Lineamientos en el Ejército Nacional para garantizar la protección de datos en los términos de la Ley 1581 de 2012, a partir de la implementación de la Directiva 003 de 2019

Giovanny Armando Afanador Torres

Monografía para optar al título profesional:

Magister en Derechos Humanos y DICA.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

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

DATOS GENERALES		
Nombre del estudiante	**:**	Giovanny Armando Afanador Torres
Identificación	**:**	7188298
Programa académico	**:**	Maestría en Derechos Humanos y DICA.
Tutor metodológico	**:**	Mauricio Antonio Torres Guarnizo
Tutor temático	**:**	Jonnathan Jiménez Reina
Fecha de entrega	**:**	02-septiembre-2025
Extensión	**:**	12284

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.

Esta monografía 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-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que esta monografía sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Lineamientos en el Ejército Nacional para garantizar la protección de datos en los términos de la Ley 1581 de 2012, a partir de la implementación de la Directiva 003 de 2019

Guidelines for the National Army to ensure data protection under Law 1581 of 2012, following the implementation of Directive 003 of 2019.

Giovanny Armando Afanador Torres [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La protección de datos personales se ha fortalecido tanto en el escenario nacional como en el internacional, particularmente ante la evolución acelerada de las tecnologías de la información y la comunicación. Desde el contexto nacional, Colombia ha venido reforzando el marco de protección de la información personal, en armonía con las disposiciones de la Carta Política de 1991, en concordancia con normas como la Ley 1266 de 2008 y la Ley Estatutaria 1581 de 2012. Si bien estos marcos normativos han permitido importantes avances, en instituciones como el Ejército Nacional persisten desafíos significativos para garantizar la seguridad y el tratamiento adecuado de los datos personales. Mediante la presente investigación, se ha planteado como objetivo general analizar los lineamientos existentes en el Ejército Nacional para garantizar la protección de datos personales, evaluando los desafíos normativos, éticos y tecnológicos que enfrenta la institución y proponiendo recomendaciones que permitan fortalecer su marco regulatorio interno. Dentro de un escenario metodológico aplicando el método cualitativo, se respondió a la pregunta ¿Qué lineamientos deberían establecerse en el Ejército Nacional para garantizar la protección de datos en los términos de la Ley 1581 de 2012, a partir de la implementación de la Directiva 003 de 2019? Finalmente se propusieron recomendaciones para el fortalecimiento un sistema integral de protección de datos acorde con la normativa vigente y con los estándares internacionales en contextos de defensa y seguridad.

Palabras clave: protección, datos personales, Ejército nacional, seguridad, tratamiento

Abstract: The protection of personal data has been strengthened both nationally and internationally, particularly in light of the rapid development of information and communications technologies. At the national level, Colombia has been reinforcing its personal data protection framework, in line with the provisions of the 1991 Political Constitution and with regulations such as Law 1266 of 2008 and Statutory Law 1581 of 2012. While these regulatory frameworks have enabled significant progress,

[1] Coronel del Ejército Nacional de Colombia. Candidato a magíster en estrategia y geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0000-0003-2004-7466 - Contacto: landinezj@esdeg.edu.co.

institutions such as the National Army still face significant challenges in ensuring the security and proper handling of personal data. This research aims to analyze the existing guidelines within the National Army to guarantee the protection of personal data, assessing the regulatory, ethical, and technological challenges facing the institution, and proposing recommendations to strengthen its internal regulatory framework. Within a methodological framework applying the qualitative method, the question was answered: What guidelines should be established in the National Army to guarantee data protection under the terms of Law 1581 of 2012, following the implementation of Directive 003 of 2019? Finally, recommendations were proposed for strengthening a comprehensive data protection system in accordance with current regulations and international standards in defense and security contexts.

Keywords: protection, personal data, National Army, security, processing

Introducción

La protección de los datos personales ha adquirido una relevancia creciente en el escenario contemporáneo, impulsada por el acelerado desarrollo de las tecnologías de la información y la comunicación, así como por la masificación del uso de plataformas digitales en la gestión pública y privada. Este fenómeno ha transformado radicalmente la manera en que los Estados, las instituciones y los ciudadanos procesan, almacenan y circulan información personal, lo que ha generado nuevos desafíos jurídicos, éticos y tecnológicos para la garantía de los derechos fundamentales, en particular la intimidad, la autodeterminación informativa y el habeas data.

Si bien se trata de una garantía reconocida desde mediados del siglo XX, a raíz de la consolidación del derecho internacional de los derechos humanos, su desarrollo normativo ha cobrado fuerza en las últimas décadas. Instrumentos como la Declaración Universal de Derechos Humanos (art. 12), el Pacto Internacional de Derechos Civiles y Políticos (art. 17) y la Convención Americana sobre Derechos Humanos (art. 11) han sido determinantes para establecer límites al uso de información personal por parte de los Estados. En América Latina, aunque no existe un modelo normativo uniforme, se han consolidado principios orientadores que promueven legislaciones nacionales que reconozcan el derecho a la privacidad y al control de los datos personales.

En Colombia, el artículo 15 de la Constitución Política consagra el derecho de todas las personas a conocer, actualizar y rectificar la información que sobre ellas se haya recogido en bases de datos o archivos, lo que constituye el fundamento del habeas data. Este mandato ha sido desarrollado por leyes como la 1266 de 2008 y, especialmente, la Ley Estatutaria

1581 de 2012, que establece el régimen general de protección de datos personales, junto con sus decretos reglamentarios. Sin embargo, al trasladar este marco normativo al ámbito de la seguridad y defensa nacional, y en particular al contexto del Ejército Nacional, surgen complejidades adicionales por la naturaleza estratégica, reservada y en muchos casos sensible de la información que se maneja.

En este contexto, la Directiva Permanente N. º 003 de 2019 del Ejército Nacional busca armonizar los principios legales de protección de datos con las necesidades operativas del sector defensa. No obstante, diversas investigaciones, diagnósticos institucionales y pronunciamientos jurídicos han advertido deficiencias en su implementación, vacíos normativos, debilidad en los controles y un bajo nivel de apropiación por parte del personal militar. Estas falencias comprometen no solo los derechos fundamentales de los titulares de la información, sino también la legitimidad y transparencia institucional.

En este marco, la presente investigación tiene como propósito analizar los lineamientos adoptados por el Ejército Nacional para garantizar la protección de datos personales conforme a la Ley 1581 de 2012, a partir de la implementación de la Directiva 003 de 2019, identificando sus alcances, limitaciones y desafíos, con el fin de proponer recomendaciones que fortalezcan su eficacia jurídica, operativa y tecnológica, en consonancia con los estándares nacionales e internacionales de derechos humanos.

