



SEGURIDAD CIUDADANA EN LA ERA DE LA INTERCONECTIVIDAD GLOBAL: DESDE UNA VISIÓN SOCIOPOLÍTICA

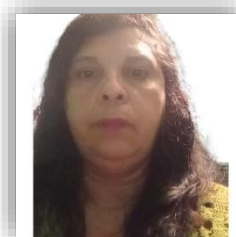
CITIZEN SECURITY IN THE ERA OF GLOBAL INTERCONNECTIVITY: FROM A SOCIOPOLITICAL PERSPECTIVE

Ligia Mercedes Olivares Herrera

Especialista en Procesal Penal. Abogado
Asesor Jurídico en la prefectura Corazón de Jesús.
Municipio Barinas Edo. Barinas -Venezuela

Correo electrónico: ligiaolivares123@gmail.com

Código ORCID: <https://orcid.org/0000-0002-4503-2853>



Recibido: 13/05/2026 **Aprobado:**20/06/2026

RESUMEN

El presente estudio se enfocó en analizar la transformación de la seguridad ciudadana en la era de la interconectividad global, el cual reviste el uso de las tecnologías digitales. Desde una visión sociopolítica, la transición de la seguridad ciudadana hacia el plano digital exige reconfigurar las obligaciones del Estado. En función de este contexto, la investigación asumió una postura epistemológica basada en la teoría crítica, empleando un diseño cualitativo de tipo documental-analítico. Enfocado al método deductivo se constituyó como el eje conductor para examinar, de manera sistemática, la relación existente entre la seguridad ciudadana y el entorno virtual en cuanto a la protección de los derechos humanos. Los resultados demuestran la existencia de una delgada línea entre las políticas de ciberdefensa del Estado y la simultánea vulneración de los derechos humanos. Se concluye, analizar estos fenómenos con el foco puesto en los mecanismos, ejercicio y distribución del poder otorga una perspectiva analítica crucial en el plano político-jurídico, dotando a la investigación de una estricta pertinencia institucional. En el contexto de una sociedad en red, esta conceptualización permite comprender que la seguridad ciudadana ya no se gestiona de manera unidireccional por el aparato estatal, sino que se disputa como una co-construcción en los espacios virtuales-globales define la interconectividad. De este modo, la vinculación de esta temática con la línea de investigación de Estado, Derecho y Justicia, así como con las directrices estratégicas del Plan de la Patria, adquiere una profunda relevancia al responder con rigor a las demandas actuales del contexto universitario venezolano.

Palabras clave: Seguridad Ciudadana, Interconectividad Global, Derechos Humanos Digitales, Visión Sociopolítica.



BA2018000023

ABSTRACT

This study focused on analyzing the transformation of citizen security in the era of global interconnectivity, particularly regarding the use of digital technologies. From a sociopolitical perspective, the transition of citizen security to the digital realm requires a reconfiguration of the State's obligations. Within this context, the research adopted an epistemological stance based on critical theory, employing a qualitative, documentary-analytical design. The deductive method served as the guiding principle for systematically examining the relationship between citizen security and the virtual environment in terms of human rights protection. The results demonstrate the existence of a fine line between state cyber defense policies and the simultaneous violation of human rights. It is concluded that analyzing these phenomena with a focus on the mechanisms, exercise, and distribution of power provides a crucial analytical perspective in the political-legal sphere, giving the research strict institutional relevance. In the context of a networked society, this conceptualization allows us to understand that citizen security is no longer managed unidirectionally by the state apparatus, but rather is contested as a co-construction in virtual-global spaces that define interconnectivity. Thus, the connection of this topic with the research line of State, Law, and Justice, as well as with the strategic guidelines of the Plan de la Patria (Homeland Plan), acquires profound relevance by rigorously addressing the current demands of the Venezuelan university context.

Keywords: Citizen Security, Global Interconnectivity, Digital Human Rights, Sociopolitical Vision.

