Gobernanza policéntrica, *big data* e inteligencia artificial: herramientas para la seguridad ciudadana en Colombia

Polycentric governance, big data and artificial intelligence: Tools for citizen security in Colombia

Governança policêntrica, big data e inteligência artificial: ferramentas para a segurança cidadã na Colômbiaa

• Fecha de recepción: 2024/05/06
• Fecha de evaluación: 2024/07/14
• Fecha de aprobación: 2024/08/05

Para citar este artículo / To reference this article / Para citar este artigo: Fernández-Osorio, A., Villalba-García, L. y Velandia-Pardo, E. (2024). Gobernanza policéntrica, *big data* e inteligencia artificial: herramientas para la seguridad ciudadana en Colombia. *Revista Criminalidad, 66*(3), 11-25. https://doi.org/10.47741/17943108.658

Andrés Eduardo Fernández-Osorio
Ph. D. en Derecho y Ciencia Política
Escuela Militar de Cadetes
General José María Córdova
Bogotá, Colombia
andres.fernandez@esmic.edu.co
https://orcid.org/0000-0003-0643-0258

Luisa Fernanda Villalba-García
Ph. D. (c) en Estudios Estratégicos, Seguridad y Defensa
Universidad Militar Nueva Granada
Bogotá, Colombia
luisa.villalba@unimilitar.edu.co
https://orcid.org/0000-0003-3169-9312

Elmers Freddy Velandia-Pardo
Ph. D. en Derecho, Educación y Desarrollo
Universidad Militar Nueva Granada
Bogotá, Colombia
elmers.velandia@unimilitar.edu.co
https://orcid.org/0000-0003-1217-9178

Resumen

En la era digital, en la cual los ciberataques son cada vez más sofisticados y persistentes, la capacidad de recopilar y analizar datos en tiempo real es fundamental para responder rápidamente a las amenazas emergentes. No obstante, la complejidad de administrar las diversas redes de interacción así como la multiplicidad de sus actores motiva la búsqueda de nuevas perspectivas para la lucha contra los delitos informáticos. Este artículo propone la utilización de una gobernanza policéntrica en Colombia, soportada en herramientas como la *big data* (BD) y la *inteligencia artificial* (IA), para contribuir a la seguridad ciudadana mediante nuevas perspectivas para la protección de datos. Por medio de un enfoque cualitativo se explora el escenario de ciberseguridad y ciberdefensa colombiano para interpretar el contexto de las amenazas en el ciberespacio e identificar los desafíos y las oportunidades relacionadas con el uso de la gobernanza policéntrica, la BD y la IA para la anticipación estratégica y la defensa de la nación.

Palabras clave:

Big data; ciberdefensa; ciberseguridad; gobernanza policéntrica; inteligencia artificial; seguridad ciudadana

Abstract

In the digital era, in which cyber-attacks are becoming increasingly sophisticated and persistent, the ability to collect and analyse data in real time is essential to respond quickly to emerging threats. However, the complexity of managing the various interaction networks, as well as the multiplicity of their actors, motivates the search for new perspectives in the fight against cybercrime. This article proposes the use of polycentric governance in Colombia, supported by tools such as big data (BD) and artificial intelligence (AI), to contribute to citizen security through new perspectives for data protection. Through a qualitative approach, the Colombian cybersecurity and cyber-defence scenario is explored to interpret the context of threats in cyberspace and identify challenges and opportunities related to the use of polycentric governance, BD and AI for strategic anticipation and defence of the nation.

Keywords:

Big data; cyber-defence; cybersecurity; polycentric governance; artificial intelligence; citizen security

Resumo

Na era digital, em que os ataques cibernéticos estão se tornando cada vez mais sofisticados e persistentes, a capacidade de coletar e analisar dados em tempo real é essencial para responder rapidamente às ameaças emergentes. No entanto, a complexidade de gerenciar as várias redes de interação, bem como a multiplicidade de seus atores, motiva a busca de novas perspectivas na luta contra o crime cibernético. Este artigo propõe o uso da governança policêntrica na Colômbia, apoiada por ferramentas como big data (BD) e inteligência artificial (IA), para contribuir com a segurança cidadã por meio de novas perspectivas de proteção de dados. Por meio de uma abordagem qualitativa, o cenário colombiano de segurança cibernética e defesa cibernética é explorado para interpretar o contexto das ameaças no espaço cibernético e identificar os desafios e as oportunidades relacionados ao uso da governança policêntrica, do BD e da IA para a antecipação estratégica e a defesa da nação.

Palavras-chave:

Big data; defesa cibernética; segurança cibernética; governança policêntrica; inteligência artificial; segurança cidadã

Introducción

En el escenario global, la sofisticación de las amenazas del ciberespacio compromete cada vez más la gobernabilidad de los Estados y la seguridad ciudadana. Al ser esta última definida como el "proceso de establecer, fortalecer y proteger el orden civil democrático, eliminando las amenazas de violencia en la población y permitiendo una coexistencia segura y pacífica" (PNUD, 2013, p. 1), se vuelve una prioridad la creación de estrategias que protejan los sistemas de información de la multiplicidad de actores que ponen en riesgo la integralidad de la infraestructura de datos y la privacidad de las personas (Ahsan et al., 2022; Semanate Esquivel y Recalde, 2023).

Aunque en la esfera internacional se han adelantado diversos esfuerzos individuales para mitigar las amenazas del ciberespacio (Margulies, 2013; Shackelford y Andres, 2010), dificultades en la determinación de responsabilidades en los ataques (Sánchez Barahona, 2021; Tsagourias, 2012), ópticas disímiles en la aplicación de la ley (García Torres, 2024; Moynihan, 2019) y múltiples intereses geopolíticos en juego (Buchanan, 2020; Pons Gamon, 2017) han demostrado la necesidad de una visión global extensa con participación de todos los sectores.

Dado que ninguna nación se encuentra encerrada en una burbuja impenetrable que la convierta en un actor autosuficiente y hermético frente a esta amenaza (Bancal et al., 2022), es fundamental que los Estados, para evitar el deterioro de su gobernabilidad, construyan una estrategia cíber con visión interinstitucional y transdisciplinar que anticipe y debilite posibles ataques a los intereses nacionales.

Esta anticipación estratégica del Estado a los delitos informáticos puede "contribuir de manera importante a la gestión de la seguridad orientada a la resiliencia, ya que permite centrarse sincronizadamente en múltiples amenazas dentro de una perspectiva de seguridad a más largo plazo" (Habegger, 2022, p. 2). Por el contrario, la falta de una visión de país para prever las amenazas en el ciberespacio puede llevar a una potencial pérdida de importancia por parte del Estado evidenciada en "el empoderamiento de otros actores a nivel internacional, los cuales podrían poseer un margen de actuación y decisión más amplio sobre el internet" (Perafán Del Campo et al., 2021, p. 13).

Desde esta óptica, diversos sectores han realizado análisis para solventar los delitos informáticos y han propuesto la creación de estructuras de liderazgo para aumentar la seguridad informática (Cavelty y Egloff, 2019; Herald y David, 2018); manejar el impacto de posibles ataques (Lawson et al., 2016; Sokolov et al., 2021), y obtener el apoyo público necesario para justificar respuestas económicas, diplomáticas o militares después de los ciberataques (Jardine et al., 2024; Solar, 2020). Así mismo, han sugerido la incorporación de herramientas como la big data (BD) (Chayal y Patel, 2021; Kochhar et al., 2022) y la inteligencia artificial (IA)

(Guembe et al., 2022; Yamin et al., 2021) para facilitar que la adquisición, almacenamiento, gestión y análisis de la información se realicen en forma sinérgica y propositiva.