Metodología

La presente investigación adoptó un enfoque metodológico cualitativo, sustentado en la interpretación y análisis crítico del marco jurídico y normativo que regula la protección de datos personales en el Ejército Nacional de Colombia, particularmente a partir de la

implementación de la Directiva Permanente N.° 003 del 25 de febrero de 2019. Este enfoque permitió abordar el fenómeno desde una perspectiva comprensiva, orientada a la exploración de significados, principios y prácticas institucionales, más allá de la mera cuantificación de variables, lo que resulta especialmente pertinente cuando se estudian derechos fundamentales y marcos regulatorios complejos.

Desde la clasificación por finalidad, se trata de una investigación aplicada, ya que tuvo como propósito no solo generar conocimiento teórico y descriptivo, sino también contribuir a la solución de una problemática práctica: la necesidad de fortalecer las garantías normativas e institucionales del tratamiento de datos personales dentro del Ejército Nacional.

Asimismo, la investigación se inscribió dentro de un diseño no experimental y de tipo documental-descriptivo, que tiene como base la recolección, revisión y sistematización de fuentes secundarias normas legales, directivas institucionales, manuales internos, jurisprudencia, doctrinas, informes de auditoría y literatura científica con el objetivo de reconstruir el marco normativo y las prácticas institucionales en torno a la protección de datos.

La técnica principal empleada fue la revisión documental, que permitió realizar un análisis exhaustivo de las fuentes normativas nacionales, en especial la Ley Estatutaria 1581 de 2012, el Decreto 1377 de 2013, la Sentencia C-748 de 2011 que establece los límites del tratamiento de datos personales, así como la Directiva Permanente N.° 003 de 2019 del Ejército Nacional, instrumento mediante el cual se regulan los procedimientos internos sobre protección de datos.

Resultados

Marco normativo colombiano sobre protección de datos personales en relación en el Ejército Nacional

En el mundo actual, donde la digitalización y automatización de la información personal, es cada vez más dinámica, la protección de los datos personales se ha convertido en una exigencia y garantía dentro del amplio campo de los derechos fundamentales, especialmente, por su conexidad con derechos como la intimidad, la autodeterminación informativa y el habeas data. Dentro del ordenamiento jurídico colombiano, es la Constitución Política de 1991, la que promueve la protección de los datos personales y la intimidad, y posteriormente se fue expidiendo el marco normativo, que inicialmente se delimito por disposiciones que crearon los delitos informáticos, para luego dar paso a la promulgación de la Ley 1581 de 2012, enfocada en la protección de los datos personales, por parte de las instituciones públicas, como de las organizaciones privadas, incluyendo principios rectores como la libertad, finalidad, legalidad, veracidad y seguridad. Sin embargo, en el ámbito de la seguridad y la defensa nacional, donde se encuentran las Fuerzas Militares, el tratamiento de los datos personales, adquiere un mayor grado de complejidad debido a la naturaleza reservada, estratégica y en ocasiones sensibles de la información que se maneja. En razón de ello, desde el Ministerio de Defensa fue expedida la Directiva 003 de 2019, con el objetivo de armonizar la actividad de las Fuerzas Militares con los lineamientos de la Ley 1581, promoviendo buenas prácticas en la gestión del habeas data.

No obstante, hay que decir que sobre este escenario persisten grandes desafíos, vacíos jurídicos y barreras operativas, que generan implicaciones frente a la protección jurídica de los datos personales en este ámbito. Frente a lo expuesto, algunos autores han expresado una preocupación sobre algunos aspectos relacionados con la protección de datos personales en diversos escenarios, especialmente aquellos relacionados con la seguridad nacional y los derechos fundamentales.

Uno de estos es (Bernal, 2022), quien asegura que dicha situación en las fuerzas militares en Colombia, requiere de la promoción de protocolos claros y mecanismos de seguridad para el tratamiento de la información sensibles en escenarios como operativos de inteligencia, y demás, haciendo énfasis en aquellos desafíos a los que se enfrenta la Ley 1581 de 2012 de cada a los requerimientos específicos del sector defensa.(p.41) En esta misma línea, (Peña, 2023) subraya que las Fuerzas Militares enfrentan grandes retos en materia de ciberseguridad, lo que requiere no solo infraestructura tecnológica, sino también una sólida normativa para proteger la información crítica en entornos cada vez más vulnerables a ataques cibernéticos. (p.15)

No obstante, desde la perspectiva de (Rojas, 2014), dentro del sistema jurídico colombiano se avizoran serios vacíos en relación con la protección del habeas data, lo cual tiene una relación directa con la información sensible que se maneja las fuerzas militares, requiriendo una normatividad eficaz y adaptable a los estándares internacionales. En efecto, (Quiñones, 2022) argumenta esta teoría, asegurando que el país ha venido avanzado significativamente en esta materia, pero que aun, persisten brechas en la implementación práctica de la ley, especialmente en sectores donde la información tiene connotaciones

estratégicas. Asimismo, (Miranda, 2023)hace especial énfasis en que la normatividad colombiana, si bien es robusta en la materia, tratándose de datos sensibles, como aquellos que se manejan en el ámbito militar, sería muy importante que se reforzara la protección. (p.55)

Otras perspectivas, hacen una lectura crítica y tecnológica. (Machuca, Vinueza, Sampedro, & Santillán, 2022), advierten que en Colombia, requiere formular y diseñar sistemas informáticos robustos que sirvan para la gestión de datos personales, especialmente en ámbitos como el militar, debido a la categoría de la información que manejan en sus operaciones. (p. 12) En la misma línea, (Zárate, 2020), considera que es preciso enfocarse en una modificación del régimen normativo, permitiendo que se garantice el cumplimiento de principios como la confidencialidad, seguridad y circulación restringida de la información, aspectos esenciales en contextos militares. (p.41) A su vez, (Martínez, 2019)) plantea que tecnologías emergentes como la inteligencia artificial y el big data deben ser abordadas con criterios éticos y normativos, pues su aplicación indiscriminada puede vulnerar derechos fundamentales.

