ECOSISTEMAS DIGITALES DE VIGILANCIA E INTELIGENCIA GLOBAL Y SU IMPACTO EN LA SEGURIDAD Y DEFENSA NACIONAL

DIGITAL ECOSYSTEMS OF GLOBAL SURVEILLANCE AND INTELLIGENCE AND THEIR IMPACT ON NATIONAL SECURITY AND DEFENSE

PP. 30-46

Luis Gustavo Castro González
Ejército del Perú
dago2022a@gmail.com
ORCID: https://orcid.org/0009-0001-8025-8989

Emilio Felipe Planas Woll
Centro de Altos Estudios Nacionales – Escuela de Posgrado, Perú
25676088@caen.edu.pe
ORCID: https://orcid.org/0009-0006-1799-7945

Luis Gustavo Castro González, es Coronel de Infantería del Ejército del Perú, Magister en Ciencias Militares, Magister en Docencia Universitaria, con estudios culminados en la Maestría de Inteligencia Estratégica y la Maestría en Defensa y Desarrollo Nacional en el Centro de Altos Estudios Nacionales (CAEN-EPG). Ha realizado los cursos de Resolución de Conflictos Socio Ambientales en la Universidad Católica del Perú, Técnicas de Interrogatorio en la Universidad Tecnológica del Perú, los diplomados de Seguridad Integral en la Universidad Alas Peruanas, y Seguridad de la Información y Ciberseguridad en la Universidad Privada del Norte.

Emilio Felipe Planas Woll es abogado por la Universidad de Lima, Bachiller en Derecho y Ciencias Políticas. Cursó el General Management Program en The Wharton School, University of Pennsylvania; Advanced Management Program, Columbia University; Advanced Certificate for Executives in Management, Innovation and Technology, Massachusetts Institute of Technology Sloan School Management; Executive Program in General Management, MIT Management Sloan School. Postgraduate in Digital Business Emeritus in collaboration with MIT Management Executive Education and Columbia Business School. Aresty Scholar Wharton, University of Pennsylvania.

Recibido: 27 Feb 24	**Aceptado:** 08 May 24	**Publicado:** 17 Jun 24

Resumen

El presente articulo tiene como objetivo identificar los ecosistemas digitales de vigilancia e inteligencia global y cómo estos impactan en la seguridad y defensa nacional. El desarrollo exponencial de la tecnología y la utilización del ciberespacio ha permitido que muchos gobiernos utilicen los sistemas de vigilancia global mediante inteligencia artificial y metadatos; al menos 77 países ya se encuentran usando sistemas públicos de reconocimiento facial, ciudades seguras con técnicas de vigilancia policial inteligente, actividades de inteligencia y contrainteligencia con el monitoreo masivo de las comunicaciones. Este articulo busca determinar con exactitud qué es lo que causa el aumento de vigilancia y conocer las capacidades de estos sistemas. Para abordar el análisis de este problema, se utilizó el enfoque cualitativo mediante un método hermenéutico interpretativo de las categorías de estudio usando la técnica documental. El articulo analiza aspectos como la vigilancia e inteligencia global y la seguridad y defensa nacional. La conclusión más significativa de la presente investigación es que la vigilancia e inteligencia global impactan significativamente en la seguridad y defensa nacional de los países.

Palabras clave: Ecosistema digital, vigilancia global, inteligencia global, seguridad nacional, análisis de inteligencia, seguridad y defensa nacional.

Abstract

This article aims to identify the digital ecosystems of global surveillance and intelligence and how these impact national security and defense. The exponential development of technology and the use of cyberspace has allowed many governments to use global surveillance systems through artificial intelligence and metadata; At least 77 countries are already using public facial recognition systems, safe cities with intelligent police surveillance techniques, intelligence and counterintelligence activities with mass monitoring of communications. This article seeks to determine exactly what is causing the increase in surveillance and to understand the capabilities of these systems. To address the analysis of this problem, the qualitative approach was used through an interpretive hermeneutic method of the study categories using the documentary technique. The article analyzes aspects such as global surveillance and intelligence and national security and defense. The most significant conclusion of this research is that global surveillance and intelligence significantly impact the national security and defense of countries.

Keywords: Digital ecosystem, global surveillance, global intelligence, national security, intelligence analysis, national security and defense.