INTRODUCCIÓN

La seguridad ciudadana en la era de la interconectividad global, experimenta una profunda transformación impulsada por el uso generalizado de tecnologías digitales y plataformas sociodigitales. Tradicionalmente, el análisis de este fenómeno se ha abordado desde una perspectiva sociopolítica que prioriza el enfoque macroestructural e institucional. Bajo este paradigma clásico, la atención se centra rigurosamente en el Estado como la institución matriz cuyo objetivo fundamental es la organización y el ejercicio legítimo del poder (Morán et al., 2024). En el contexto de una sociedad en red, esta conceptualización ampliada permite entender que la seguridad ciudadana ya no se gestiona de manera unidireccional por el aparato estatal, sino que se disputa y co-construye en los espacios virtuales y globales de la interconectividad.



BA2018000023

En el caso de Venezuela, este proceso analizado desde una perspectiva sociopolítica impacta de manera directa en áreas críticas como la seguridad ciudadana y la interconectividad. Como señala la literatura reciente, específicamente la transición de la seguridad ciudadana hacia el plano digital exige reconfigurar las obligaciones del Estado moderno en la era de la interconectividad. Por un lado, Tapia Hernández et al. (2021) demuestran que las amenazas en la red, aunque parezcan intangibles, vulneran derechos humanos fundamentales como la intimidad, la integridad psicológica y el patrimonio de las personas. Esta realidad transforma la ciberseguridad en un asunto de orden público. Ante este escenario, la respuesta gubernamental no puede limitarse a la informática tradicional; tal como señala Cano (2024), se requiere una visión sociopolítica donde la ciberdefensa y la gobernanza de datos actúen como capacidades estratégicas del Estado para anticipar riesgos y salvaguardar de manera holística la estabilidad democrática y ciudadana.

Es en la dimensión político-jurídica donde emerge uno de los desafíos más críticos del contexto actual. Existe una delgada línea entre la respuesta institucional que brinda el Estado para la protección de la seguridad en el entorno virtual y la simultánea vulneración o indebida limitación a los derechos humanos fundamentales. Acciones estatales que pretendan mitigar los riesgos digitales corren el peligro de traducirse en intromisiones que afecten la privacidad, la intimidad y la no intervención de comunicaciones privadas, entre otros derechos esenciales. Lejos de incidir positivamente en la solución de las amenazas, estas extralimitaciones institucionales ponen en cuestión las certidumbres tradicionales sobre la naturaleza del poder y legitimidad de su ejercicio (Morán et al., 2024). Por ende, el problema en Venezuela no se reduce únicamente a combatir los delitos informáticos para sino a determinar cómo el Estado puede garantizar una seguridad en red eficiente sin que el control tecnológico devenga en un detrimento de las garantías ciudadanas están vinculadas a esta profunda tensión entre seguridad, soberanía digital y derechos fundamentales con la línea de investigación de Estado, Derecho y Justicia, así como con las directrices estratégicas del Plan de la Patria (2026-2031), le otorga a este proyecto la pertinencia institucional y social obligatoria en el contexto universitario venezolano actual, al buscar un equilibrio armónico entre la protección colectiva y el respeto normativo.



BA2018000023

Frente a esta fragilidad civil, la respuesta gubernamental requiere una transformación profunda, en la ciberseguridad ha dejado de ser un asunto puramente técnico para convertirse en un instrumento crítico de política estatal y resiliencia nacional. Así, el diseño de estrategias de ciberdefensa y gobernanza de datos debe articularse bajo un enfoque holístico que anticipe los riesgos geopolíticos de la red sin convertir al Estado en un ente opresor o hipervigilante. El objetivo central de esta investigación es analizar cómo la ciberseguridad, lejos de ser un campo puramente informático, constituye el eje articulador de la seguridad ciudadana contemporánea, donde la preservación de los derechos humanos en el entorno virtual representa el mayor desafío sociopolítico de los Gobiernos en la era interconectada.