Ahora bien, hay que decir, que otro de los aspectos determinantes en el ámbito del tratamiento de datos personales, tiene que ver con el consentimiento. Al respecto, (Polo, 2020), considera que este mismo, es un elemento estructural y axial en el tratamiento de datos personales, pero también constituye una debilidad cuando no se adapta a contextos complejos como el militar. Finalmente, la investigación de (Londoño, 2021) evidencia que incluso tecnologías comunes como las cookies pueden vulnerar el principio de transparencia si no se ajustan adecuadamente a la normativa vigente, lo cual sugiere una lectura crítica sobre el uso

de cualquier tecnología en instituciones que manejan información personal de alto valor estratégico. (p.15)

A partir de lo expuesto, hay que deducir que existen previos estudios que han podido determinar la necesidad de formular un marco normativo, más completo e integral en materia de protección de datos personales, en el ámbito militar. Pues bien, tal como se ha propuesto en este objetivo, se plantea identificar el marco normativo enfocado en la protección de datos personales. En primera medida, es importante contextualizar las disposiciones de la Ley 1581 de 2012, que reconoce los principios, derechos y procedimientos aplicables al tratamiento de datos en el país. En la misma, se reconoce el rol significativo e importante de la protección del habeas data y define parámetros para el tratamiento de datos sensibles, incluyendo aquellos relacionados con la salud, la orientación política o la pertenencia a organizaciones, aspectos particularmente relevantes en contextos militares. Esta norma, tiene una ventaja excepcional, y es que promueve la protección de datos personales, de forma general, aplicable tanto en el sector privado, como en el público, incluyéndose excepciones para casos relacionados con la seguridad nacional y la defensa, permitiendo el tratamiento de datos personales sin consentimiento del titular cuando se justifique bajo estas circunstancias. Esto implica una flexibilidad normativa que, aunque funcional para la operatividad del Ejército Nacional, también abre la puerta a riesgos de vulneración de derechos fundamentales por falta de límites claros y control efectivo sobre las actividades de inteligencia y contrainteligencia.

Por su parte, en el ámbito de las fuerzas armadas, y especialmente del Ejercito Nacional, se han expedido normativas como la Directiva 003 de 2019, como una herramienta

para la armonización de las actividades ejecutadas por las Fuerzas Militares, bajo los parámetros de la Ley 1581 de 2012. En la misma, se avizoran una serie de orientaciones internas para la gestión del habeas data, incluyendo pautas sobre la recolección, almacenamiento, uso y supresión de datos personales. De la misma manera, se hace una designación de oficiales de protección de datos y la adopción de protocolos institucionales para la atención de solicitudes de los titulares. Sin embargo, su alcance es limitado debido a su naturaleza no legislativa, lo que significa que carece de obligatoriedad frente a posibles omisiones o incumplimientos, y no contempla sanciones específicas ni mecanismos de supervisión externa.

Sin embargo, no se puede desconocer que ante la existencia de este tipo de instrumentos, el Ejército Nacional presenta dificultades estructurales en la implementación efectiva del régimen de protección de datos. Las investigaciones y análisis académicos han evidenciado una aplicación desigual de las políticas de protección, una baja capacitación del personal sobre las obligaciones legales, y fallas en la trazabilidad y seguridad de las bases de datos utilizadas en operaciones militares. Estas deficiencias se agravan ante la ausencia de una regulación clara y específica para los sistemas de inteligencia y la falta de control independiente sobre estas actividades, lo que deja un vacío legal preocupante frente al principio de legalidad y al derecho a la intimidad.

Desafíos éticos y tecnológicos que enfrenta el Ejército Nacional en la recolección, almacenamiento y uso de datos personales, considerando los principios de seguridad, privacidad y transparencia.

En un contexto donde las tecnologías de la información y la comunicación han transformado radicalmente la forma en que se recopila, almacena y utiliza la información, la protección de los datos personales se ha convertido en una necesidad urgente, especialmente en instituciones como el Ejército Nacional, que por su naturaleza estratégica maneja datos altamente sensibles. La gestión de esta información plantea múltiples desafíos, no solo desde el punto de vista técnico, sino también desde una perspectiva ética y jurídica, en la que se entrecruzan principios fundamentales como la seguridad, la privacidad y la transparencia. A continuación, se detallan los principales desafíos enfrentados:

Tensión entre derechos fundamentales y necesidades operativas de defensa

Uno de los desafíos más complejos que enfrenta el Ejército Nacional de Colombia en la gestión de datos personales es la tensión estructural entre la garantía de los derechos fundamentales particularmente el derecho a la intimidad, al habeas data y a la autodeterminación informativa y las necesidades estratégicas de defensa y seguridad nacional. Esta tensión se manifiesta en múltiples niveles: normativo, operativo, ético y práctico, y constituye un campo de fricción constante entre el interés público y la protección de la esfera privada del individuo.

En el contexto militar, dicha autorización suele no materializarse plenamente, especialmente en situaciones relacionadas con actividades de inteligencia, operaciones tácticas, control de zonas geoestratégicas o gestión de recursos humanos. La seguridad nacional, invocada como fundamento para el acceso a información sin consentimiento, opera como una excepción que en la práctica se ha naturalizado como regla. Esta excepcionalidad permanente, si no está sujeta a estrictos controles, puede llevar a vulneraciones sistemáticas del derecho a la intimidad y al uso desproporcionado de información personal sin garantías de legalidad, necesidad o proporcionalidad.

En este sentido, organismos como el Comité de Derechos Humanos de las Naciones Unidas han reiterado que cualquier restricción al derecho a la privacidad debe estar prevista en la ley, responder a una necesidad imperiosa y ser proporcional al objetivo legítimo perseguido (Observación General N. º 16, 1988). La Corte Constitucional colombiana también ha señalado que el derecho a la intimidad no puede ser suspendido arbitrariamente, ni siquiera bajo argumentos de seguridad nacional (Sentencia C-748 de 2011). Por tanto, se requiere que el Ejército Nacional implemente mecanismos que equilibren el interés de defensa con el respeto a los derechos fundamentales, mediante el principio de proporcionalidad como criterio de análisis normativo y operativo.

Además, la falta de delimitación clara entre los datos personales de carácter sensible (como afiliaciones políticas, religiosas, étnicas o de salud) y los datos necesarios para fines militares, genera un riesgo adicional de discriminación, estigmatización y uso indebido de la información, sobre todo en territorios históricamente afectados por el conflicto armado, donde el Ejército ha tenido una fuerte presencia. La recopilación de datos sin una justificación

transparente puede reforzar prácticas de control social y vigilancia que desbordan los límites de la legalidad democrática.

Otro aspecto relevante es que, en muchas ocasiones, los procedimientos de inteligencia no cuentan con protocolos diferenciados que permitan evaluar el impacto sobre los derechos de los titulares, ni con estándares claros de minimización y temporalidad en la conservación de los datos. La ausencia de un plazo definido para la eliminación o anonimización de la información recolectada perpetúa el riesgo de uso posterior para fines distintos a los inicialmente previstos, lo que contradice el principio de finalidad establecido en el artículo 4 de la Ley 1581 de 2012.