No obstante, además de fomentar la existencia de instituciones encargadas de combatir los riesgos del ciberespacio y del empleo de herramientas para el reconocimiento de patrones predictivos que detecten vulnerabilidades y contrarresten posibles consecuencias, para la eficiencia de una estrategia cíber es fundamental el desarrollo de una visión coordinada entre estos elementos que permita articular actores y esfuerzos.

Este es el objetivo del presente artículo, el cual, mediante el análisis del caso colombiano, propone la utilización de una gobernanza policéntrica en la estrategia cíber estatal soportada en la utilización de la BD y la IA, que contribuya al incremento de la seguridad ciudadana y a la protección de los intereses nacionales por medio de nuevas perspectivas para la protección de datos. Se usa un enfoque cualitativo a fin de explorar el escenario de ciberseguridad en Colombia como recurso analítico para interpretar el contexto de las amenazas en el ciberespacio. Así mismo, se utilizan fuentes secundarias de la literatura e informes oficiales y medios de comunicación. Al proporcionar una perspectiva interpretativa de los hallazgos (Aguilera Eguía, 2014), se pueden identificar los desafíos y las oportunidades relacionadas con el uso de la gobernanza policéntrica, la BD y la IA como estrategia para la seguridad ciudadana en Colombia.

La seguridad ciudadana y los delitos informáticos en Colombia

La seguridad ciudadana es un bien público que "implica la salvaguarda eficaz de los derechos humanos inherentes a la persona, especialmente el derecho a la vida, la integridad personal, la inviolabilidad del domicilio y la libertad de movimiento" (PNUD, 2013, p. 1) y, por ende, los Estados tienen la responsabilidad de protegerla. Al respecto, varios estudios han demostrado la necesidad de generar estrategias innovadoras que permitan dar una respuesta institucional al menos a tres aspectos principales: (a) prevenir actividades delictivas (Adorno, 2024; Díaz Samper et al., 2024; Duxbury y Andrabi, 2024; Miró Llinares, 2020), (b) mitigar el impacto de la criminalidad (Díaz-Roman, 2024; Oatley, 2022; Rodríguez-Ortega, 2024; Verhelst et al., 2020), y (c) fomentar el apoyo y confianza en las instituciones (Brayne, 2020; Fernández-Hernández, 2024; Manzano-Chávez et al., 2024; Padilla-Oñate, 2024).

Colombia no se sustrae a esta problemática. Las mediciones de criminalidad, operatividad y efectividad policial (Gómez y Zapata, 2020; Tamayo Arboleda y Norza Céspedes, 2017), así como las complejas variables que acompañan el delito (Elizalde Castañeda et al., 2021; Macana Gutiérrez, 2021; Medina Martínez et al., 2021; Valencia Casallas, 2020), han resaltado un aumento de las amenazas a la seguridad ciudadana, incluyendo un incremento creciente de factores y amenazas de seguridad, más allá del enfoque tradicional Estado-céntrico (Acevedo-Navas, 2023), especialmente los ataques en el ciberespacio. En efecto, las cifras de delitos informáticos reportadas por el Ministerio de Defensa Nacional (tabla 1) indican un crecimiento constante durante los últimos 10 años y un incremento comparativo del 27 % entre los meses de enero y junio de 2023 y 2024.

Por otra parte, el índice de inteligencia de amenazas X-Force de la compañía IBM para 2024 indicó que Colombia es el país con más ataques de ciberseguridad en Latinoamérica (Forbes, 2024); diversas empresas han sido afectadas por estos ataques durante los últimos años (Murillo Herrera, 2023; Vargas, 2023), y los análisis prospectivos para los años futuros enfatizan la necesidad de identificar con urgencia los retos emergentes que aprovechan vulnerabilidades inherentes (Cano-Martínez, 2022, p. 829).

Tabla 1. | Delitos informáticos en Colombia entre 2014 y junio de 2024

Año	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Delitos	3676	7404	8651	15057	21279	22092	49359	52224	61992	63250	37878

Nota: los delitos informáticos son las conductas que violan la "protección de la información y de los datos", establecidos en el Código Penal colombiano (arts. 269A al 269J), Ley 599 de 2000, y que corresponden a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, así como los atentados informáticos y otras infracciones.

Fuente: elaborada con base en cifras del Ministerio de Defensa Nacional (2024, p. 34).

Al entenderse la ciberseguridad como la "capacidad del Estado para minimizar el nivel de riesgo cibernético al que están expuestos los ciudadanos, en áreas como transacciones financieras, protección a la información y propiedad intelectual" (Cortés Borrero, 2015, p. 7), se busca promover el avance de la institucionalidad en términos de protección, integridad y seguridad de la infraestructura cibernética en Colombia con el fin de prevenir actividades delictivas, mitigar el impacto de la criminalidad y fomentar el apoyo y confianza en las instituciones. No obstante, para comprender la dimensión de la problemática es necesario diferenciar entre los términos ciberseguridad y ciberdefensa. La tabla 2 provee una caracterización de estos dos términos.

Tabla 2. | Caracterización de la ciberseguridad y la ciberdefensa

Término	Características
Ciberseguridad	Puede ser vista como una condición de seguridad en el ciberespacio en el que se han mitigado riesgos, peligros y amenazas para que ciudadanos y organizaciones gocen del dominio ciber, esta es una visión estratégica que describe un estado óptimo. En este estado los sistemas y la información están protegidos, y se conserva la integridad, confidencialidad y disponibilidad de los datos en el entorno digital. Por otro lado, también puede ser vista como la protección de las condiciones anteriormente descritas de forma operativa. Desde este enfoque se pueden crear mecanismos de protección efectivos ante ciberataques. Esto implica implementar medidas de seguridad tecnológicas, como firewalls, sistemas de detección de intrusiones, encriptación de datos y autenticación de usuarios, entre otros. Estos mecanismos se diseñan para impedir la vulneración de sistemas y el acceso no autorizado a la información e implica el establecimiento de normas y políticas que rigen el uso seguro de los sistemas informáticos y la protección de la información. Estas dos visiones incluyen normativas para proteger la privacidad por medio de la gestión de datos, la notificación de incidentes de seguridad y la responsabilidad en caso de brechas de seguridad. De la misma forma, las políticas de ciberseguridad en este marco refuerzan las pautas y lineamientos para promover buenas prácticas en el uso de la tecnología y fomentar la conciencia sobre la importancia de proteger la información en el entorno digital.
Ciberdefensa	Son las acciones que toma un Estado para mantener su ciberseguridad en el marco de la protección de su población, territorio y soberanía. Estas acciones pueden involucrar el uso del poder militar o no, y pueden implicar la implementación de rutas estratégicas que permitan la mitigación de riesgos y control de amenazas de una forma efectiva. Así, la ciberdefensa busca garantizar la protección de los sistemas y la información e implica la capacidad de realizar ataques en respuesta a amenazas cibernéticas. Su enfoque principal es disuadir y responder a ataques o amenazas cibernéticas que pueden generar inestabilidad en un Estado y su población. En este sentido, es el conjunto de medios que se utilizan para responder a posibles ataques cibernéticos. Estas tareas preservan la seguridad de los sistemas críticos y la infraestructura digital, salvaguardando la integridad de los servicios esenciales y manteniendo la confianza en el funcionamiento de las instituciones y la sociedad en general.