Dicho fenómeno erosiona directamente, en la seguridad ciudadana en la era de la interconectividad global, trasciende los límites geográficos tradicionales. En la actualidad, la lucha contra el crimen organizado y el terrorismo fenómenos que ya no conocen fronteras exige el reconocimiento formal de redes transnacionales de apoyo y respuesta. En consecuencia, se vuelve indispensable intensificar la cooperación internacional y optimizar el intercambio de información en tiempo real. Solo mediante una gobernanza interconectada es posible vislumbrar estrategias efectivas que neutralicen las amenazas globales que afectan directamente la tranquilidad al entorno global. Desde una visión sociopolítica, ha reconfigurado profundamente el ejercicio del poder, la participación ciudadana y la gobernanza. Las nuevas plataformas han transformado el espacio público tradicional al descentralizar el control de la narrativa política, lo cual ha acelerado tanto el empoderamiento social como la polarización. En este contexto, Venezuela se ha convertido en un escenario principal de disputa geopolítica y ciberdefensa, donde las organizaciones y el Estado deben articular nuevas estrategias de seguridad más allá del territorio físico.

Frente a la realidad descrita en el plano geopolítico, se vuelve indispensable adoptar estrategias avanzadas de protección. En este sentido, Cano (2024) propone un modelo de ciberdefensa basado en retos, datos y aprendizaje; esta estructura integrada permite concebir la información como un vínculo esencial para proteger de manera integral tanto a las empresas como a las naciones. Esta perspectiva estratégica no solo resguarda la infraestructura soberana, sino que redefine por completo la seguridad en el ecosistema virtual. A partir de ello, la doctrina legal



contemporánea, ha tenido que evolucionar tal como señala Núñez (2025), en este entorno se identifican nuevos derechos fundamentales digitales: la existencia digital, la identidad digital, el honor y la reputación digital, la libertad y responsabilidad digital, la privacidad, el anonimato, el olvido, el domicilio digital y el derecho a la paz en el ciberespacio.

Cada una de estas prerrogativas es analizada desde una perspectiva constitucional, técnica y social, lo que destaca su contenido esencial y delimita con precisión las obligaciones correspondientes tanto al Estado como a los actores privados. Es importante destacar que esta interconexión exige un enfoque multidimensional que contemple no solo la seguridad física, sino también la protección de los derechos humanos y la promoción de la justicia social (Rodríguez, 2024). Bajo esta premisa, el papel que juega la seguridad ciudadana se erige como un factor crucial que involucra una alta complejidad dentro del entorno virtual. En este espacio coexisten delitos que utilizan la red como un medio de comisión y delitos que surgen de manera nativa dentro de dicho entorno. En el caso de los primeros, las conductas delictivas ya se encuentran tipificadas en los códigos penales tradicionales, por lo que el infractor simplemente utiliza el ecosistema virtual como una herramienta tecnológica para ejecutar el delito.

Este análisis cobra una relevancia fundamental a la luz de los planteamientos de Vasco (2025), quien argumenta que las dinámicas sociales y las estructuras políticas interactúan de manera profunda, moldeando la organización colectiva y la relación entre los individuos y el Estado. Desde esta perspectiva sociopolítica, se subraya que las políticas públicas no deben ser interpretadas únicamente como herramientas de control, sino como vehículos esenciales para fortalecer el tejido social y construir confianza colectiva ante las transformaciones de las sociedades contemporáneas. Esto se traduce en un fenómeno político donde la protección de la dignidad humana exige adaptar el marco constitucional al nuevo entorno digital, reconociendo y garantizando los derechos de cuarta generación como herramientas indispensables para preservar la libertad, la autonomía y el bienestar del individuo en el ciberespacio.

Frente a esta concepción, termina reduciéndose en los supuestos jurídicos establecidos juegan un papel determinante en la preservación del orden social; un claro ejemplo de ello es el artículo 55 de la Constitución de la República Bolivariana de Venezuela (1999), el cual instituye



BA2018000023

el derecho de los ciudadanos a la protección por parte del Estado frente a situaciones de amenaza o vulnerabilidad. No obstante, en la era de la interconectividad global, las hipótesis de hecho generadas por el avance tecnológico y las complejas situaciones que se suscitan en el entorno virtual rebasan constantemente las garantías constitucionales tradicionales, exigiendo una urgente actualización de los mecanismos de tutela digital.