Por ello, la tensión entre la protección de derechos fundamentales y las necesidades operativas del Ejército no puede resolverse a favor de una lógica de excepción permanente, sino que debe abordarse a través de mecanismos institucionales de autorregulación, control judicial y vigilancia externa, que aseguren que toda actuación estatal en materia de datos personales sea legal, legítima y respetuosa del orden constitucional. En este escenario, se vuelve indispensable que el Ejército Nacional adopte políticas internas estrictas sobre consentimiento informado, segmentación de datos sensibles, protocolos de minimización y eliminación de información, y medidas de compensación frente a posibles abusos.

Riesgos de vigilancia masiva y perfilamiento sin control

El segundo gran desafío que enfrenta el Ejército Nacional en la recolección y tratamiento de datos personales es el riesgo creciente de que estas actividades deriven en prácticas de vigilancia masiva, perfilamiento indebido y uso arbitrario de la información sin controles eficaces, lo cual representa una amenaza directa al ejercicio de los derechos

fundamentales de los ciudadanos, en especial el derecho a la intimidad, la no discriminación, el debido proceso y la autodeterminación informativa.

La vigilancia masiva se define como el monitoreo sistemático y constante de grandes grupos poblacionales mediante tecnologías que permiten recolectar, almacenar, analizar y cruzar datos personales sin el consentimiento informado de los titulares ni criterios claros de legalidad, necesidad o proporcionalidad. En el contexto colombiano, este riesgo se agrava en zonas rurales o periféricas, donde históricamente han coexistido estructuras armadas ilegales, pobreza estructural y presencia intermitente del Estado. En dichos territorios, el Ejército Nacional ha desarrollado operaciones que implican la recolección masiva de información de comunidades enteras, a través de formularios de caracterización poblacional, patrullajes con dispositivos de geolocalización, toma de fotografías, huellas dactilares y uso de cámaras corporales o drones con sistemas de reconocimiento facial. Si bien muchas de estas acciones se justifican en nombre del orden público, la ausencia de protocolos diferenciados, regulación específica y supervisión independiente transforma un mecanismo de seguridad en una práctica de vigilancia no consentida.

Esta problemática se intensifica con el uso de tecnologías que permiten el perfilamiento automatizado de personas, es decir, la construcción de categorías, patrones o niveles de riesgo a partir de variables como antecedentes penales, ubicación geográfica, redes sociales, afinidades ideológicas, etnia, edad o sexo. Estas herramientas, generalmente derivadas del análisis algorítmico o el big data, pueden conducir a estigmatizaciones indebidas, decisiones automatizadas y discriminaciones estructurales, especialmente si operan con datos incompletos, descontextualizados o sesgados.

El perfilamiento en el ámbito militar, cuando se realiza sin control judicial o sin mecanismos de rendición de cuentas, contradice principios constitucionales como la igualdad ante la ley, el respeto por la dignidad humana y la presunción de inocencia. Además, vulnera directamente lo dispuesto en el artículo 4 de la Ley 1581 de 2012, que establece los principios de finalidad, necesidad, proporcionalidad y veracidad como límites al tratamiento de datos. Según este marco normativo, los datos personales no pueden utilizarse para fines distintos a los autorizados, ni mantenerse indefinidamente si no existe una justificación legal.

Un aspecto crítico de este desafío es la asimetría informativa entre la institución militar y la población civil. En muchas ocasiones, las personas objeto de vigilancia o perfilamiento no saben que sus datos han sido recolectados ni tienen acceso a mecanismos efectivos de reclamo, corrección o supresión, lo que viola el derecho fundamental al habeas data. Además, no existen criterios claros sobre quién autoriza, supervisa y limita el acceso a esta información, ni garantías sobre su seguridad, conservación o eliminación.

Esta situación se vuelve aún más preocupante si se considera la historia reciente de abusos institucionales en Colombia, como los casos de perfilamientos ilegales realizados por organismos de inteligencia militar o la recopilación indebida de información de líderes sociales, defensores de derechos humanos y periodistas. Tales antecedentes evidencian la fragilidad de los controles internos y el riesgo de instrumentalización de los datos personales con fines políticos, represivos o extralegales.

Débil implementación del principio de transparencia

La transparencia es uno de los principios fundamentales del régimen de protección de datos personales, consagrado en el artículo 4 de la Ley Estatutaria 1581 de 2012. Según este principio, los titulares de la información deben poder conocer con claridad, veracidad y

oportunidad quién recolecta sus datos, con qué finalidad, bajo qué condiciones, por cuánto tiempo se conservarán y cómo pueden ejercer sus derechos. Sin embargo, en el contexto militar colombiano, este principio enfrenta serias limitaciones en su implementación real y efectiva, lo que configura un tercer gran desafío para el Ejército Nacional.

La Directiva Permanente N.° 003 de 2019 del Ejército Nacional, expedida para armonizar las obligaciones de la Ley 1581 de 2012 con las necesidades operativas de la institución, constituye un primer esfuerzo por incorporar la transparencia como parte de las prácticas administrativas internas. No obstante, esta directiva posee un carácter meramente orientador, sin fuerza normativa vinculante ni mecanismos de control externo o sanción por su incumplimiento. Además, no incluye parámetros verificables de cumplimiento, indicadores de gestión, ni un protocolo uniforme que asegure su aplicación en todas las unidades militares del país.

La ausencia de un marco operativo que haga exigible el principio de transparencia genera varios problemas críticos:

Desconocimiento del titular sobre el uso de su información: en la mayoría de los casos, los ciudadanos y en muchas ocasiones, los propios miembros del Ejército no son informados de manera clara y oportuna sobre la recolección, tratamiento y finalidad de los datos personales que se almacenan en bases de datos militares. Esto ocurre, por ejemplo, en los procesos de reclutamiento, ascensos, procesos disciplinarios internos, atención médica institucional o recolección de datos biométricos en zonas de presencia militar. (Castañeda, Lopez, & Camacho, 2019)

Inaccesibilidad de la información: no existen canales institucionales claramente identificados para que los titulares puedan consultar el uso de su información, solicitar

correcciones o ejercer sus derechos de habeas data. La página web oficial del Ejército Nacional no contiene un enlace directo ni visible para estos trámites, ni ofrece formatos estandarizados de solicitud o tiempos de respuesta definidos. Además, muchas dependencias operan en entornos cerrados al público, lo que limita el acceso físico o electrónico a la información.

Falta de mecanismos de rendición de cuentas: la transparencia implica no solo informar, sino también permitir que terceros como organismos de control, jueces o la ciudadanía puedan auditar, evaluar o cuestionar las prácticas institucionales de tratamiento de datos. En el caso del Ejército, los sistemas de información y bases de datos están en gran medida exentos de vigilancia por parte de la Superintendencia de Industria y Comercio, autoridad nacional en materia de protección de datos, debido al carácter reservado de muchas de sus actividades. Esto genera un vacío institucional, donde no hay contrapeso externo efectivo que verifique el cumplimiento del principio de transparencia.