Fuente: elaborada a partir de Vargas Borbúa et al. (2017).

A la par de la experiencia internacional, Colombia fundamenta la seguridad de sus intereses, frente a los nuevos desafíos nacionales e internacionales (Pastrana Buelvas y Gehring, 2019) en el campo de la ciberseguridad, la ciberdefensa y la gestión digital de la información sensible en el ciberespacio, mediante el trabajo conjunto desde las Fuerzas Armadas (constituidas por el Ejército Nacional, Armada Nacional, Fuerza Aérea y Policía Nacional) y otras instituciones gubernamentales. Estas entidades son las responsables de coordinar a escala nacional los aspectos relacionados con la ciberseguridad y la ciberdefensa.

Esta estructura institucional colombiana para el ciberespacio es gestionada por la Oficina de Respuesta a Incidentes Cibernéticos (CSIRT), como parte de la formulación e implementación del Plan Estratégico Sectorial (Ley 1273 de 2009.). La normativa genérica frente al ejercicio y uso del ciberespacio ampara las tareas derivadas del avance tecnológico, y es esta la razón por la que, mediante el Decreto 1874 del 30 de diciembre de 2021 del Ministerio de Defensa Nacional, su artículo 5 dispone que esta oficina se encargue de "coordinar las capacidades de ciberseguridad y ciberdefensa con la Dirección de Seguridad Nacional y los organismos del Sector Defensa y otros sectores" (Decreto 1874 de 2021).

Para fortalecer este cometido, las acciones conducentes a asegurar y proteger la infraestructura crítica, física y virtual de un país y su entorno de sitios de redes, sitios

de contacto, sitios de intercambio de información visual, realidad virtual y toda la variante circular del ciberespacio, son desarrolladas por tres organizaciones principales establecidas en el Documento Conpes 3701 "Lineamientos de política para ciberseguridad y ciberdefensa" (República de Colombia, 2011): (a) el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) del Ministerio de Defensa Nacional y del Ministerio de Tecnologías de la Información y las Comunicaciones; (b) el Comando Conjunto Cibernético de las Fuerzas Militares (CCOCI), conformado por el Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa del Ejército (CAOCC), el Comité de Dirección del Sistema de Gestión de Seguridad de la Información (CDSGSI) de la Armada Nacional, el Equipo de Respuesta ante Incidentes Cibernéticos para la Infraestructura Crítica Aeronáutica (CSIRTFAC) de la Fuerza Aérea Colombiana; y (c) el Centro Cibernético Policial (CCP) de la Policía Nacional (tabla 3).

Tabla 3. | Organizaciones colombianas encargadas de la ciberseguridad y la ciberdefensa

Entidad	Organización	Misión
Ministerio de Defensa Nacional Ministerio de Tecnologías de la Información y las Comunicaciones	Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT)	Identificar infraestructuras críticas, gestionar sus riesgos de ciberseguridad, ofrecer a las empresas del sector público y privado información preventiva sobre amenazas y vulnerabilidades, apoyo y asesoría en la gestión de los incidentes de ciberseguridad, que garanticen la continuidad de las operaciones y servicios a la ciudadanía colombiana.
Comando General de las Fuerzas Militares	Comando Conjunto Cibernético de las Fuerzas Militares (CCOCI)	Direccionar, planear, coordinar, integrar y sincronizar, mediante unidades y/o dependencias, el desarrollo, la ejecución y conducción de actividades y operaciones cibernéticas conjuntas, combinadas, coordinadas e interagenciales con el fin de defender las infraestructuras críticas cibernéticas que le sean asignadas, de acuerdo con su misión constitucional, ante las amenazas que atenten contra la seguridad y defensa del Estado colombiano en el ámbito cibernético, dentro del marco de la legalidad soporte de la legitimidad institucional.
Ejército Nacional	Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa (CAOCC)	Desarrollar operaciones de apoyo en comando, control, comunicaciones, computación y ciberdefensa (C5), con el objetivo de brindar al Ejército Nacional las capacidades para coadyuvar al desarrollo de operaciones militares conjuntas, coordinadas, interinstitucionales, multinacionales.
Armada Nacional	Comité de Dirección del Sistema de Gestión de Seguridad de la Información (CDSGSI)	Supervisar y dirigir las actividades relacionadas con la gestión de seguridad de la información, a fin de asegurar que se cumplan las políticas y procedimientos establecidos. Por su parte, la División de Informática es responsable de implementar y mantener las medidas de seguridad tecnológicas necesarias para proteger la información misional.
Fuerza Aérea Colombiana	Equipo de Respuesta ante Incidentes Cibernéticos para la Infraestructura Crítica Aeronáutica (CSIRTFAC)	Brindar servicios de ciberseguridad para prevenir, detectar, mitigar y responder a incidentes cibernéticos. La Fuerza Aérea también define lineamientos de controles criptográficos para proteger la información de la institución, de manera que se garantice la confidencialidad, autenticidad e integridad de la información.
Policía Nacional	Centro Cibernético Policial (CCP)	Investigar los delitos informáticos y apoyar la investigación criminal de los fenómenos en el ciberespacio, por medio del análisis de información, atención de incidentes cibernéticos y el desarrollo de estrategias, programas, acciones y proyectos de ciberseguridad.

Fuente: elaborada con base en República de Colombia (2011), Ministerio de Tecnologías de la Información y las Comunicaciones (2022) y Peña Suárez (2023).

Estas organizaciones buscan fortalecer la ciberseguridad y ciberdefensa de Colombia asegurando que los activos de información estén protegidos contra amenazas internas y externas. Al proteger la integridad, confiabilidad, confidencialidad y disponibilidad de la información, se promueve la eficiencia del actuar de los organismos de seguridad, el respeto de la ley y el cumplimiento del Documento Conpes 3854 "Política Nacional de Seguridad Digital" (República de Colombia, 2016). En este sentido, los lineamientos legales existentes buscan brindar un marco jurídico que permita desarrollar capacidades de prevención, detección y contención en el ciberespacio; además, se proponen establecer normas en el ámbito de la respuesta, la recuperación y la defensa del entorno digital.

Prevención de actividades delictivas cíber

Para atender este desafío, la Ley 1273 de 2009 introdujo modificaciones al Código Penal para establecer un nuevo ámbito de protección jurídica denominado protección de la información y de los datos. Esta ley tiene como objetivo principal salvar de manera integral los sistemas que utilizan tecnologías de la información y las comunicaciones (TIC). Además de abordar los delitos informáticos y otras infracciones, tiene como propósito garantizar la confidencialidad, integridad y disponibilidad de los datos y los nuevos sistemas informáticos.