En consecuencia, la transición de la seguridad ciudadana hacia el entorno virtual representa uno de los desafíos sociopolíticos más complejos de la era de la interconectividad global. El análisis desarrollado demuestra que el ciberespacio ha dejado de ser un mero canal de comunicación para convertirse en un territorio geopolítico en disputa, donde las amenazas digitales trascienden las pérdidas económicas e impactan directamente la integridad psicológica, el patrimonio y las libertades fundamentales de los ciudadanos. Ante esta realidad, los marcos normativos tradicionales se enfrentan a una mutación constitucional por vía interpretativa; si bien el artículo 55 de la Constitución de la República Bolivariana de Venezuela (1999) consagra la obligación del Estado de proteger a la población ante situaciones de vulnerabilidad, las dinámicas y transfronterizas de la red rebasan constantemente los supuestos jurídicos convencionales.

Por lo tanto, garantizar el orden público y la justicia social en el siglo XXI, exige un cambio de paradigma estatal. Tal como se argumentó a lo largo de este ensayo, la solución no radica en la implementación de políticas punitivas o hipervigilantes que sacrifiquen las libertades civiles en nombre del control, sino en la adopción de un modelo multidimensional de ciberdefensa basado en la gobernanza de datos y el aprendizaje continuo. El Estado y los actores privados deben articular esfuerzos para reconocer y tutelar los nuevos derechos fundamentales digitales tales como la identidad, el olvido y el derecho a la paz en el ciberespacio. En última instancia, el éxito de la seguridad ciudadana contemporánea dependerá de la capacidad de los Gobiernos para construir un ecosistema digital resiliente, donde la tecnología sirva como un vehículo para fortalecer el tejido social y blindar, de manera irrenunciable, los derechos humanos en la era interconectada. Esto conlleva en líneas generales a dilucidar las siguientes discutas: ¿Cuál es la relación entre la interconectividad global y la seguridad ciudadana dese una visión sociopolítica?



FUNDAMENTACIÓN TEÓRICA

Desde una perspectiva macroestructural, se puede comprender cómo diversos elementos e instituciones interactúan entre sí y de qué manera estas dinámicas configuran los grandes procesos de interconexión, intercambio y transformación en la historia global. No obstante, las narrativas predominantes tienden a centrarse en patrones generales tales como la expansión de imperios, el comercio transnacional, la migración y el desarrollo tecnológico, dejando de lado los matices y las contribuciones específicas de ciertas regiones. Al respecto, Aranibar (2025) señala que este enfoque globalizador suele omitir las particularidades de cada sociedad, invisibilizando dinámicas locales cruciales. En razón de esto, la lógica del Estado contemporáneo debe analizarse a partir de un proceso histórico actual, donde la globalización se manifiesta como un entramado complejo de interdependencias sociopolíticas, económicas y culturales. Este fenómeno se traduce, en última instancia, en la consolidación de la denominada sociedad en red, la cual surge como corolario de la creciente desterritorialización de las interacciones humanas en el ecosistema virtual.

En ese sentido, la interconectividad global y la seguridad ciudadana plantean un equilibrio complejo que debe gestionarse con rigurosidad, dadas las profundas desigualdades y tensiones sociales que coexisten dentro de las comunidades. Por lo tanto, las políticas de seguridad ciudadana deben orientarse de manera explícita hacia la promoción de la dignidad humana, erradicando prácticas discriminatorias que vulneren a los grupos más desfavorecidos de la sociedad en red. Desde una perspectiva estructural, los supuestos jurídicos establecidos juegan un papel determinante en la preservación del orden social y el resguardo civil ante las transformaciones de las sociedades contemporáneas. Con relación a esto, Guerra et al. (2023) sostienen que la eficacia de estos marcos normativos depende de su alineación con las dinámicas de poder vigentes y las realidades sociales. Un claro ejemplo de ello es el artículo 55 de la Constitución de la República Bolivariana de Venezuela (1999), el cual instituye formalmente el derecho de los ciudadanos a la protección por parte del Estado frente a situaciones de amenaza, vulnerabilidad o riesgo a su integridad física y patrimonial.