Ambigüedad entre reserva y opacidad: si bien es legítimo que determinadas operaciones militares o actividades de inteligencia se clasifiquen como reservadas por razones de seguridad nacional, esta reserva no puede extenderse automáticamente a todos los procesos administrativos o de gestión documental del Ejército. Sin embargo, la práctica institucional tiende a exagerar el uso de la clasificación reservada, lo que encubre procesos ineficientes o irregulares bajo la excusa de la confidencialidad operativa.

Desconfianza ciudadana y erosión institucional: la falta de transparencia en el tratamiento de datos no solo vulnera derechos individuales, sino que afecta la legitimidad y credibilidad de las Fuerzas Militares ante la sociedad. En un contexto como el colombiano, marcado por el conflicto armado, la violencia institucional y el uso político de los aparatos

de seguridad, el respeto por el principio de transparencia es esencial para reconstruir la confianza pública y evitar la instrumentalización de la información personal como herramienta de control o represión.

En Colombia, la Ley 1712 de 2014, conocida como Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, obliga a todas las entidades públicas, incluidas las del sector defensa, a publicar y mantener actualizada información mínima obligatoria, incluyendo el tratamiento de datos personales, presupuesto, estructura orgánica y manual de procedimientos. No obstante, el Ejército Nacional aún no ha adaptado completamente esta normativa a sus procesos internos, lo que se traduce en bajos niveles de cumplimiento y escasa interoperabilidad con otros sistemas de información del Estado.

Fragmentación tecnológica e infraestructura obsoleta

Uno de los principales obstáculos que enfrenta el Ejército Nacional en la gestión eficiente y segura de los datos personales es la fragmentación de su infraestructura tecnológica y el uso de sistemas de información obsoletos, desarticulados y sin interoperabilidad. Este problema estructural se traduce en una administración deficiente de los datos, mayores riesgos de violaciones a la seguridad de la información y un incumplimiento sistemático de los principios establecidos en la Ley 1581 de 2012, particularmente los principios de seguridad, circulación restringida y veracidad.

A diferencia de entidades públicas civiles que han avanzado en procesos de transformación digital e interoperabilidad institucional (por ejemplo, el sistema de interoperabilidad de datos entre la Registraduría, la Dian y la Policía Nacional), el Ejército Nacional presenta un panorama caracterizado por:

Sistemas fragmentados y no interoperables: Muchas unidades militares utilizan plataformas informáticas propias, aisladas o desarrolladas de forma artesanal, que no se comunican entre sí ni con otras entidades del Estado. Esta situación impide la consolidación de un sistema centralizado de información, lo que dificulta el control del ciclo de vida de los datos personales: desde su recolección y actualización hasta su conservación o supresión.

Uso de software desactualizado o sin mantenimiento: La infraestructura tecnológica del Ejército Nacional, en varias regiones del país, sigue operando con sistemas de gestión de información obsoletos, sin soporte técnico ni actualizaciones de seguridad. Esto aumenta considerablemente la exposición a fallos de funcionamiento, pérdida de información, errores en la trazabilidad de los datos y vulnerabilidades ante ciberataques o accesos indebidos.

Ausencia de políticas de estandarización de bases de datos: No existen políticas unificadas para la creación, administración y depuración de las bases de datos institucionales, lo que da lugar a registros duplicados, inconsistentes o incompletos. Esta deficiencia compromete la calidad de la información, afectando tanto a los procesos administrativos internos como al tratamiento justo y legal de los datos personales de terceros.

Débil implementación de protocolos de gestión documental electrónica: Aunque Colombia ha avanzado en normativas como el Decreto 620 de 2020 sobre gestión documental y archivos digitales, el Ejército Nacional no ha adoptado plenamente estos estándares. En consecuencia, muchos documentos que contienen datos personales (historias laborales, registros médicos, hojas de vida, procedimientos disciplinarios) siguen siendo manejados en papel, escaneados sin criterios técnicos o almacenados en carpetas compartidas sin control de acceso.

La situación también impacta negativamente en la capacidad de supervisión interna, pues al no contar con un sistema unificado, la trazabilidad de las operaciones sobre las bases de datos (quién accede, cuándo, con qué finalidad) es prácticamente inexistente o se registra manualmente, lo cual impide detectar posibles abusos, mal uso o filtraciones de datos.

Este desafío es particularmente grave en el contexto del uso de tecnologías emergentes. Por ejemplo, la adopción de soluciones de inteligencia artificial o reconocimiento facial en sistemas de seguridad perimetral o patrullajes con drones exige una infraestructura digital sólida, segura e integrada, capaz de almacenar grandes volúmenes de información sensible con criterios de protección de datos desde el diseño (privacy by design). En ausencia de esta base tecnológica, cualquier innovación corre el riesgo de operar en un vacío normativo y técnico, amplificando las vulnerabilidades existentes.

A nivel institucional, la falta de inversión en modernización tecnológica dentro del sector defensa en contraste con la asignación de recursos para operaciones o armamento— ha generado un rezago estructural en materia de transformación digital, ciberseguridad y gobernanza de datos. Pese a que el Ministerio de Defensa Nacional ha formulado documentos como el Plan Estratégico Sectorial TIC o los lineamientos de ciberdefensa, estos no se han traducido en acciones concretas dentro del Ejército Nacional, y no existe una estrategia de largo plazo orientada específicamente al tratamiento responsable de datos personales.

El análisis de los desafíos éticos y tecnológicos que enfrenta el Ejército Nacional en relación con la recolección, almacenamiento y uso de datos personales pone de manifiesto una tensión persistente entre las exigencias constitucionales de protección de los derechos fundamentales y las dinámicas institucionales propias del sector defensa. A pesar de la existencia de un marco legal robusto, como la Ley Estatutaria 1581 de 2012, y de

instrumentos administrativos como la Directiva Permanente N.º 003 de 2019, la realidad demuestra que su aplicación efectiva resulta limitada, fragmentada y, en muchos casos, simbólica.

En primer lugar, la garantía de los derechos a la intimidad, al habeas data y a la autodeterminación informativa suele entrar en conflicto con las necesidades operativas y de inteligencia militar, lo que ha generado una cultura institucional en la que la excepción se convierte en regla. Esta práctica, justificada bajo el argumento de la seguridad nacional, da lugar a tratamientos de datos sin consentimiento, sin control judicial ni criterios claros de legalidad, necesidad o proporcionalidad, afectando particularmente a poblaciones vulnerables o ubicadas en zonas con alta presencia militar.