La Ley 1273 establece disposiciones específicas para combatir los ataques cibernéticos y otros actos delictivos relacionados con el uso indebido de la información y los sistemas informáticos. También se enfoca en prevenir la violación de la confidencialidad de la información, garantizar la integridad de los datos y proteger la disponibilidad de los sistemas informáticos esenciales. Esta ley amplía el marco jurídico existente al incluir disposiciones que abordan de manera más precisa los delitos informáticos y la protección de la información y los datos en el contexto de las TIC. Esto refuerza la importancia de garantizar la seguridad cibernética y la protección de la información en un entorno cada vez más digitalizado.

Para lograr este objetivo, existen tres instancias clave encargadas de la protección tanto interna como externa del país en el ámbito digital. En primer lugar, el COLCERT es responsable de responder de manera rápida y efectiva a las emergencias cibernéticas, así como coordinar las acciones relacionadas con la seguridad digital nacional. En segundo lugar, el CCOCI se encarga de liderar las operaciones de ciberdefensa estratégica y coordinar los esfuerzos de las diferentes entidades involucradas en la seguridad digital. En tercer lugar, el CCP investiga y persigue los delitos cibernéticos, así como brindar apoyo técnico y operativo en materia de ciberseguridad.

Adicionalmente, la Ley 1928 de 2018 fue aprobada con el objetivo de adoptar el Convenio sobre la Ciberdelincuencia del 2001 en Budapest el cual establece medidas para prevenir y combatir delitos cibernéticos y fortalecer la cooperación internacional. En la Sentencia C-224 de 2019, la Corte Constitucional de Colombia se pronunció acerca de la constitucionalidad de esta normativa internacional. Así mismo, se determinó que el Convenio de Budapest sobre Ciberdelincuencia se adecua a los objetivos constitucionales en materia de política criminal y soberanía (Mejía-Lobo et al., 2023, p. 363).

Mitigación del impacto de la criminalidad cíber

Frente a este desafío, la Ley 527 de 1999 se enfoca en regular el comercio electrónico, y el uso y acceso de mensajes de datos. Dicha ley establece disposiciones claras sobre las transacciones realizadas por medios electrónicos, buscando fomentar la confianza y la seguridad en las transacciones en línea. Además, regula el uso de firmas digitales como mecanismo de autenticación y protección de la integridad de los documentos electrónicos.

En lo que respecta a BD, la normatividad busca amparar el ejercicio de la gestión de datos masivos, o macrodatos, este último término adoptado por la Unión Europea, para alcanzar la sinergia entre proveedores de servicios y usuarios a fin de resguardar el acceso y uso de datos que, ya operados en masa, precisan una dinámica ajustada a reglas de juego cuya legalidad es imperiosa. En Colombia, ya que el BD puede incluir el tratamiento de datos personales, quienes hagan uso de estos deben acogerse a la Ley 1581 de 2012 que reglamente lo relacionado a la protección de tales datos.

No obstante, esa regulación enfrenta una dificultad de tipo dialéctico, ya que la legislación de protección de datos, dado el carácter anónimo de sus titulares, no sería factible de aplicar en tanto no exista una personalización expresa del usuario. De esta forma, "no serían datos personales y, en consecuencia, no se proyectará el régimen normativo. Como se puede prever, saber si se trata o no de datos personales es una cuestión esencial para conformar el régimen jurídico aplicable" (Cotino, 2016, p. 16).

Efectivamente, no se trata únicamente del consentimiento y del tratamiento de datos personales, sino que el establecimiento de patrones de BD para identificar la procedencia de la información supone más exigencia en el momento de abordar una normativa por sectores específicos para regular el tratamiento de datos y el aspecto macro de estos. En este sentido, se requiere una acción jurídica de mayor alcance porque, desde el seno de las garantías constitucionales de los Estados democráticos, el control sobre el conglomerado de algoritmos, la complejidad de las rutas BD, los retos de la IA asociada, precisará de una protección ante el uso dispar e impredecible del ciberespacio.

En forma complementaria, la Ley 1341 de 2009 establece principios y conceptos fundamentales sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones (TIC). Además, instituye la creación de la Agencia Nacional de Espectro, encargada de regular y supervisar el uso del espectro electromagnético en el país.

Esta Ley tiene como objetivo principal establecer los parámetros y lineamientos para el uso adecuado del espectro electromagnético, asegurando su correcta aplicación y gestión, dado que el espectro electromagnético es un recurso limitado y estratégico que se utiliza para la transmisión de las comunicaciones inalámbricas, como telefonía móvil, televisión, radio, entre otros servicios.

Fomento del apoyo y confianza en las instituciones frente a las amenazas cíber

Respecto a este desafío, se promulgó en Colombia la Ley 1712 de 2014, que establece la Ley de Transparencia y el Derecho de Acceso a la Información Pública Nacional. Esta ley tiene como objetivo garantizar el compromiso de brindar garantías para el ejercicio del derecho de acceso a la información. Así mismo, establece disposiciones específicas sobre la divulgación de información por parte de entidades públicas, promoviendo la transparencia y la rendición de cuentas. Se busca que los ciudadanos tengan acceso a la información pública de manera clara y oportuna, con lo cual se fortalece la participación ciudadana y la construcción de una sociedad informada.

En el artículo 19 de esta ley se establecen excepciones para el acceso a la información, especialmente cuando se involucran daños a los intereses públicos. La información considerada reservada busca dimensionar la naturaleza, alcance y efecto de las disposiciones jurídicas y englobar el cuerpo legal de modo consistente con la necesidad de la seguridad de la ciberdefensa.

Adicionalmente, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC) ha impulsado la formulación de una estrategia de cuatro puntos para hacer de Colombia una potencia en ciberseguridad, enfocada en la prevención, la mitigación, la gestión y la respuesta ante incidentes de seguridad digital (MinTIC, 2023); no obstante, sus resultados aún distan de las necesidades del país. La rapidez del cambio de las amenazas, mas no de las regulaciones estatales, es la que motiva la búsqueda de nuevas estrategias para la lucha integral contra los delitos informáticos.

La gobernanza policéntrica como estrategia para la seguridad ciudadana

Una visión sobre la gobernanza policéntrica sugerida por Ostrom (1999) implica que muchos elementos sean capaces de hacer ajustes mutuos para ordenar sus relaciones entre sí dentro de un sistema general de reglas donde cada elemento actúa con independencia de los demás. De igual modo, McGinnis (2013) sugiere que, por medio de la gobernanza policéntrica, cualquier grupo que se enfrente a un problema colectivo debería poder abordarlo de la mejor manera posible, incluyendo la utilización de estructuras de gobernanza existentes o la creación de nuevos sistemas que faciliten la solución creativa de problemas en todos los niveles.

Por tal motivo, Shackelford (2013) sugiere la aplicación de la gobernanza policéntrica en el ciberespacio, ya que no solo se soporta en el Estado la actuación contra las amenazas, sino que se les brinda la posibilidad a múltiples actores interesados de hacer frente a estos desafíos cíber, presentes y futuros, mediante opciones de autoorganización y creación de redes en múltiples niveles. Al brindar un marco general de regulación en cabeza del Estado y una libertad de iniciativa y acción a los actores (policía, fuerzas militares, centros de pensamiento, organizaciones no gubernamentales, industria privada y personas, entre otros), se pueden generar oportunidades para la pronta detección de nuevas amenazas cíber y el encontrar propuestas novedosas para hacerles frente.