No obstante, en la era de la interconectividad global, estas hipótesis de hecho sufren una mutación profunda, debido a que el avance tecnológico y las complejas situaciones que se suscitan de forma nativa en el entorno virtual rebasan constantemente el alcance de las garantías constitucionales tradicionales. En consecuencia, las amenazas a las que se enfrentan los usuarios en el ciberespacio ya no solo repercuten en el ámbito estrictamente económico, sino que vulneran de manera directa la esfera de la seguridad integral, provocando graves afectaciones a los derechos humanos y exigiendo una urgente adaptación institucional. Para Morán (2024), la consolidación de un orden global capaz de abordar problemas complejos, regular las relaciones entre las naciones y garantizar los derechos emergentes de la globalización sociopolítica, requiere la integración de múltiples enfoques teóricos.

Esta mirada integral contribuye a una comprensión más profunda y realista de los fenómenos que moldean a la sociedad contemporánea. Bajo esta premisa, el autor realza que un sistema multilateral enfocado en la lucha contra la delincuencia transnacional exige la adopción de instrumentos jurídicos e informáticos innovadores. Estas herramientas deben permitir a los gobiernos y a las organizaciones internacionales responder de manera eficaz a las amenazas criminales modernas, actuando conforme a los tratados internacionales y en estrecha armonía con cada legislación interna. De este modo, la acción coordinada se mantiene sólidamente sustentada en los principios que definen el fenómeno adopta una visión integral para entender el pacto social con respecto al ordenamiento jurídico, el cual se fundamenta en la Interconectividad Global y la Seguridad Ciudadana desde una visión sociopolítica.

Ante esta figura, se asume una postura epistemológica fundamentada en la teoría crítica. Este enfoque implica concebir el conocimiento como un constructo sustentado en el contexto histórico-cultural, donde la participación activa de los sujetos resulta indispensable para propiciar la transformación de la realidad y la comprensión de las nuevas dinámicas sociopolíticas. Bajo esta premisa, la investigación se orienta hacia la necesidad de fomentar políticas institucionales y alternativas de acción que impulsen la praxis social desde los centros de investigación y las universidades. De este modo, la producción de conocimiento tecno-jurídico no se limita a la



abstracción teórica, sino que se articula de forma directa con la formación esencial de los futuros ciudadanos en la era interconectada.

MATERIALES Y MÉTODOS

La presente investigación se desarrolló mediante un diseño cualitativo con un enfoque de tipo documental-analítico. Este método deductivo se constituyó como el eje conductor para examinar, de manera sistemática, la relación existente entre la seguridad ciudadana en la era de la interconectividad global y su influencia directa en la protección y el ejercicio de los derechos humanos, desde los preceptos generales contenidos en la normatividad venezolana para analizar la forma en que estos se manifiestan en casos concretos relacionados con el entorno virtual.

A partir de lo anterior, se infiere en el método inductivo a nivel macroestructural, a través del estudio de fenómenos jurídicos específicos y realidades digitales particulares, lo que permite inferir el contenido esencial de los derechos humanos y delimitar sus fronteras en la norma actual. Por otra parte, el método exegético se emplea rigurosamente en el análisis de la connotación del derecho al olvido, facilitando la exploración de la problemática contemporánea derivada de la omisión o mutación constitucional sobre el tema. Por último, en lo que respecta al método comparativo, se efectúa un examen de las diversas formas de interpretar y comprender el Derecho frente al uso de las tecnologías de la información; esta técnica permite contrastar las conductas delictivas virtuales con esos mismos comportamientos en entornos analógicos, estableciendo además un paralelo analítico con las respuestas jurídicas formuladas por Vasco et.al. (2025), propone un modelo que analiza el entorno virtual, permite un viaducto en relación a la Seguridad ciudadana en la era de la interconectividad global, pretende destacar la importancia que reviste el enfoque humanista.