A ello se suma el riesgo creciente de que las tecnologías disponibles, muchas veces implementadas sin regulación específica, propicien escenarios de vigilancia masiva, perfilamiento automatizado y uso arbitrario de la información. El principio de transparencia, esencial para legitimar cualquier tratamiento de datos personales, se ve seriamente debilitado por la inexistencia de canales efectivos para el ejercicio de los derechos de los titulares, la ambigüedad entre la reserva legítima y la opacidad institucional, y la falta de mecanismos de rendición de cuentas y supervisión externa.

Desde el punto de vista técnico, el Ejército Nacional enfrenta serias limitaciones estructurales derivadas de la fragmentación de sus sistemas de información, la ausencia de interoperabilidad entre plataformas, el uso de tecnologías obsoletas y la inexistencia de políticas estandarizadas de gestión documental. Esta situación compromete no solo la calidad de la información almacenada, sino también la seguridad de los datos personales, al no contar con medidas de protección robustas ni trazabilidad adecuada de los accesos y modificaciones.

El rezago en materia de ciberseguridad constituye, además, un riesgo transversal que expone a la institución frente a filtraciones, hackeos y vulneraciones sistemáticas de la información sensible. Las bases de datos militares, correos electrónicos y redes de comunicación carecen de protocolos obligatorios de cifrado, autenticación o monitoreo continuo, lo que pone en entredicho la capacidad real del Ejército para cumplir con los principios de seguridad establecidos en la Ley 1581 de 2012. A ello se suma la limitada formación del personal en buenas prácticas de protección de datos, así como la inexistencia de una cultura organizacional orientada al respeto del habeas data como parte del cumplimiento de los derechos humanos.

Recomendaciones para fortalecer el marco normativo y garantizar un la protección de datos en el Ejército Nacional a partir de la implementación de la directiva 003 de 2019

El tercer objetivo de esta investigación se enfocó en formular un conjunto de recomendaciones orientadas a mejorar el tratamiento de datos personales dentro del Ejército Nacional, partiendo del análisis crítico de la Directiva Permanente N.º 003 de 2019. A partir de allí, se plantean las siguientes recomendaciones:

Institucionalización de una cultura de protección de datos personales en el Ejército Nacional

Uno de los pilares fundamentales para garantizar una protección efectiva de los datos personales en el Ejército Nacional es la consolidación de una cultura organizacional que comprenda, respete y priorice el derecho fundamental al habeas data. Esta recomendación surge de un diagnóstico claro: la Directiva Permanente N.º 003 de 2019, aunque representa un avance jurídico significativo, no ha sido acompañada por procesos formativos,

pedagógicos ni estratégicos de apropiación institucional, lo que limita su aplicación práctica y reduce su impacto transformador dentro de la institución castrense.

En efecto, los desafíos identificados en la implementación de la directiva muestran que existe un bajo nivel de conocimiento técnico y jurídico sobre el tratamiento adecuado de datos personales entre el personal militar y civil. Esta falta de apropiación no es menor, ya que puede derivar en tratamientos ilegales, negligentes o arbitrarios de información sensible, afectando tanto los derechos fundamentales de los titulares como la legitimidad y credibilidad del Ejército frente a la ciudadanía. La ausencia de una cultura de protección de datos también perpetúa prácticas informales, la desatención de protocolos y el desconocimiento de las consecuencias legales derivadas de las vulneraciones al régimen de habeas data.

En este sentido, se propone como primera acción el diseño e implementación de un programa de formación y capacitación obligatorio, permanente y transversal, que abarque todos los niveles jerárquicos, especialidades y unidades del Ejército Nacional. Este programa debe estructurarse bajo una perspectiva integral, abordando los aspectos:

Normativos, con énfasis en la Constitución Política, la Ley 1581 de 2012, el Decreto 1377 de 2013, la Directiva 003 de 2019, y otras normas complementarias como el Código Penal (arts. 269F y 269G sobre delitos informáticos).

Técnicos, relacionados con buenas prácticas en la recolección, clasificación, almacenamiento, transmisión, supresión y auditoría de datos.

Éticos, para consolidar una conciencia institucional basada en el respeto a la dignidad humana, la intimidad y la seguridad jurídica de los ciudadanos y de los propios miembros de las Fuerzas Militares.

La metodología pedagógica debe priorizar el aprendizaje práctico, el análisis de casos reales y la simulación de incidentes de seguridad que permitan al personal comprender los riesgos asociados al uso indebido de los datos. Esta formación no debe ser esporádica ni puntual, sino que debe estar integrada en los planes curriculares de las escuelas de formación militar y civil, en los programas de actualización profesional, y en las inducciones para el personal nuevo.

Además, se recomienda el diseño e implementación de campañas internas de concientización institucional orientadas a reforzar el respeto por la privacidad como un valor castrense. Estas campañas deben ir más allá de la formación técnica e incluir componentes comunicativos, visuales y simbólicos que integren el respeto por los datos personales como parte del ethos institucional. Slogans como "Proteger la información es proteger la vida", o "La seguridad empieza por el respeto a los datos", podrían ser integrados en cartelería, videos institucionales, manuales de operaciones, redes internas y procesos de evaluación de desempeño.

Para garantizar sostenibilidad, se requiere también la asignación de recursos institucionales y presupuestales específicos para el desarrollo de estas estrategias, así como la definición de metas de cobertura, periodicidad, evaluación y mejora continua. La institucionalización de una cultura de protección de datos no puede depender de voluntades personales o liderazgos coyunturales, sino que debe convertirse en una política pública militar, con respaldo legal, directivo y operativo.

Creación de una unidad especializada en protección de datos personales en el Ejército Nacional

La creación de una unidad especializada y autónoma en protección de datos personales dentro del Ejército Nacional constituye una medida indispensable para fortalecer la implementación efectiva de la Directiva Permanente N.º 003 de 2019 y del régimen normativo previsto por la Ley 1581 de 2012. Esta recomendación parte del reconocimiento de que el volumen, la sensibilidad y la criticidad de la información manejada por la institución militar supera con creces la capacidad de los esquemas de control actualmente existentes, los cuales suelen estar dispersos, subordinados a funciones operativas y carentes de experticia técnica y jurídica específica en la materia.

A diferencia de las áreas jurídicas convencionales o de los departamentos de tecnología, una unidad especializada en protección de datos tendría como propósito exclusivo diseñar, coordinar y supervisar la política interna de tratamiento de información personal, garantizando que el Ejército Nacional actúe conforme a los principios de legalidad, finalidad, libertad, veracidad, seguridad, acceso y circulación restringida, y confidencialidad. Su existencia permitiría cerrar brechas estructurales en materia de cumplimiento normativo y disminuir los riesgos institucionales frente a demandas, sanciones, filtraciones o abusos en el manejo de información sensible.