A las dificultades propias de la lucha contra los delitos cibernéticos, mencionadas anteriormente, se suma la complejidad existente en la coordinación de estos actores que buscan mitigar los delitos informáticos, de modo que es necesario emplear nuevas perspectivas y herramientas diferenciales que faciliten su interacción. En efecto, al examinar el modelo relacional del COLCERT establecido por el Conpes 3701 (figura 1), se puede identificar una estructura organizacional jerárquica tradicional basada en el control, más que en la coordinación, donde los actores tienen una limitada interacción entre ellos.

Algunos actores importantes en la actualidad, como los individuos, la industria y las entidades internacionales públicas y privadas, no están incluidos claramente dentro de la organización. Por otra parte, la naturaleza y la dirección de las relaciones entre los actores pareciera que estuviesen más enfocadas en la respuesta a los delitos informáticos que a su prevención, lo cual conlleva que se tenga que dedicar una gran cantidad de recursos a la investigación y persecución penal y a que se desaprovechen iniciativas independientes basadas en las capacidades de los actores.

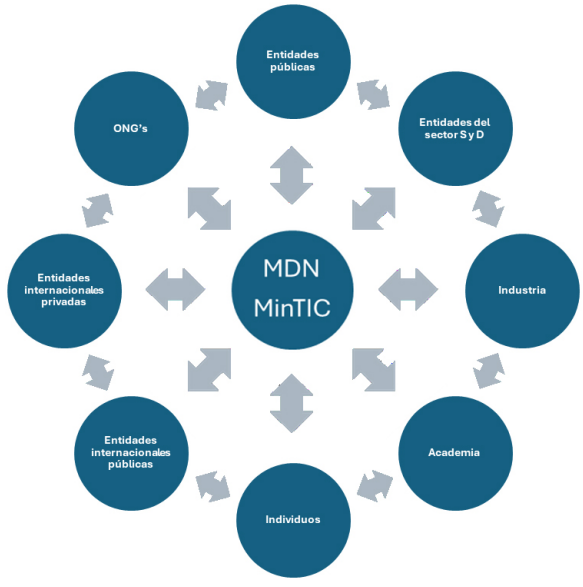
Figura 1. | Modelo relacional del COLCERT

Fuente: República de Colombia (2011, p. 24).

Es precisamente la complejidad de crear una red multinivel autorregulada la que motiva al empleo de una gobernanza policéntrica con apoyo de la BD y la IA en la lucha común contra los delitos informáticos. Con una gobernanza policéntrica se establecerían normas generales de cumplimiento para empoderar a los actores a fin de privilegiar la iniciativa y la proactividad. Así mismo, la BD, con el uso de algoritmos avanzados de análisis y aprendizaje automático mediante la IA, puede contribuir a que los actores, gobiernos y organismos de seguridad puedan identificar amenazas potenciales y tomar medidas proactivas para garantizar la seguridad pública (figura 2).

La gobernanza policéntrica, la BD y la IA se pueden emplear para el análisis de patrones y tendencias con el fin de predecir y prevenir actividades delictivas; así mismo, pueden utilizarse para mejorar los tiempos de respuesta ante emergencias y asignar recursos de manera más eficiente en tiempos de crisis. Por ejemplo, las autoridades pueden utilizar el análisis de BD e IA para estudiar la actividad delictiva pasada e identificar los puntos críticos con mayor probabilidad de ser escenarios delictivos. Al respecto, Fontalvo-Herrera et al. (2023) sugieren la organización de clústeres de delitos violentos en Colombia por departamentos junto con una estructura de redes neuronales para su clasificación y pronóstico. A partir de esta estructura inicial, se aumenta la presencia de personal policial o militar en las zonas priorizadas para disuadir a potenciales infractores, con base en sistemas integrados de información que incluyen desarrollos tecnológicos como cámaras con reconocimiento facial, centros de mando integrado y uso de drones, entre otros (Villalobos Fonseca, 2020).

Figura 2. | Modelo relacional con gobernanza policéntrica del COLCERT



Fuente: elaboración propia.

Por su parte, los equipos de respuesta a emergencias pueden utilizar datos actualizados de redes sociales y sensores para evaluar rápidamente la gravedad de una

crisis y asignar los recursos requeridos, lo que podría conducir a salvaguardar vidas humanas. De igual forma, fundamentándose en los datos recopilados y las acciones tomadas, los actores de esta gobernanza policéntrica pueden establecer iniciativas para la generación o actualización de la normatividad existente con el fin de demostrar, tal como lo sugieren Garzón Pulgar y Cuero Quiñones (2022, p. 203), "que los tipos penales de carácter informático requieren un tratamiento diferencial, mayor conocimiento y estrategias tendientes a mejorar las medidas de prevención y autoprotección de la sociedad", o la necesidad de que "los aspectos de política pública se deben considerar como prioritarios, teniendo en cuenta los incentivos económicos para los ciberdelincuentes y la efectividad de la Ley 1273 de 2009" (Rincón Arteaga et al., 2022, p. 95).

En el caso de los delitos cibernéticos, el COLCERT, liderado por el Ministerio de Defensa Nacional (MDN) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), puede dar instrucciones de coordinación a diversas entidades públicas y entidades del sector Seguridad y Defensa (CCOCI, CAOCC, CDSGSI, CSIRTFAC y CCP) para la articulación cooperativa entre individuos, industria, academia, organizaciones no gubernamentales y entidades internacionales públicas y privadas con el fin de maximizar la prevención, por medio del intercambio de información, implementación de sistemas de gestión, aumento de las denuncias, análisis aleatorio de páginas, y campañas de conocimiento, y perfeccionar la persecución penal para afectar las estructuras delictivas y el establecimiento de conexiones entre casos investigados y autores.

Sin embargo, el uso de la BD y la IA en una gobernanza policéntrica para la seguridad ciudadana presenta desafíos, ya que la ubicación de datos imprecisos o incompletos podría resultar en una asignación incorrecta de los recursos disponibles. En caso de que los datos utilizados para determinar los puntos críticos de delincuencia estén desactualizados o sesgados, existe la posibilidad de que las entidades concentren incorrectamente sus esfuerzos en áreas específicas, lo que podría llevar a la falta de protección en otras zonas de riesgo elevado.

La BD y la IA como herramientas de la gobernanza policéntrica

La BD abarca datos que contienen una "mayor variedad, [...] volúmenes crecientes y una velocidad superior, [los cuales] son tan voluminosos que el software de procesamiento de datos convencional no puede gestionarlos, pero que pueden [...] abordar problemas que antes no hubiera sido posible solucionar" (Oracle, 2023). Esta gran cantidad de datos producidos por múltiples fuentes, como redes sociales, sensores y cámaras de vigilancia, son fundamentales para administrar y evaluar la seguridad en el entorno digital y virtual.

Esta considerable recopilación de flujos de información requiere de un análisis macro con la ayuda de la IA, como "tecnología que permite que las computadoras simulen la inteligencia humana y las capacidades humanas de resolución de problemas" (IBM, 2023), lo que facilita su manejo y sistematización para contribuir a la comprensión multidisciplinar de los datos recopilados y su posterior utilización para la solución de problemáticas actuales y futuras en seguridad.