BA2018000023

ANÁLISIS DE RESULTADOS

En relación a la aplicación de los métodos deductivo, exegético y comparativo descritos en el apartado metodológico permite evidenciar que el entorno virtual ha dejado de ser un espacio neutral para convertirse en un vector crítico de vulnerabilidad ciudadana. A partir del análisis cualitativo del corpus documental, se constata que las amenazas digitales no constituyen fallas técnicas aisladas, sino estrategias sofisticadas de manipulación conductual que impactan de manera directa en el tejido social.

Al respecto, Vasco et. al (2025), identifica las principales técnicas operativas utilizadas mediante la ingeniería social para quebrantar la seguridad de los usuarios. Entre estos hallazgos, destacan prácticas recurrentes como la suplantación de identidad del personal corporativo para extraer información confidencial y el envío masivo de correos electrónicos fraudulentos comúnmente asociados al *phishing*, cuyo propósito es inducir a las personas a revelar credenciales de acceso. Asimismo, el autor señala el uso de ventanas emergentes diseñadas para redirigir el tráfico web hacia portales apócrifos o para ejecutar descargas maliciosas (*malware*) en los dispositivos, así como la difusión de ofertas engañosas a través de plataformas de mensajería instantánea orientadas a la recopilación masiva de datos personales mediante encuestas falsas.

Desde una visión sociopolítica, estos vectores de ataque inciden directamente en los nodos epistémicos de la sociedad contemporánea, donde la información y los datos personales han sido mercantilizados y convertidos en armas de control. Este fenómeno revela que la seguridad ciudadana en el entorno virtual ya no se limita a proteger la infraestructura tecnológica, sino a salvaguardar los flujos de conocimiento y la privacidad del tejido social frente a las nuevas dinámicas de dominación digital. Conlleva estas conductas delictivas virtuales, no solo atentan contra el patrimonio económico de los ciudadanos, sino que vulneran de forma flagrante los derechos fundamentales de cuarta generación definidos en el marco teórico, tales como la privacidad, la identidad digital y el honor. En consecuencia, la existencia de estas amenazas masivas en la red demuestra por qué las hipótesis de hecho de la delincuencia contemporánea rebasan las capacidades de los mecanismos tradicionales de protección analógica, obligando a



replantear las políticas de seguridad ciudadana bajo un enfoque de ciberdefensa del Estado venezolano.

**Tabla N° 1.-
Matriz de Triangulación Teórica y Normativa**

Categoría Apriorística (Eje Central)	Subcategoría/ Dimensión	Indicadores / Variables de Análisis	Hallazgo Técnico / Hallazgo Jurídico	Impacto Sociopolítico / Conclusión Analítica
Seguridad Ciudadana en la Era Digital	Entorno Virtual y Delito	Tipificación del ciberdelito. Delitos nativos virtuales. Uso de la red como medio.	Clasificación de conductas delictivas analógicas trasladadas a internet y delitos que nacen propiamente en el ciberespacio.	Las amenazas virtuales no son intangibles; repercuten directamente en la vida, el patrimonio y la integridad del ciudadano.
Gobernanza y Defensa del Estado	Estrategia y Ciberdefensa	Cultura basada en datos. Resiliencia nacional Hegemonía discursiva.	Modelo conceptual de ciberdefensa basado en cuatro culturas: preguntas, retos, datos y aprendizaje.	La ciberseguridad deja de ser un asunto técnico para convertirse en un instrumento crítico de política de Estado en Venezuela.
Garantías Individuales Contemporáneas	Derechos Humanos de Cuarta Generación	Existencia e identidad digital. Derecho al olvido. Paz en el ciberespacio.	Catálogo de prerrogativas digitales analizadas desde perspectivas constitucionales, técnicas y sociales.	La dignidad humana en el siglo XXI exige la actualización del marco constitucional para blindar la autonomía del individuo en red.
Marco Legal Nacional	Supuestos Jurídicos y Realidad	Artículo 55 Constitucional. • Hipótesis de hecho. • Tutela civil.	Instituye el derecho a la protección del Estado ante situaciones de amenaza o vulnerabilidad.	Las hipótesis de hecho generadas por las tecnologías rebasan las garantías tradicionales, forzando una brecha operativa en el Estado venezolano.
Justicia Social y Cooperación	Multilateralismo y Bienestar	• Instrumentos innovadores. • Tejido social. • Tratados internacionales	Técnicas de ingeniería social (<i>phishing</i> , <i>malware</i>); necesidad de un sistema multilateral contra el cibercrimen transnacional.	Las políticas públicas no deben ser solo herramientas de control; deben ser vehículos para construir confianza colectiva y defender a grupos vulnerables.