La seguridad nacional expresa una situación o condición por alcanzar; de tener una sociedad sin amenazas, para lo cual el estado enfrenta preocupaciones y desafíos, que se afrontan mediante la adopción de estrategias de diversa índole. En este escenario es donde se utiliza la tecnología como herramienta para la vigilancia y colección de inteligencia para evitar vulneraciones a la seguridad nacional.

Para este trabajo se estableció como objetivo analizar e identificar los ecosistemas digitales de vigilancia e inteligencia global y cómo estos impactan en la seguridad y defensa nacional, es así que los programas de vigilancia brindan, a las sociedades democráticas, ventajas para enfrentar diversas amenazas como el terrorismo que son de tipo complejo, poco convencionales y sofisticados; sin embargo, hay posiciones encontradas sobre dicho empleo ya que vulneraría algunos derechos fundamentales de las personas.

La vigilancia estatal no es ilegal en sí misma, los gobiernos tienen razones legítimas para la vigilancia, pero el propósito no es imponer represión política y limitar las libertades individuales. Las herramientas de seguimiento y vigilancia global son cruciales para prevenir el terrorismo, además, ayudan a resolver casos problemáticos, así se ha evidenciado con el gasto militar que involucra tecnología de vigilancia de inteligencia artificial; se toma en serio la seguridad y los responsables están dispuestos a invertir importantes recursos. Las herramientas son muy similares entre sí; sin embargo, las tecnologías disruptivas han innovado la forma en que opera el gobierno en monitorear y lo que deciden monitorear, internet ha aumentado el volumen de datos transaccionales o "metadatos" sobre una persona, como información sobre correos electrónicos enviados y recibidos, información de identificación seguimiento de ubicación, seguimiento web y otras actividades en línea.

Para abordar el análisis de este problema, se utilizó un enfoque cualitativo mediante un método hermenéutico interpretativo y un análisis documental con el mapeo conceptual de las categorías de estudio; por tal motivo, los resultados buscan analizar y determinar la relevancia de estos sistemas de vigilancia e inteligencia global en función de lo que se encuentra en la literatura existente, bajo las consideraciones que conlleva las herramientas y avances de tecnología en constante desarrollo.

Resulta importante señalar, que, de acuerdo al análisis de la bibliografía estudiada, las categorías de estudio para la presente investigación son: vigilancia global, inteligencia global y seguridad nacional.

Método

El presente artículo es abordado desde un enfoque cualitativo; con un método hermenéutico interpretativo y como técnica de acopio de información el análisis documental. Al respecto, Dulzaides & Molina (2004) afirma que "el análisis de documentos es una forma de investigación técnica, un conjunto de actividades intelectuales diseñadas para describir y representar de manera sistemática y uniforme documentos para facilitar su recuperación" (p.12). Para a Hernández, Tobón y Vázquez (2015, p. 12) refiere que, "el análisis documental consiste en buscar, seleccionar, organizar y analizar un conjunto de materiales escritos para responder una o varias preguntas sobre un tema". En ese contexto, en el estudio se analizan documentos relacionados con el proceso mediante un proceso de análisis integral de un entorno digital donde la vigilancia e inteligencia global se han constituido en herramientas de alianzas regionales que impactan en la seguridad y defensa nacional, tanto de los países vigilados como lo de los propios que nos vigilan.

Técnica de Análisis

En el presente estudio se empleó el mapeo conceptual; punto de inicio para analizar el material seleccionado en el intento de organizar, sistematizar, construir, transmitir y enseñar conceptos académicos de importancia a partir de seis ejes principales (Hernández, et al., 2015). Al respecto, Vivas y Martos (2010, pp. 95-124) refieren que, "esta estrategia ayuda a organizar y construir conocimientos, promueve el aprendizaje y la adaptación a un nuevo entorno, ya que revela la complejidad de las relaciones entre conceptos". Además, proporciona una mirada global del estado del conocimiento, así como una mirada específica del punto de vista de cada componente en relación con otros componentes y sus conexiones. Una adaptación de este modelo serán seis ejes de la base del análisis permite una comprensión concreta de los aspectos involucrados y las acciones a tomar; estos ejes, se describen en la tabla 1.