Las ventajas competitivas de estas herramientas para la gobernanza policéntrica están dadas por sus capacidades de volumen, alta velocidad y variedad considerable para hacer confluir una definición de algoritmos en que las vulnerabilidades de los sistemas de automatización, sumadas a los ejercicios de análisis, predicción y proyección, aseguren un corredor digital de óptima precaución bajo una sinergia operante en la gama de respuestas anticipantes.

Con el uso de la gestión del riesgo con BD e IA se genera una oportunidad para la utilización de estándares comunes en el manejo de la información entre diversos actores. Al abarcar una amplia gama de información, la BD incluye desde datos personales hasta datos corporativos, instituciones y gobiernos, bajo el lente de un tratamiento automatizado en que los algoritmos informáticos se ponen de presente en el almacenamiento de flujo continuo y transmisión. Por su parte, la IA opera la analítica de macrodatos bajo supuestos, aciertos, veracidades y estimaciones para confluir en tareas de protección, antelación, trazabilidad y proyección.

La BD, por su naturaleza, capta, almacena, clasifica y analiza volúmenes ingentes de datos en tiempo real, y actúa con la IA y la analítica predictiva que operan como herramientas para soportar la eficacia del manejo de la BD. De esta forma, adquiere especial importancia la minería de datos, la minería de textos y el machine learning en tanto, al definir patrones de relación de datos, analizar capos de flujos informativos y procesar especificidades, se logra una trazabilidad en el tiempo y el espacio de riesgos, alternativas y supuestos, por lo que forja versatilidad en la utilidad de su diseño y la efectividad de su alcance.

Dado que la BD y la IA son herramientas para la gobernanza policéntrica, es fundamental que sean respaldadas por lineamientos colaborativos que impidan el abuso de sus capacidades. Así mismo, su implementación implica una serie de procesos, métodos y técnicas de gestión del conocimiento en los cuales el bien común debe primar. En este sentido, la BD y la IA

pueden proporcionar una visión más amplia y profunda de los fenómenos y tendencias, sin reemplazar la experiencia y el conocimiento de los expertos, ya que son estos últimos los que desempeñan un papel crucial en la formulación de preguntas adecuadas, la selección de técnicas más apropiadas y la interpretación de los resultados obtenidos.

Al caracterizarse la gobernanza policéntrica por contar con varios centros de decisión que tienen, al mismo tiempo, prerrogativas limitadas y autónomas y que operan bajo un conjunto compartido de reglas generales, la BD y la IA desempeñan un papel determinante en el momento de formular una anticipación estratégica con el propósito de otorgar confiabilidad respecto a la tarea de administración de datos y apreciación de resultados.

Dado que la protección de los intereses nacionales frente a amenazas es de vital importancia, el uso de la BD y la IA como herramientas es fundamental para la seguridad y la defensa. Esto tiene como objetivo garantizar la estabilidad y prevenir el robo o uso malintencionado de la información. La implementación de la BD y la IA en el ámbito de la seguridad y la defensa del país permite realizar una anticipación estratégica frente a posibles amenazas. Al utilizar técnicas de análisis de datos avanzados es posible detectar patrones y tendencias que podrían indicar actividades maliciosas o intentos de robo de información.

Las intrusiones cibernéticas, el asalto a las páginas oficiales del Estado y de compañías privadas, el secuestro de datos, la suplantación de sitios web, y demás ataques, han exigido el perfeccionamiento de las capacidades institucionales y motivado a innovar hasta el punto de desarrollar BD e IA de antelación en que convergen diversos escenarios de salvaguarda, bajo mecanismos de sofisticación cuya complejidad reta a los centros especializados por la implementación de protección a los sistemas de seguridad cibernéticos.

La adopción de BD e IA en el ámbito de la seguridad informática y la anticipación estratégica ha ganado una gran importancia debido a su capacidad para mejorar la protección de los intereses nacionales y enfrentar los desafíos de los nuevos escenarios generados por el desarrollo tecnológico. Al aplicar técnicas avanzadas de análisis de datos, como el aprendizaje automático y la minería de datos, se podrían descubrir patrones ocultos, correlaciones y comportamientos anómalos que podrían ayudar a prevenir y combatir amenazas de manera más efectiva.

Conclusiones

El fortalecimiento de la estrategia integral de ciberseguridad es fundamental para proteger las infraestructuras críticas y salvaguardar la información sensible. En la era digital, en que los ciberataques son cada vez más sofisticados y persistentes, la capacidad de recopilar y analizar datos en tiempo real se vuelve crucial para detectar y responder rápidamente a posibles amenazas cibernéticas.

La ciberseguridad es un desafío multifacético, pues trasciende las fronteras nacionales y se ha convertido en un reto complejo que requiere una respuesta integral y coordinada. Las amenazas cibernéticas evolucionan constantemente, de forma que exigen una adaptación continua de las estrategias de defensa.

La adopción de una gobernanza policéntrica en el ámbito de la ciberseguridad en Colombia demuestra ser una estrategia prometedora. Al permitir la participación de múltiples actores, se fomentan la innovación, la agilidad y la capacidad de respuesta ante las amenazas emergentes. Sin embargo, es fundamental establecer mecanismos de coordinación y colaboración efectivos para evitar duplicidades y garantizar la coherencia en las acciones.

La gobernanza policéntrica debe ser flexible y adaptable para responder a las rápidas evoluciones del entorno cibernético; por esta razón, la sociedad tiene un papel fundamental en la construcción de una ciberseguridad más resiliente, mediante la participación, denuncia de incidentes e integración con los demás actores.

Herramientas como la BD y la IA ofrecen poderosas oportunidades para analizar grandes volúmenes de datos, identificar patrones y predecir amenazas. Su implementación en el contexto de la ciberseguridad puede optimizar la detección de incidentes, la respuesta a emergencias y la prevención de futuros ataques. No obstante, es necesario abordar los desafíos asociados a la privacidad, la seguridad de los datos y la ética en el uso de estas tecnologías.

La ciberseguridad es un desafío constante que requiere una inversión sostenida en recursos humanos, tecnológicos y financieros. Es fundamental desarrollar una visión a largo plazo que permita construir una infraestructura cibernética resiliente y adaptable a los cambios tecnológicos y sociales. Las amenazas cibernéticas no consideran fronteras, por lo que la cooperación internacional es esencial para fortalecer la ciberseguridad a nivel global. El intercambio de información, la estandarización de protocolos y la creación de alianzas estratégicas son elementos clave para enfrentar este desafío común.

Promover una mayor colaboración entre las diferentes entidades gubernamentales, el sector privado y la academia, y fomentar la investigación en el campo de la ciberseguridad a fin de desarrollar nuevas tecnologías y soluciones innovadoras, es fundamental para optimizar la gestión de la ciberseguridad. Así mismo, impulsar programas de educación y capacitación en ciberseguridad para todos los niveles de la sociedad, y profundizar

marcos regulatorios que equilibren la protección de la privacidad con la necesidad de garantizar la seguridad cibernética, debe considerarse prioritario para la lucha contra los delitos informáticos. El establecimiento de una cultura de ciberseguridad en la sociedad, con el propósito de que sea considerada como un activo estratégico para el desarrollo económico y social de un país, incentivando la adopción de prácticas seguras en el uso de las tecnologías de la información, significará un gran avance en la identificación y mitigación de amenazas.