Esta unidad debe tener un grado de autonomía técnica y estar adscrita directamente al más alto nivel de la estructura administrativa del Ejército (por ejemplo, al Comando General o al Inspector General), a fin de evitar subordinaciones jerárquicas que puedan comprometer su independencia funcional. Además, debe contar con personal altamente calificado y multidisciplinario, con formación en derecho constitucional, derecho informático, ciberseguridad, gestión documental, archivística, administración pública y gestión del riesgo.

Adicionalmente, esta unidad deberá desempeñar un rol estratégico en la revisión, formulación y actualización de la política interna de protección de datos, garantizando su armonización con los avances normativos, las recomendaciones internacionales y las nuevas tecnologías emergentes que impactan el tratamiento de información (por ejemplo, inteligencia artificial, biometría, big data, geolocalización o vigilancia digital).

Desde una perspectiva organizacional, esta unidad también podría liderar la creación de una red institucional de oficiales de protección de datos (OPD), designados en cada comando, batallón o dependencia, con funciones operativas de implementación y control local. Esta estrategia facilitaría la descentralización de la política de protección de datos y permitiría mayor capilaridad en la gestión de riesgos y en la sensibilización del personal en todo el territorio nacional.

En suma, la creación de una unidad especializada no es un lujo administrativo, sino una necesidad institucional urgente para enfrentar los desafíos contemporáneos del Ejército Nacional en materia de información personal. La existencia de esta estructura permitiría consolidar una política de protección de datos sistemática, eficaz y coherente con los estándares nacionales e internacionales, contribuyendo al fortalecimiento del Estado de Derecho, al respeto por los derechos humanos y a la legitimidad del sector defensa en el marco de una democracia constitucional.

Revisión, actualización y armonización del marco normativo interno en materia de protección de datos personales

La necesidad de revisar, actualizar y armonizar el marco normativo interno del Ejército Nacional en lo que respecta al tratamiento de datos personales se presenta como una acción urgente para garantizar coherencia jurídica, eficacia institucional y seguridad jurídica

en la aplicación de la Directiva Permanente N.º 003 de 2019. La existencia de normas dispersas, contradictorias o desactualizadas, sumada a la falta de una reglamentación interna unificada, genera vacíos interpretativos, debilita los mecanismos de control y aumenta el riesgo de prácticas institucionales incompatibles con los estándares legales y constitucionales.

Actualmente, el Ejército Nacional no cuenta con un reglamento interno específico y completo que regule de manera sistemática el tratamiento de datos personales, especialmente en lo relacionado con el ciclo completo de gestión de la información (recolección, uso, almacenamiento, circulación, supresión, archivo y destrucción). Esta ausencia normativa limita la capacidad de aplicación efectiva de la Ley 1581 de 2012, obstaculiza la labor de los oficiales encargados de protección de datos y restringe el ejercicio de los derechos de los titulares de la información.

En este contexto, se recomienda la elaboración y adopción de un Reglamento Interno de Protección de Datos Personales del Ejército Nacional, con fundamento en los artículos 15 y 20 de la Constitución Política de Colombia, en la Ley Estatutaria 1581 de 2012 y en sus decretos reglamentarios (especialmente el Decreto 1377 de 2013 y el Decreto 886 de 2014). Este reglamento debe contar con fuerza vinculante y ser obligatorio para todas las dependencias, unidades operativas y niveles jerárquicos de la institución. Su redacción debe ser clara, técnica y contextualizada a la realidad militar, y su aplicación debe estar respaldada por mecanismos sancionatorios y de control disciplinario.

Entre los contenidos esenciales que debería incluir este reglamento interno se destacan:

Definiciones claras y adaptadas al contexto castrense sobre datos personales, datos sensibles, datos clasificados, datos operacionales, datos biométricos, y sistemas de información.

Principios rectores del tratamiento de datos personales dentro del Ejército Nacional, incluyendo los de legalidad, finalidad, libertad, seguridad, veracidad, circulación restringida, necesidad, proporcionalidad y confidencialidad.

Estándares técnicos mínimos exigibles para la recolección, almacenamiento, circulación y supresión de información, incluyendo el uso de protocolos de seguridad, medidas de cifrado, trazabilidad de accesos y auditorías.

Procedimientos obligatorios para la autorización, rectificación, cancelación y oposición por parte de los titulares de los datos (ARCO), conforme lo establece el artículo 8 de la Ley 1581 de 2012.

Disposiciones específicas sobre el tratamiento de datos sensibles, incluidos datos de salud, afiliación sindical, religión, orientación sexual o información genética, así como datos biométricos y georreferenciados.

Normas sobre el uso de tecnologías emergentes en contextos operativos (por ejemplo, inteligencia artificial, reconocimiento facial, sistemas de vigilancia masiva, etc.) y sus límites frente al principio de legalidad y necesidad.

Reglas para la conservación, archivo y destrucción de bases de datos personales, con especial énfasis en la información recolectada durante operaciones militares, tareas de inteligencia o actividades administrativas.

Protocolos de respuesta ante incidentes de seguridad de la información y mecanismos de comunicación con autoridades externas, como la Superintendencia de Industria y Comercio.

La formulación de este reglamento debe realizarse mediante una mesa técnica interinstitucional, integrada por representantes del Comando General, asesores jurídicos, expertos en ciberseguridad, oficiales en ejercicio, personal de archivo y delegados de la Superintendencia de Industria y Comercio, a fin de garantizar su calidad normativa y su aplicabilidad práctica. Igualmente, debe estar sujeto a un proceso periódico de evaluación y actualización, conforme evolucione el entorno tecnológico, operativo y legal.

Además de la expedición del reglamento, se sugiere realizar una revisión jurídica integral del conjunto de normas internas y manuales operativos que regulan directa o indirectamente el uso de información personal, con el propósito de identificar contradicciones, redundancias o vacíos normativos. Esta armonización no solo contribuirá a prevenir conflictos de interpretación, sino que fortalecerá la articulación entre las normas militares y el ordenamiento jurídico nacional en materia de derechos fundamentales.

En suma, el diseño de un marco normativo interno coherente, específico y actualizado es una condición esencial para garantizar que el Ejército Nacional cumpla efectivamente con su obligación constitucional de respetar y proteger los datos personales de todos los individuos, sin que ello menoscabe sus funciones estratégicas ni comprometa la seguridad nacional. Este equilibrio entre operatividad y legalidad es uno de los grandes retos contemporáneos para cualquier institución armada que actúe en el marco de un Estado social y democrático de derecho.