Tabla 1

Ejes de la cartografía conceptual y explicación

Eje	Explicación	Pregunta central	Componentes
1. Noción	Conceptualización Términos relacionados a la investigación .	¿Cuál es el concepto de vigilancia total, inteligencia global u otro concepto relacionado al tema?	-Definición actual -Desarrollo histórico del concepto de vigilancia e inteligencia global -Inteligencia Artificial
2. Categorización	Identificar categorías del tema a analizar	¿Qué clases ¿De vigilancia e inteligencia global se identifican?	-Clase inmediatas, realizar un desagregado identificando sus principales dimensiones
3. Características	Identificar los elementos propios del estudio.	¿Cuáles son los elementos que caracterizan a un ecosistema digital y la vigilancia e inteligencia global?	Características claves del enfoque: 1) Transversal, 2) Es global 3) Uso de la tecnología 4) Atiende las necesidades de seguridad y defensa nacional.
4. Diferenciación	Describir la relación y diferencias del tema de estudio con otros enfoques	¿Qué otros enfoques relacionados con la categoría se diferencia la vigilancia e inteligencia global?	Se describen los enfoques o modalidades de la vigilancia e inteligencia global
5. Vinculación	Se describe la relación del tema de estudio con otras teorías relacionado al tema de estudio	¿Cómo se relaciona la vigilancia e inteligencia global con la seguridad y defensa nacional?	Se describen los enfoques o teorías diferentes sobre la comprensión del impacto en la seguridad nacional

Nota. Tomado de Tobón, 2015.

Fases del Estudio

El análisis documental se realizó utilizando la cartografía conceptual de la siguiente forma:

a) Fase 1. Realizar la búsqueda de artículos en revistas indexadas y libros digitales y relacionados con la vigilancia e inteligencia global; principalmente artículos de los últimos ocho años, sin embargo, resultó indispensable ampliar la búsqueda de las fuentes con antigüedad mayor de ocho años relacionados con la investigación.

b) Fase 2. Determinar los criterios para la selección de artículos y libros científicos relevantes para este estudio: 1) Cada documento seleccionado debe tener autor, título y fecha de versión; 2) Abordar uno de los cinco ejes del mapeo conceptual; 3) Adoptar un enfoque que se centre en la vigilancia e inteligencia global que se relacionen principalmente con aspectos y cuestiones de interés planteados en el estudio.

c) Fase 3. Ya seleccionados los documentos de interés, elaborar el mapeo conceptual de acuerdo a los seis ejes propuestos por Tobón (2015).

d) Fase 4. El análisis final de los documentos con el apoyo de expertos en el proceso de inteligencia para revisar y perfeccionar la investigación realizada.

La investigación se realizó utilizando palabras clave mediante la búsqueda a través de los recursos digitales y de otras fuentes como artículos de revistas indexadas, libros que tratan el tema de estudio; cada documento debió seguir ciertos parámetros para ser seleccionados:

a) Relacionada a las palabras claves.

b) Enfocarse en el tema de investigación.

c) Consignar autor, año y responsable de la edición

Tabla 2

Formulación de los términos de búsqueda o palabras clave

Términos	Sufijos y palabras alternativas
Inteligencia global	Colección de inteligencia de todas las fuentes Inteligencia nacional Inteligencia del ciberespacio
Vigilancia global	Vigilancia estatal, vigilancia masiva
Seguridad nacional	Seguridad estatal
Ecosistema digital	Entorno digital

Documentos Analizados

Los documentos más relevantes para la preparación de estudios fueron seleccionados de los repositorios Scopus, Esevir, Scielo, Dialnet, Redalyc y Google Scholar, así como de fuentes primarias como: libros, artículos de investigación y revistas electrónicas profesionales; de esta manera, se describen los principales documentos que cumplen plenamente con los criterios desarrollados en la fase de investigación y sustentan el estudio de acuerdo a la tabla 2.