Conflicto de intereses

No se presentó conflicto de interés en el desarrollo de la presente investigación académica. Los autores declaramos que no tenemos ninguna relación financiera o personal que pudiera influir en el diseño de la investigación realizada, así como la interpretación y publicación de los resultados obtenidos. Asimismo, aseguramos cumplir con las normas éticas y de integridad científica en todo momento, de acuerdo con las directrices establecidas por la comunidad académica y las dictaminadas por la presente revista.

Referencias

Acevedo-Navas, C. (2023). Ejes temáticos estratégicos en seguridad y defensa en Colombia. *Revista Científica General José María Córdova*, *21*(42), 303-326. https://doi.org/10.21830/19006586.1215

Adorno, S. (2024). Collective action and sociological research networks in the fight against crime in Brazil. *Revista Científica General José María Córdova*, *22*(46), 433-456. https://doi.org/10.21830/19006586.1315

Aguilera Eguía, R. (2014). ¿Revisión sistemática, revisión narrativa o metaanálisis? *Revista de la Sociedad Española del Dolor*, *21*(6), 359-360. https://doi.org/10.4321/S1134-80462014000600010

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N. y Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using machine learning—a review. *Journal of Cybersecurity and Privacy*, *2*(3), 527-555. https://doi.org/10.3390/jcp2030027

Bancal, D., Ebel, F., Vicogne, F., Fortunato, G., Beirnaert-Huvelle, J., Hennecart, J., Clarhaut, J., Schalkwijk, L., Rault, R., Dubourgnoux, R., Crocfer, R. y Lasson, S. (2022). *Seguridad informática. Ethical Hacking: Conocer el ataque para una mejor defensa*. Ediciones ENI.

Brayne, S. (2020). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Cano-Martínez, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, *20*(40). https://doi.org/10.21830/19006586.866

Cavelty, M. D. y Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the State. *St Antony's International Review*, *15*(1), 37-57.

Chayal, N. M. y Patel, N. P. (2021). Review of machine learning and data mining methods to predict different cyberattacks. En K. Kotecha, V. Piuri, H. Shah y R. Patel (eds.), *Data Science and Intelligent Applications* (pp. 43-51). Springer. https://doi.org/10.1007/978-981-15-4474-3_5

Cortés Borrero, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, *14*, 1-17.

Cotino, L. (2016). El Dret enfrontat las reptes del Big Data i l'automatització de les decisions. *Seminario de Derecho de la Universidad de Valencia, España*, 1-28. https://tinyurl.com/4n9kctaf

Decreto 1874 de 2021. Por el cual se modifica la estructura del Ministerio de Defensa Nacional, se crean nuevas dependencias, funciones y se dictan otras disposiciones. Ministerio de Defensa Nacional. https://tinyurl.com/yw6fz5uk. República de Colombia. (2021).

Díaz-Roman, M. P. (2024). Crimen organizado en el Centro Histórico de la Ciudad de México: paradoja, percepción y evidencia. *Revista Científica General José María Córdova*, *22*(46), 361-382. https://doi.org/10.21830/19006586.1296

Díaz Samper, G. A. J., Molina Garzón, A. L. y Serrador Osorio, L. E. (2024). Aproximación al ciberdelincuente desde la perspectiva del control social. *Revista Criminalidad*, *65*(3), 81-95. https://doi.org/10.47741/17943108.508

Duxbury, S. W. y Andrabi, N. (2024). The boys in blue are watching you: The shifting metropolitan landscape and big data police surveillance in the United States. *Social Problems*, *71*(3), 912-937. https://doi.org/10.1093/socpro/spac044

Elizalde Castañeda, R. R., Flores Ramírez, H. H. y Castro Lorzo, E. M. (2021). Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado. *Ius Comitialis*, *4*(8), 252. https://doi.org/10.36677/iuscomitialis.v4i8.17320

Fernández-Hernández, J. Á. (2024). Eficacia colectiva para dos espacios urbanos en la zona metropolitana del valle de México. *Revista Científica General José María Córdova*, *22*(46), 265-288. https://doi.org/10.21830/19006586.1304

Fontalvo-Herrera, T. J., Vega-Hernández, M. A. y Mejía-Zambrano, F. (2023). Método de clustering e inteligencia artificial para clasificar y proyectar delitos violentos en Colombia. *Revista Científica General José María Córdova*, *21*(42), 551-572. https://doi.org/10.21830/19006586.1117

Forbes. (2024). *Colombia sigue siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM*. Forbes. https://tinyurl.com/4ths8vmy

García Torres, M. L. (2024). Ciberseguridad vs.ciberdelincuencia: obstáculos procesales en la persecución de la ciberdelincuencia organizada. Propuestas para una más eficaz represión de los ciberdelitos. *Ciencia Policial*, *182*, 15-69.

Garzón Pulgar, J. O. y Cuero Quiñones, K. S. (2022). Una mirada a la Cibercriminalidad en Colombia y su asimilación con los delitos de impacto. *Revista Criminalidad*, *64*(3), 203. https://doi.org/10.47741/17943108.373

Gómez, O. y Zapata, S. (2020). Efectividad de la política criminal colombiana hacia la prevención del delito. *Revista Criminalidad*, *62*(3), 103-118.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L. y Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), 1-34. https://doi.org/10.1080/08839514.2022.2037254

Habegger, B. (2022). Securing the future: The use of strategic foresight in the security sector. *Strategic Security Analysis*, *23*, 1-12. https://tinyurl.com/vk6ups8f

Herald, N. E. y David, M. W. (2018). A framework for making effective responses to cyberattacks. *2018 IEEE International Conference on Big Data (Big Data)*, 4798-4805. https://doi.org/10.1109/BigData.2018.8622537

IBM. (2023). *¿Qué es la IA?* https://tinyurl.com/4m9d4at4

Jardine, E., Porter, N. y Shandler, R. (2024). Cyberattacks and public opinion – The effect of uncertainty in guiding preferences. *Journal of Peace Research*, *61*(1), 103-118. https://doi.org/10.1177/00223433231218178

Kochhar, S. K., Bhatia, A. y Tomer, N. (2022). Using deep learning and big data analytics for managing cyber-attacks. En K. Periyaswami, P. F. Katina y S. P. Anandaraj (eds.), *New Approaches to Data Analytics and Internet of Things Through Digital Twin* (pp. 146-178). IGI Global. https://doi.org/10.4018/978-1-6684-5722-1.ch008

Lawson, S. T. yeo, S. K., Haoran Yu y Greene, E. (2016). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. *2016 8th International Conference on Cyber Conflict (CyCon)*, 65-80. https://doi.org/10.1109/CYCON.2016.7529427

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la info. Congreso de la República de Colombia. https://tinyurl.com/mhmdu3tx

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Congreso de la República de Colombia. https://tinyurl.com/bdhz2mba

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Congreso de la República de Colombia. https://tinyurl.com/fevej96c

Ley 1928 de 2018. Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. Congreso de la República de Colombia. https://tinyurl.com/ys2w8dzv

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Congreso de la República de Colombia. https://tinyurl.com/yetf7esd

Macana Gutiérrez, N. (2021). El castigo como institución social. Una aproximación de la literatura a partir del estudio del castigo en los delitos sexuales en Colombia. *Revista Vía Iuris*, *31*, 1-42. https://doi.org/10.37511/viaiuris.n31a1

Manzano-Chávez, L., Jiménez-García, W. y Vega-Torrejon, F. (2024). Validación del concepto de eficacia colectiva. Un estudio en barrios latinoamericanos. *Revista Científica General José María Córdova*, *22*(46), 383-407. https://doi.org/10.21830/19006586.1298

Margulies, P. (2013). Sovereignty and cyber attacks: Technology's challenge to the law of state responsibility. *Melbourne Journal of International Law*, *14*(2), 496-519.