Las tres recomendaciones formuladas la institucionalización de una cultura de protección de datos, la creación de una unidad especializada y la revisión normativa interna representan el núcleo estructural para consolidar un sistema sólido, coherente y eficaz de gestión de datos personales en el Ejército Nacional de Colombia. Estas propuestas no son independientes ni aisladas, sino profundamente interdependientes y complementarias, en tanto configuran los tres pilares de una arquitectura institucional robusta: cultura, estructura y norma.

Conclusiones

En primer lugar, el análisis del marco normativo evidenció que, si bien existe una estructura legal que regula el tratamiento de datos personales, esta no es suficientemente específica ni adaptable a las particularidades del sector defensa. La Directiva 003 de 2019 carece de carácter vinculante y no contempla mecanismos eficaces de supervisión, seguimiento y sanción, lo cual debilita su capacidad para operar como un instrumento regulador robusto. Además, la ausencia de una legislación sectorial especializada para las Fuerzas Militares limita el alcance y la efectividad del actual régimen de protección de datos.

En segundo lugar, el Ejército Nacional enfrenta desafíos sustantivos en materia ética y tecnológica. Desde el punto de vista ético, se presentan tensiones constantes entre las exigencias de seguridad nacional y los principios constitucionales de legalidad, proporcionalidad, necesidad y transparencia. El uso de tecnologías como la biometría, la inteligencia artificial o los sistemas de geolocalización, sin un marco regulador claro, incrementa los riesgos de prácticas discriminatorias, invasivas o arbitrarias, que afectan no solo a civiles, sino también a miembros activos y retirados de la institución. Desde el plano tecnológico, la fragmentación de los sistemas de información, la falta de protocolos

unificados, el escaso nivel de interoperabilidad y las debilidades en ciberseguridad comprometen seriamente la integridad, confidencialidad y disponibilidad de los datos.

En tercer lugar, se identificó una débil apropiación institucional de la cultura de protección de datos personales. La formación del personal es deficiente y no existen campañas sostenidas de sensibilización o programas de capacitación permanentes que fortalezcan la ética del tratamiento de la información. Esto se traduce en prácticas inadecuadas de recolección, almacenamiento y acceso a los datos, así como en una baja capacidad de respuesta ante incidentes de seguridad.

En suma, garantizar la protección efectiva de los datos personales en el ámbito militar no solo es una obligación jurídica derivada del bloque de constitucionalidad y los estándares internacionales, sino una condición estratégica para preservar la legitimidad institucional, la confianza ciudadana y el equilibrio entre seguridad y derechos fundamentales. El Ejército Nacional debe avanzar hacia un modelo de gobernanza de datos que priorice la ética, la legalidad y la innovación, entendiendo que la protección de la información personal no es incompatible con la defensa nacional, sino que es parte integral de una democracia sólida y moderna.

Referencias

Álvarez, C. M. (2018). *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital.* Premio de Investigación de la Cátedra Google sobre Privacidad, Sociedad e Innovación de la Universidad CEU-San Pablo de Madrid. Obtenido de https://www.uexternado.edu.co/wp-content/uploads/2024/02/10-ANOS-DE-LA-LEY-DE-PROTECCION-DE-DATOS-1.pdf

Bernal, H. J. (2022). *La protección de datos personales de los miembros de las Fuerzas Militares de Colombia en el cumplimiento de trabajos misionales.* Escuela Superior de Guerra "General Rafael Reyes Prieto. Obtenido de https://www.esdegrepositorio.edu.co/handle/20.500.14205/11099

Cabezas, A. J. (2023). Tratamiento de datos personales y compliance en Colombia. *Revista De La Facultad De Derecho Y Ciencias Políticas*. Obtenido de https://doi.org/10.18566/rfdcp.v53n138.a2

Calle, D. S. (2009). Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de hábeas data en Colombia. *Revista Jurídica*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=9015856

Galvis, C. L., & Pesca, M. D. (2020). *Límites del tratamiento de los datos personales en el ámbito laboral frente al uso de las tecnologías de la información y comunicación en la era digital.* Obtenido de https://doi.org/10.15332/25005286.5482

Londoño, C. A. (2021). *Tratamiento de datos personales a través de web cookies: Análisis bajo la legislación colombiana de protección de datos personales.* Universidad de los

Andes. Obtenido de https://repositorio.uniandes.edu.co/server/api/core/bitstreams/f68935fe-ed9c-42b4-88d5-e5865411ff00/content

Machuca, V. S., Vinueza, O. N., Sampedro, G. C., & Santillán, M. A. (2022). *Habeas data y protección de datos personales en la gestión de las bases de datos.* Universidad y Sociedad. Obtenido de https://rus.ucf.edu.cu/index.php/rus/article/view/2698

Martínez, D. A. (2019). La inteligencia artificial, el big bata y la era digital: ¿una amenaza para los datos personales? *Revista La Propiedad Inmaterial.* Obtenido de https://revistas.uexternado.edu.co/index.php/propin/article/view/6071/7789

Miranda, G. D. (2023). Los Datos Personales y su regulación en Colombia (datos sensibles, datos públicos, semiprivado y privado): enfoque, ámbito de aplicación y contenido. *Blog Jurídico - TECNOLOGÍA*. Obtenido de https://telecomunicaciones.uexternado.edu.co/los-datos-personales-y-su-regulacion-en-colombia-datos-sensibles-datos-publicos-semiprivado-y-privado-enfoque-ambito-de-aplicacion-y-contenido/

Peña, S. J. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. *Revista Perspectivas en Inteligencia*. Obtenido de https://doi.org/10.47961/2145194X.628

Pérez, E. M. (2019). Pérez Estrada, M. J. (2019). La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira de Direito Processual Penal*. Obtenido de

file:///C:/Users/USUARIO/Downloads/Dialnet-LaProteccionDeLosDatosPersonalesEnElRegistroDeDisp-7169230.pdf

Pierini, A. (1998). *Habeas data, derecho a la intimidad.* . Buenos Aires: Editorial Universidad.

Polo, R. A. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político, 108(mayo-agosto), 165-193. UNED.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7527690

Quiñones, Z. D. (2022). *¿10 años de la Ley de protección de datos: ¿Qué tanto hemos avanzado? ¿Qué nos hace falta? La ley al tablero.* Universidad Externado de Colombia. Obtenido de https://www.uexternado.edu.co/wp-content/uploads/2024/02/10-ANOS-DE-LA-LEY-DE-PROTECCION-DE-DATOS-1.pdf

Rojas, B. M. (2014). *Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.* Universidad Católica de Colombia. Obtenido de https://novumjus.ucatolica.edu.co/article/view/652/670

Zárate, R. C. (2020). *Gestión de la seguridad de la información de datos personales en el derecho informático.* Repositorio Institucional Universidad Externado de Colombia. Obtenido de https://bdigital.uexternado.edu.co/bitstreams/382212ee-998c-48dd-8745-e23