Tabla 3

Documentos claves seleccionados para el estudio

Documento	País	Titulo	Referencia	Temas
Libro	España	El ecosistema y la economia digital en América Latina	Katz (2015)	Ecosistema digital
				Digitalización
				Economia digital
Libro	USA	Entre cinco ojos: 50 años de intercambio de inteligencia	Wells (2020)	Vigilancia electrónica
				Sigint
Libro	USA	Cinco ojos	Kerbaj (2022)	Ciudadania digital
				Vigilancia
				Datificación
				Snowden
Articulo revista indexada	USA	La expansión global de la IA	Feldstein (2019)	Tecnologia de vigilancia
				Vigilancia de IA
Informe	Parlamento europeo	Sobre la existencia de un sistema mundial de interceptación de comunicaciones	Parlamento Europeo (2016)	Sistema de interceptación
				Respeto vida privada
				Protección ciudadanos
				Espionaje industrial
Articulo revista indexada	USA	Vigilancia digital y democracia cotidiana	Bigo (2016)	Vigilancia digital
				Monitoreo
				Lucha contra el terrorismo
Articulo revista indexada	Reino Unido	Sociedad de Vigilancia y Ciudadania Digital	Hintz, Dencik, & Wahl-Jorgensen (2017)	Ciudadania digital
				vigilancia
				Datificación
				Snowden
Articulo revista indexada	Australia	Hipercolección: un posible nuevo paradigma en Vigilancia moderna	Walker-Munro (2023)	Hipervigilancia
				vigilancia
				Vigilancia moderna
Articulo revista indexada	Canadá	Seguridad contra Vigilancia: La Seguridad TI como Resistencia a la vigilancia generalizada	Zajko (2019)	Vigilancia estatal
				Vigilancia generalizada
				Cinco ojos
				Seguridad y privacidad
Libro	Australia	Vigilancia masiva gubernamental y ley en los paises de los cinco ojos	James (2018)	Vigilancia electrónica
				Vigilancia masiva
				Red global de vigilancia
				Cinco ojos
Articulo revista indexada	USA	La aceptación de la vigilancia digital en la era del big data	Westerlund, Isabelle, Seppo (2019)	Vigilancia digital
				Big data
Articulo revista indexada	España	Vigilancia masiva y opciones de politica tecnológica: mejorar la seguridad de las	Schuster, Berg, Larrucea, Slewe, & Ide-Kostic (2017)	Vigilancia masiva
	Alemania			Cifrado
				Privacidad en linea

Nota. Adaptado de (Tobón, 2015)

Resultados

Nociones y Conceptos

Según Katz (2015) el ecosistema digital es definido "como el conjunto de infraestructuras y prestaciones plataformas, dispositivos de acceso asociadas a la provisión de contenidos y servicios a través de Internet" (p. 12). Además, la universidad europea (2023) llama ecosistema digital a un entorno que utiliza tácticas digitales que interactúan entre sí para obtener un objetivo en un contexto determinado así, por ejemplo: Google, Workspace, Amazon Web Services y Apple.

Esto se relaciona con lo manifestado con Feldstein (2019) que manifiesta que al menos setenta y cinco de 176 países en todo el mundo están utilizando activamente herramientas tecnológicas, sistemas de reconocimiento facial (sesenta y cuatro países) y vigilancia policial inteligente (cincuenta y dos países). Otra definición la brinda, Hintz et al., (2017, p. 734) refiere, que:

> la recopilación de datos, a escala masiva, permite un modo de gobernanza basado en perfilar, clasificar y categorizar a las poblaciones en formas cada vez más proliferantes, el estado, junto con los actores corporativos, llega a dividir y compartimentar según hábitos de consumo, preferencias políticas o la probabilidad de cometer un delito.

Entender lo que es vigilancia global e inteligencia global son conceptos modernos de una era globalizada al respecto (Hintz, et al. 2017) refiere que:

> muchas de nuestras actividades en línea y, cada vez más, fuera de línea, generan datos de ubicación geográfica cuando caminamos con nuestro teléfono móvil; metadatos de nuestra comunicación en línea; datos sobre nuestros gustos y preferencias, datos sobre nuestras actividades en ciudades inteligentes y hogares inteligentes que están cada vez más llenos de sensores. Estos datos son recopilados, almacenados, monitoreados, compartidos y vendidos por servicios de redes sociales, otras plataformas en línea, intermediarios de datos, agencias de inteligencia y la administración pública; impulsado y sostenido por una lógica de acumulación, este orden informativo actual ha sido descrito como capitalismo de vigilancia. (p.2)

Según Schustera, et al. (2017) a pesar de que los metadatos, por definición, no contienen el contenido de un mensaje, su combinación y análisis pueden revelar una cantidad extraordinaria de información, la aplicación de novedosas técnicas de fusión, análisis y procesamiento de datos que trabajan sobre grandes cantidades de datos analizados de diferentes fuentes, comúnmente llamadas Big Data Analytics, que permite identificar patrones y relaciones y sacar conclusiones sobre detalles muy íntimos sobre los hábitos de las personas.