McGinnis, Michael D. (2013). Costs and challenges of polycentric governance: An equilibrium concept and examples from U.S. health care. *SSRN Electronic Journal*, 1-23. https://doi.org/10.2139/ssrn.2206980

Medina Martínez, J. J., Cárdenas Osorio, C. H. y Mejía Lobo, M. (2021). Análisis del phishing y la ley de delitos informáticos en Colombia. *Cuaderno de investigaciones: semilleros andina*, *1*(14), 75-80. https://doi.org/10.33132/26196301.1948

Mejía-Lobo, M., Hurtado-Gil, S. V. y Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de Ciencias Sociales*, *XXIX*(2), 356-372.

Ministerio de Defensa Nacional. (2024). *Seguimiento a indicadores de seguridad y resultados operacionales junio 2024*. Ministerio de Defensa Nacional.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). *Acerca de colCERT*. https://tinyurl.com/2btchxrx

MinTIC. (2023). *Ministro TIC presenta la estrategia de cuatro puntos para hacer de Colombia una potencia en Ciberseguridad*. Cyber Summit. https://tinyurl.com/3bz53uc4

Miró Llinares, F. (2020). Predictive policing: utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement. *IDP: revista de Internet, derecho y política*, *30*, 1-18.

Moynihan, H. (2019). The application of international law to cyberspace: Sovereignty and non-intervention. En *Just Security* (December). Chatham House. https://tinyurl.com/4kszfnyy

Murillo Herrera, J. M. (2023). *Por qué Colombia recibió tantos ciberataques durante primer semestre*. Portafolio. https://tinyurl.com/3dfvhadw

Oatley, G. C. (2022). Themes in data mining, big data, and crime analytics. *WIREs Data Mining and Knowledge Discovery*, *12*(2). https://doi.org/10.1002/widm.1432

Oracle. (2023). *What Is Big Data?* https://tinyurl.com/bdf4aadn

Ostrom, V. (1999). Polycentricity. En Michael Dean McGinnis (ed.), *Polycentricity and Local Public Economies. Readings from the Workshop in Political Theory and Policy Analysis* (pp. 52-74). University of Michigan Press.

Padilla-Oñate, S. (2024). Policía de proximidad y confianza ciudadana. *Revista Científica General José María Córdova*, *22*(46), 289-312. https://doi.org/10.21830/19006586.1297

Pastrana Buelvas, E. y Gehring, H. (eds.). (2019). *Fuerzas Militares de Colombia: nuevos roles y desafíos nacionales e internacionales*. Fundación Konrad Adenauer.

Peña Suárez, J. S. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. *Perspectivas en Inteligencia*, *15*(24), 333-359. https://doi.org/10.47961/2145194X.628

Perafán Del Campo, E. A., Polo Alvis, S., Sánchez Acevedo, M. E. y Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi Et Iudicandi*, *16*(1), 1-45. https://doi.org/10.15332/19090528.6480

PNUD. (2013). Sinopsis: seguridad ciudadana. En *Prevención de Crisis y Recuperación*. Programa de las Naciones Unidas para el Desarrollo. http://www.undp.org/content/undp/en/home/librarypage/crisis-prevention-and-recovery/IssueBriefCitizenSecurity.html

Pons Gamon, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, *20*, 80. https://doi.org/10.17141/urvio.20.2017.2563

República de Colombia. (2011). *Conpes 3701. Lineamientos de política para ciberseguridad y ciberdefensa*. Consejo Nacional de Política Económica y Social. https://tinyurl.com/mw746r4z

República de Colombia. (2016). *Conpes 3854. Política Nacional de Seguridad Digital*. Consejo Nacional de Política Económica y Social. https://tinyurl.com/4tynwubv

Rincón Arteaga, J. A., Quijano Díaz, A., Castiblanco Hernández, S. A., Urquijo Vanegas, J. D. y Pregonero León, Y. K. P. L. (2022). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista Criminalidad*, *64*(3), 95-116. https://doi.org/10.47741/17943108.368

Rodríguez-Ortega, J. D. (2024). El uso de la información ciudadana en la investigación criminal mediante un proceso de innovación tecnológico colaborativo para contrarrestar el hurto a personas en Bogotá. *Revista Criminalidad*, *65*(3), 11-30. https://doi.org/10.47741/17943108.522

Sánchez Barahona, S. (2021). Perfiles del ciberdelito: un campo de estudio inexplorado. *Revista de Derecho*, *30*, 67-76. https://doi.org/10.5377/derecho.v1i30.12223

Semanate Esquivel, A. y Recalde, L. (2023). El Estado y la defensa del ciberespacio. *Revista de la Academia del Guerra del Ejército Ecuatoriano*, *16*(1), 11. https://doi.org/10.24133/AGE.VOL16.N01.2023.07

Shackelford, S. J. (2013). Toward cyberpeace: Managing cyberattacks through polycentric governance. *American University Law Review*, *62*(5), 1273-1364.

Shackelford, S. J. y Andres, R. B. (2010). State responsibility for cyberattacks: Competing standards for a growing problem. *Georgetown Journal of International Law*, *42*, 972-990.

Sokolov, S., Nyrkov, A., Knysh, T. y Shvets, A. (2021). Countering cyberattacks during information operations. En A. Mottaeva (ed.), *Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020. ISCAC 2020* (pp. 84-100). Springer. https://doi.org/10.1007/978-981-33-6208-6_9

Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, *5*(3), 392-412. https://doi.org/10.1080/23738871.2020.1820546

Tamayo Arboleda, F. L. y Norza Céspedes, E. (2017). Midiendo el crimen: cifras de criminalidad y operatividad policial en Colombia. *Revista Criminalidad*, *60*(3), 49-71.

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229-244. https://doi.org/10.1093/jcsl/krs019

Valencia Casallas, O. L. (2020). Delitos de corrupción en Colombia: variables socioculturales, institucionales y criminológicas. *Diversitas*, *16*(1), 181-199. https://doi.org/10.15332/22563067.5550

Vargas Borbúa, R., Reyes Chicango, R. P. y Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, *20*, 31-45. https://doi.org/10.17141/urvio.20.2017.2571

Vargas, N. (2023). *Las empresas que han sido blanco de ciberataques en Colombia en el último año*. La República. https://tinyurl.com/3d5pasey

Verhelst, H. M., Stannat, A. W. y Mecacci, G. (2020). Machine learning against terrorism: How big data collection and analysis influences the privacy-security dilemma. *Science and Engineering Ethics*, *26*(6), 2975-2984. https://doi.org/10.1007/s11948-020-00254-w

Villalobos Fonseca, 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.

Yamin, M. M., Ullah, M., Ullah, H. y Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, *57*, 1-35. https://doi.org/10.1016/j.jisa.2020.102722