Nota. Interconectividad Global: Capacidad técnica y sociopolítica que poseen los sistemas informáticos para mantener a los usuarios en un estado de conexión permanente a través de internet. *Fuente:* Elaboración propia (2026) basado en autores.

Este fenómeno actúa como un canal inmediato que permite a los individuos y a las organizaciones acceder a flujos masivos de información, optimizar el intercambio de datos y alcanzar objetivos estratégicos complejos más allá de las fronteras territoriales tradicionales. Más allá, de trasladar esta matriz de amenazas al escenario específico de Venezuela, se evidencia que



la suplantación de identidad y la recopilación ilícita de datos a través de la ingeniería social adquieren una gravedad de orden público y geopolítico.

En este contexto nacional, tal como señalan Guerra et al. (2023), la efectividad del marco normativo se ve tensionada por las dinámicas del poder y las transformaciones sociales contemporáneas. Las plataformas digitales se han transformado en el teatro de operaciones principal donde se disputa la hegemonía discursiva y el activismo político, lo cual expone a los ciudadanos a riesgos que trascienden el plano analógico tradicional. Ante este panorama, el artículo 55 de la Constitución de la República Bolivariana de Venezuela (1999), que consagra el derecho irrenunciable a la seguridad ciudadana y la protección del Estado se enfrenta a una evidente brecha operativa, puesto que las hipótesis de hecho delictivas ejecutadas en la red rebasan constantemente los mecanismos de tutela física e institucional previstos originalmente.

CONCLUSIONES

A partir del análisis documental-analítico desarrollado bajo el prisma de la teoría crítica y la aplicación del método deductivo, se derivan las siguientes conclusiones fundamentales:

1. La tensión dialéctica entre ciberdefensa y derechos fundamentales. Se confirma la existencia de una delgada y conflictiva línea limítrofe entre las políticas de ciberdefensa implementadas por el Estado y la simultánea vulneración de los derechos humanos en el entorno virtual. Esta tensión no responde a una disfunción técnica, sino a una contradicción estructural propia del ejercicio del poder en la era digital, donde los mecanismos de vigilancia y control, destinados a garantizar la seguridad, terminan frecuentemente erosionando las garantías ciudadanas.
2. La reconfiguración del rol estatal y la gobernanza en red. Se concluye que la seguridad ciudadana ha dejado de ser una competencia unidireccional y excluyente del aparato estatal para transformarse en una co-construcción disputada dentro de los espacios virtuales-globales. Esta transición exige reconfigurar las obligaciones del Estado, que ya no opera como un actor monopólico, sino como



BA2018000023

un agente clave que debe aprender a negociar su autoridad y a ejercer su potestad sancionadora en un ecosistema descentralizado, marcado por la interconectividad y la multiplicidad de actores.

3. El poder como categoría analítica crucial. El enfoque en los mecanismos, ejercicio y distribución del poder ha demostrado ser una perspectiva analítica de estricta pertinencia político-jurídica. Esta óptica permite desvelar que la vulneración de los derechos humanos en el ciberespacio no constituye un mero efecto colateral de la seguridad, sino un riesgo sistémico vinculado a la asimetría de poder y a la concentración de capacidades tecnológicas en manos estatales o privadas, lo cual otorga a la investigación una profundidad crítica necesaria para desnaturalizar discursos hegemónicos.

4. Pertinencia institucional y alineación estratégica en el contexto venezolano. La investigación adquiere una relevancia sustancial al vincularse orgánicamente con la línea de investigación Estado, Derecho y Justicia y con las directrices estratégicas del Plan de la Patria. En este sentido, las conclusiones aportan insumos teóricos y críticos para repensar las políticas públicas venezolanas desde la academia, respondiendo con rigor a las demandas contemporáneas de justicia, equidad y protección de la soberanía digital, sin desatender el imperativo ético de salvaguardar la dignidad humana frente a los excesos del control tecnológico.