Para (Westerlund, et al. 2021) la vigilancia puede haberse convertido en una condición clave normalizada para vivir en una “sociedad tecnosecuritizada” moderna, como una forma de garantizar la seguridad colectiva. Así, por ejemplo, para James (2018) en EEUU los Cinco Ojos están formados por las agencias de inteligencia de EEUU, Australia, Canadá, Nueva Zelanda y el Reino Unido. Con Estados Unidos como socio principal, su misión es a menudo declarado como "recopilarlo todo": interceptar y recopilar casi toda la información sobre casi todas las personas del planeta.

Harding (2015) manifiesta que, para el público en general, la filtración de secretos detallados de documentos internos de la NSA en junio de 2013 reveló el alcance masivo del espionaje de la NSA, tanto en el extranjero como en el país, la mayoría de estos fueron filtrados por un ex contratista, Edward Snowden. También para Zajko (2019) la vigilancia generalizada y la inseguridad estratégica tienen las consecuencias de hacernos más vulnerables, erosionar la confianza y enfriar la libertad. Hay peligros aún mayores para la democracia cuando estas capacidades secretas se combinan con la voluntad de vigilar el crimen, promover los negocios y manipular el sentimiento público.

Para Snowden (2019) hay varios programas de vigilancia global algunos actuales y otros más antiguos, como PRISM, XKeyscore y Tempora; cinco países occidentales de habla inglesa usan estos programas que tienen como objetivo lograr la conciencia total de la información mediante el dominio de Internet con herramientas analíticas como Boundless Informant.

Otra tecnología disruptiva es la IA, al respecto Lu (2023) dice que;

> la potencia de cálculo, la disponibilidad de datos de entrenamiento y los algoritmos son los tres ingredientes principales para el progreso de la IA y durante las primeras décadas de avances de la IA, la computación, que es la potencia computacional necesaria para entrenar un modelo de IA, creció de acuerdo con la Ley de Moore. (p.2)

Tabla 4

Modelos de IA importantes a través de la historia y la cantidad de cómputo utilizado para entrenarlos

.AI	Año	Flop
Teseo	1950	40
Perceptrón Mark I	1957–58	695,000
Neocognitrón	1980	228 millones
NetTalk	1987	81 mil millones
TD-Gammon	1992	18 billones
NPLM	2003	1.1 petaFLOPs
AlexNet	2012	470 petaFLOPs
AlphaGo	2016	1,9 millones de petaFLOPs
GPT-3	2020	314 millones de petaFLOPs
Minerva	2022	2.7 mil millones de petaFLOPs

Nota. Tomado de Compute Trends Across Three Era of Machine Learning por Sevilla et al. (2022).

Lo anteriormente mencionado nos revela la importancia de los ecosistemas digitales y los nuevos conceptos relacionados a este entorno digital: diversos países utilizan las herramientas tecnológicas y programas informáticos, que permiten realizar actividades de vigilancia digital de manera global, además de utilizar programas de Inteligencia global, buscando recopilar gran cantidad de información o metadatos para dar solución a problemas que permitan proteger a los estados contra las amenazas a la seguridad nacional.

Categorización

Para Feldstein, (2019) el índice de Vigilancia Global de Inteligencia Artificial (AIGS) que mide el uso de la tecnología de vigilancia de IA, tiene la siguiente categorización: ”gasto militar IA, plataformas de ciudades inteligentes/ciudades seguras, sistemas de reconocimiento facial y vigilancia policial inteligente; también describe tecnologías habilitadoras, como la computación en la nube y las redes de Internet de las cosas (IOT)”, que son esenciales para el funcionamiento de las herramientas de vigilancia de IA, las tecnologías habilitadoras no están incorporadas en el índice; así también para Hintz, et al. (2017) “la recopilación de datos, a escala masiva, permite un modo de gobernanza basado en perfilar, clasificar y categorizar a las poblaciones en formas cada vez más proliferantes”; es decir acores estatales y no estatales, nos analizan y clasifican según hábitos de consumo, gustos, ideas preferencias.

