivel de la ciudad del siglo XXI y el ordenamiento jurídico de los Estados que la materializan.

Bernal, D. (2022). Transformación del concepto de la ciudad inteligente: estado del arte. Ci en el ordenamiento jurídico colombiano: perspectiva holística e integral de la CI como construcción social, que impacta los desafíos multinivel de la ciudad del siglo XXI y el ordenamiento jurídico de los Estados que la materializan.

Betin, J. (2012). Propaganda y control social en Talcott Parsons. *Talcott Parsons:¿ el último clásico?*, 199.

Bolaño, M. (2022). *Tecnologías educativas para la inclusión*. Editorial Unimagdalena.

Borboa, R. (2023). Las Herramientas Digitales Aplicadas a las Ciencias Penales: Un Análisis Contemporáneo Digital Tools Applied to Criminal Sciences: A Contemporary Analysis. *Función y sentido de la Investigación en las instituciones de educación superior*.

Borges, M., & Pérez, P. (2024). Datos policiales e Inteligencia Artificial: Un equilibrio delicado entre la privacidad, la utilidad y la ética. *Revista Canaria de Administración Pública*, 143-175.

Borjas, J. (2020). Validez y confiabilidad en la recolección y análisis de datos bajo un enfoque cualitativo. *Trascender, contabilidad y gestión*, *5*(15), 79-97.

Buenadicha, C., et al. (2019). La gestión ética de los datos. *Por qué importa y cómo hacer un uso justo de los datos en un mundo digital BID, editor*.

Burger, T. (1978). Social Systems and the Evolution of Action Theory.

Cano, L. (2018). El Panóptico digital de la protección de datos personales en Colombia. *Revista Temas: Departamento de Humanidades Universidad Santo Tomás Bucaramanga*, (12), 125-140.

Cano, L. G. (2012). Protección de datos en Colombia, avances y retos. *Lebret*, (4), 195-214.

Carbajal, F. (2024). Uso de drones en las operaciones policiales para mejorar el patrullaje integrado y combatir la inseguridad ciudadana. *Revista Escpogra PNP*, *4*(1), 73-83.

Carmina, L. (2023). La ciudad videovigilada: entre la prevención del crimen y el control social. Universidad Nacional Autónoma de México, Instituto de Investigaciones Sociales.

Cebul, M., & Pinckney, J. (2021). Autoritarismo digital y acción no violenta: Desafiando la contrarrevolución digital.

Chaparro-López, H. C. (2021). Derecho a la intimidad en el marco de la relación laboral en Colombia: manejo de información personal y protección de datos personales.

Chaure, P. (2021). Aplicaciones y oportunidades de la Inteligencia Artificial para la justicia penal: predicción del riesgo de reincidencia de reos y policía predictiva.

Daucé, F. (2014). Rusia: Los artigulios del autoritarismo.

Dávila, C., & Monsalve, D. (2023). La aplicación de los contratos legales inteligentes en el contrato de mutuo y su incidencia en el mercado Fintech en Colombia.

Dencik, L. (2024). Justicia de datos: consecuencias sociales de los macrodatos, la tecnología inteligente y la IA.

Duarte, A., et al. (2021). *Lineamientos para la integración de los sistemas de seguridad del subsistema de transporte de la ciudad de Bogotá* (Bachelor's thesis, Especialización en Gerencia de Proyectos-Virtual).

Durkheim, E. (1966). *Lecciones de sociología*. Buenos Aires: Schapire.

Durkheim, É. (2002). *La educación moral*. Ediciones Morata.

Fernández, P. (2016). Acerca de los enfoques cuantitativo y cualitativo en la investigación educativa cubana actual. *Atenas, 2*(34), 1-15.

Foucault, M. (2020). Panopticism. In *The information society reader* (pp. 302-312). Routledge.

García, J. (2022). Big brother-big data-big other. Tensiones del binomio (seguridad-libertad).

García, L. (2016). La eficacia de la vigilancia electrónica en la violencia de género: Análisis criminológico (The efficacy of electronic monitoring in gender violence: criminological analysis). *International e-journal of criminal sciences*, (10).

Gerlero, M., Lezcano, J., & Liceda, E. (2019). Los derechos en la sociedad digital.

Gómez, A. D. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, (8), 169-203.

Gómez, A., & Botero, E. (2016). *Responsabilidad civil derivada de la ruptura de deberes u obligaciones de protección de información personal* (Bachelor's thesis, Universidad EAFIT).

Gómez, O. (2017). Estudio comparado de la ley colombiana 1581 de 2012 y la ley federal mexicana de protección de datos personales.

Gómez-Córdoba, A., et al. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho*, (50), 271-294.

Hirschi, T. (2003). Una teoría del control de la delincuencia. *Capítulo criminológico*, *31*(4).

Jasso, L., & Jasso, C. (2021). Abuso policial, discrecionalidad y tecnologías de vigilancia en América Latina. *Iztapalapa. Revista de ciencias sociales y humanidades*, *42*(90), 119-144.

Liévano, I. (2024). Discursos sobre violencia en el conflicto armado colombiano: legalización de las cooperativas de vigilancia privada (Convivir) y legitimación del actuar violento en el Colombiano y el Espectador, 1993-1994 (Bachelor's thesis, Escuela de Teología, Filosofía y Humanidades).

Miras, R., & Requena, A. (2014). La aplicación de los criterios de la Grounded Theory en el análisis documental: Los textos legales y normativos españoles en materia de extranjería. *Empiria: Revista de metodología de ciencias sociales*, (28), 157-182.