En definitiva, el estudio concluye que la gestión de la seguridad ciudadana en el contexto de la sociedad red exige un replanteamiento profundo del pacto social y jurídico vigente. La protección estatal debe ejercerse bajo un paradigma de gobernanza digital participativa y descentralizada, donde la eficacia en la ciberdefensa no se logre a expensas de las libertades civiles, promoviendo así un equilibrio dinámico que responda tanto a los desafíos de la interconectividad global como a las particularidades del orden sociopolítico venezolano.



BA2018000023

REFERENCIAS

- Aranibar Ramos, E. R., Zanabria Cabrera, L. C., y Daza Ramos, I. H. (2022). Seguridad Ciudadana A Través De Visiones Contrapuestas: Enfoques Desde La Realidad Social en América Latina. *Revista de Filosofía*, 39(Edición Especial 2), 379-390 _
<https://produccioncientificaluz.org/index.php/filosofia/article/view/39058>
- Constitución de la República Bolivariana de Venezuela. (1999). Gaceta Oficial N° 36.860 (Extraordinaria), 30 de diciembre de 1999.
<https://www.asambleanacional.gob.ve/storage/documentos/botones/constitucion-nacional-20191205135853.PDF>
- Cano, J. J. (2024). Seguridad y ciberseguridad 2009-2019. Lecciones aprendidas y retos pendientes. *Revista Sistemas*, (155), 81–94.
https://www.researchgate.net/publication/342048759_Seguridad_y_ciberseguridad_2009-2019_Lecciones_aprendidas_y_retos_pendientes.
- Guerra Yakeline y Olivares Ligia (2023). La seguridad Ciudadana en la nueva era de la globalización del siglo XXI. *Revista Faces* 5 (1) 1-24. Universidad de Carabobo Venezuela.
<https://servicio.bc.uc.edu.ve/faces/revista/evol5n1/art06.pdf>.
- Ley Orgánica del Plan de la Patria de las 7 Grandes Transformaciones 2026–2031. *Gaceta Oficial de la República Bolivariana de Venezuela*, N.º 6.442 (Extraordinaria).<https://accesoalajusticia.org/ley-organica-del-plan-de-la-patria-de-las-7-grandestransformaciones/>.
- Morán Calvo-Sotelo, M. L., y Benedicto Millán, J. (Eds.). (2024). *Poder y política: el análisis sociopolítico en un mundo de incertidumbres*. Marcial Pons / Universidad Autónoma de Madrid, Cátedra de estudios iberoamericanos Jesús de Polanco.https://www.marcialpons.es/media/pdf/primeras_pags_poder_poltica.pdf
- Núñez Robinson, R. (2025). Los derechos fundamentales en el ciberespacio. *THEMIS Revista De Derecho*, (88), 33–63. <https://revistas.pucp.edu.pe/index.php/themis/article/view/33549>.
- Rodríguez Mileskii J. (2024). Delitos informáticos: análisis forense de la ciberseguridad en Venezuela. *Revista Arbitrada de la Escuela de Derecho*, (16), 1-110. Fondo Editorial de la Universidad Bicentennial de Aragua.
<https://revistasuba.com/index.php/UBAIUS/article/view/1236/886>



BA2018000023

Tapia Hernández, E. F., Ruiz Canizales, R., & Vega Páez, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Misión Jurídica*, 14(20), 142-158. <https://www.revistamisionjuridica.com/wp-content/uploads/2021/06/08-20-La-importancia-de-la-ciberseguridad-y-los-derechos-humanos-en-el-entorno-virtual.pdf>.

Vasco Delgado, J. C., Ruiz Muñoz, G. F., Macas Padilla, B. A., & León Quiñónez, V. H. (2025). Ciberseguridad y protección de datos personales: desafíos y perspectivas. *Revista Científica Gade*, 5(1), 675-688. <https://revista.redgade.com/index.php/Gade/article/view/642>.