Para Westerlund, et al. (2021) se pueden identificar tres grupos de partes interesadas relevantes en el contexto de la discusión que aborda la privacidad en línea y la vigilancia masiva: a) agencias estatales y autoridades responsables de hacer cumplir la ley, b) el mundo empresarial, y c) ciudadanos. Cada uno de estos grupos tiene intereses diferentes y, en ocasiones, pueden entrar en conflicto entre sí, las agencias de seguridad y LEA sostienen que la privacidad es secundaria a la seguridad nacional.

De lo anteriormente descrito se puede decir que la seguridad es una preocupación constante de los estados, para lo cual implementan políticas de seguridad y defensa nacional que buscan el bienestar del estado y de la nación. La seguridad se constituye en un bien público, del cual el estado es responsable de administrar el monopolio del poder usando las herramientas de alta tecnología como la inteligencia artificial y el ciberespacio para proporcionar protección contra las amenazas a la seguridad, permitiendo que se efectúe la toma de decisiones acertadas teniendo en claro las estrategias para alcanzar los objetivos de las políticas de seguridad y defensa nacional.

Caracterización

La vigilancia e inteligencia global, desde el enfoque de un ecosistema se caracteriza por los siguientes elementos:

a) Es transversal: Abarca no solo inteligencia y la seguridad, está presente también en los ámbitos industrial, comercial, salud y consumo.
b) Es global: se concibe como un monitoreo total a todos y en cualquier parte del mundo.
c) Usan alta tecnología: está en constante cambio y mejora por los desarrollos tecnológicos de acuerdo a la ley de Moore, destacando el uso de la IA.
d) Atiende las necesidades de seguridad nacional y de inteligencia empresarial, y del conocimiento con una visión global y un enfoque colaborativo entre países aliados.
e) Colisiona con algunos derechos fundamentales; la vigilancia masiva plantea riesgos significativos, como la libertad de expresión, libertad de asociación, erosión de los derechos fundamentales a la privacidad, y la posibilidad de que la información sea utilizada indebidamente; además, el secreto extremo y el incumplimiento de las leyes sin consecuencias negativas erosionan los principios democráticos de separación de poderes. (James,2018, p. 17)
f) Secreto y falta de transparencia, un estribillo común en la literatura académica, se refiere al secreto de la vigilancia masiva. y la falta de supervisión que deben realizar los otros poderes democráticos en los estados.

Para Bigo (2016) las divulgaciones posteriores a Snowden sobre las prácticas de la alianza Five Eyes destacan las características centrales de la política internacional contemporánea que afecta los derechos humanos, los regímenes liberales y las prácticas democráticas. El surgimiento de los actores de vigilancia transnacional es la dinámica centrífuga bajo la cual la cooperación asimétrica entre las agencias de inteligencia se ha expandido enormemente, mientras que la facilidad de la vigilancia intrusiva de grandes grupos de sospechosos, y la capacidad de legalizar dicha vigilancia ha sido justificada por el contexto de un antiterrorismo global, en opinión de los servicios, los políticos y la mayoría de sus contratistas.

Diferenciación de la Vigilancia e Inteligencia Global

La inclusión de la vigilancia y/o la inteligencia global en relación con el impacto en la seguridad y defensa nacional a veces no queda claro en la teoría o en la aplicación: de inteligencia empresarial o inteligencia competitiva.

Tabla 3

Principales diferencias y similitudes de la vigilancia e inteligencia global

	Vigilancia global	**Inteligencia global**	**Vigilancia empresarial**
Diferencias			Busca beneficio economico Su ambito es el empresarial
Similitudes	Es total Usa ecosistemas digitales Se justifica por razones de seguridad nacional	Es total Usa ecosistemas digitales Se justifica por razones de seguridad nacional	Usa ecosistema digitales

Respecto a los puntos en común de vigilancia e inteligencia global, así como a vigilancia empresarial resaltan su alcance y campo de acción, sin embargo, a la vigilancia empresarial enfoques diferentes se da en su finalidad que es un beneficio económico.

Vinculación

Según Hintz, et al. (2017) la vigilancia global tiene un vínculo entre derechos humanos los ciudadanos digitales y la seguridad, recayendo esta tarea en los responsables políticos; en ese contexto, se dan diversas acepciones equivalentes del término, las cuales considera el estándar mínimo de su enfoque, algunas de las que involucran el costo beneficio. Al respecto Zajko (2019) la ciberseguridad –para los que conducen los estados– es una extensión de los objetivos de seguridad nacional, por lo que no sorprende que incluya los mismos tipos de actividades ofensivas y amenazantes que históricamente se han llevado a cabo bajo la justificación de la seguridad nacional:

los ciudadanos y organizaciones de todo tipo se vuelven inseguras y las capacidades de vigilancia a menudo se priorizan por encima de la confianza y la cohesión social.