Morato, K., & Quintero, A. (2022). Marco normativo y económico de las criptomonedas en Colombia en Relación con las legislaciones de México y el salvador en el Periodo 2015-2022.

Muñiz, J. (2020). La prevención de riesgos laborales y sus nuevas exigencias y retos frente al avance de la digitalización y las nuevas tecnologías. *Revista de Trabajo y Seguridad Social. CEF*, 83-115.

Neubauer, A. (2022). Elementos de la competencia intercultural: un análisis documental de la política educativa supranacional de la Unión Europea. *Revista complutense de educación*, *33*(4), 713-723.

Ochoa, E. (2017). Elementos y trámites procesales en el Código Nacional de Policía y Convivencia, Ley 1801 de 2016. *Pensamiento Jurídico*, (45), 219-239.

Oliver, N. (2021). Inteligencia artificial, naturalmente: un manual de convivencia entre humanos y máquinas para que la tecnología nos beneficie a todos.

Pacheco, A. (2019). La generación de valor público y confianza digital: retos y oportunidades de la nueva política de gobierno digital.

Parra, Y. (2018). El poder de policía en el nuevo Código Nacional de Policía y Convivencia, Ley 1801 de 2016. *Pensamiento Jurídico*, (47), 201-233.

Parsons, T. (2013). *The social system*. Routledge.

Pérez, C. (2018). El sector de seguridad y vigilancia privada: evolución reciente y principales retos laborales, regulatorios y de supervisión.

Perez, M. (2017). Punishment And Control: Collective Armed Territorial Surveillance In Mexico, The Case Of Tierra Caliente (Michoacan)/Castigo Y Control: La Vigilancia Colectiva Armada Territorial En Mexico, El Caso De Tierra Caliente (Michoacan). Direito da Cidade, 9(4), 1902-1930.

Pérez-Fernández, F. (2024). De la teoría de Bentham al "pseudopanóptico": Un modelo de análisis psicohistórico desde el "fracaso" de la reforma de prisiones en la España del siglo XIX al "panóptico digital" del siglo XXI.

Pinto, C., León, E., & Serna, N. (2024). Derechos humanos en la era digital. Análisis jurídico desde el derecho comparado para el reconocimiento de los derechos digitales como derechos de cuarta generación.

Quinn, G., et al. (2002). Derechos humanos y discapacidad. *Uso actual y posibilidades futuras de los instrumentos de Derechos Humanos de las Naciones Unidas en el contexto de la discapacidad. New York y Ginebra: Organización del Alto Comisionado de los Derechos Humanos OACDH.* ONU. http://www.ohchr. org/spanish/about/publications/docs/disability. pdf.

Ramelli, A. (2004). Sistema de fuentes del derecho internacional público y bloque de constitucionalidad en Colombia. *Cuestiones constitucionales*, (11), 157-175.

Ramió, C. (2019). *Inteligencia artificial y administración pública: robots y humanos compartiendo el servicio público*. Los libros de la Catarata.

Ramírez-Huertas, G. (2017). *Los derechos humanos a debate: perspectivas desde el derecho internacional*. Bogotá: Universidad Católica de Colombia, 2017.

Redacción INFOBAE. (2019 agosto 02). Los rayos láser que utilizan los manifestantes en Hong Kong para impedir la tecnología de reconocimiento facial de la policía. INFOBAE. https://www.infobae.com/america/mundo/2019/08/02/los-rayos-laser-que-utilizan-los-manifestantes-en-hong-kong-para-impedir-la-tecnologia-de-reconocimiento-facial-de-la-policia-china/

Rivero-Ortega, R. (2023). Derecho e inteligencia artificial: Cuatro estudios.

Saavedra Pérez, B. O. (2014). La privatización de la seguridad en Centroamérica: el caso de El Salvador.

Sanabria, J., Roa, M., & Lee, O. (2022). Tecnología de reconocimiento facial y sus riesgos en los derechos humanos. *Revista Criminalidad*, *64*(3), 61-78.

Santiago, V. (2014). El Derecho figura del Hábeas Data.

Vadell, L., Rúa, M., & Garzón, L. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, *7*(2), 1347-1384.

Valdez, G. (2019). Privacidad digital en Ecuador: el papel de la vigilancia, la jurisprudencia y los derechos humanos.

Valdez, G. (2019). Privacidad digital en Ecuador: el papel de la vigilancia, la jurisprudencia y los derechos humanos.

Valle, A., Manrique, L., & Revilla, D. (2022). La investigación descriptiva con enfoque cualitativo en educación.

Vargas, A., & Montealegre, L. (2021). El Delegado de Protección de Datos Personales, mecanismo idóneo para la protección de los usuarios de las entidades privadas en clave a la recolección, tratamiento y uso de sus datos personales en Colombia.

Velásquez, A., Martínez, R., & Palma, A. (2020). Revolución tecnológica e inclusión social: reflexiones sobre desafíos y oportunidades para la política social en América Latina.

Victoria-Díaz, M., Rosero-García, J., & Prías-Caicedo, Ó. (2016). Vigilancia tecnológica de vehículos eléctricos y tecnologías periféricas en Colombia. *Ingenio Magno, 7*, 56-68.

Villalobos, H. (2020). El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito. *Revista de relaciones internacionales, estrategia y seguridad*, *15*(1), 79-97.