Además, según James (2018) existe vinculación con empresas que proporcionan datos de clientes a los gobiernos corporaciones canadienses como las de telecomunicaciones no protegen sus datos y tampoco comparten sus sistemas con la vigilancia Prism de EEUU.

Los gobiernos de todo el mundo han sido duramente criticados por el uso de tecnologías de vigilancia digital para recopilar cantidades masivas de información personal, pero con poca evidencia de que esta vigilancia masiva sea efectiva para mejorar la seguridad de los usuarios de herramientas digitales (Westerlund, et al. 2021, citado por Zhang et al., 2017; Cayford y Pieters, 2018).

Además, para Westerlund, et al. (2021) "la vigilancia por parte de los servicios de inteligencia de los estados nación no se ha limitado a grupos marginados y merecedores de malhechores", sino que la vigilancia digital puede apuntar –a cualquiera y a todos– en una nación, sociedad o comunidad (Dencik et al., 2017). Las organizaciones están intentando beneficiarse de los datos más allá del contexto para que fueron recopilados: crear nuevos negocios (Leminen et al., 2018, 2020). Además, el riesgo de flujos inapropiados de datos confidenciales recopilados en un contexto y difundidos a otro contexto ha aumentado junto con la digitalización (Winter & Davidson, 2019).

Para (Westerlund, et al. 2021) de manera similar, empresas de todo el mundo están recopilando datos electrónicos relacionados con los consumidores y analizándolos para encontrar pistas que ayuden a aumentar la experiencia y la rentabilidad del cliente.

Los descrito en los argumentos antes mencionado nos revela la importancia de comprender los problemas sobre que se puede denominar democratización y transparencia en la vigilancia que hacen los gobiernos y su contraposición con sus críticos por la vulneración de sus derechos sin entender que los gobiernos tratan de proteger a sus ciudadanos contra las amenazas a la seguridad Nacional es decir hay una vinculación entre la vigilancia global y la seguridad nacional.

Discusión

Se evidencia el desarrollo exponencial de los entornos digitales y la transformación de los programas de vigilancia masiva o de inteligencia masiva, así por ejemplo la evolución del programa de vigilancia de Estados Unidos de América y sus aliados, que al principio se denominó BRUSA y después UKUSA, formando una alianza para compartir información e inteligencia, hasta llegar a Cinco Ojos (Five Eyes, o FVEY, por su designación inglesa), esta alianza la conforman Estados Unidos de América, Reino Unido, Canadá, Australia y Nueva Zelanda.

A pesar de la división en la alianza Five Eyes, el hecho de que sea una de las redes de cooperación de inteligencia más integradas del mundo hace que sea poco probable que se rompa, de hecho, su modelo ha sido copiado por otros grupos importantes del país como Nine Eyes o Fourteen Eyes, aunque con una colaboración más limitada buscando compartir sus hallazgos con las agencias de inteligencia nacionales.

Los avances tecnológicos han desempeñado un papel clave en el surgimiento del "Estado de vigilancia", con niveles crecientes de vigilancia estatal, la tecnología de vigilancia se ha expandido rápidamente desde la tecnología de espionaje de años anteriores, como las escuchas telefónicas y las cámaras ocultas o CCTV, hasta los modernos drones y satélites espías, así como diversos sistemas tecnológicos y a menudo autónomos para la ciber vigilancia dirigida y no dirigida que incluyen tecnologías de inteligencia artificial para monitorear y analizar llamadas telefónicas, correos electrónicos, pulsaciones de teclas, mensajes privados, redes sociales, videos y fotografías.

La búsqueda de amenazas a la seguridad nacional y la ciberseguridad ha llegado a amenazar el valor más claramente delimitado de la seguridad de TI. Es decir, la vigilancia –en nombre de la seguridad nacional y cibernética– se ha convertido en una amenaza para la seguridad informática creando como respuesta que la seguridad informática sea más eficiente y menos vulnerada siendo un medio de resistencia.

Conclusiones

Del análisis documental se concluye que existen ecosistemas digitales que se han convertido en sistemas que albergan, interactúan y facilitan la vigilancia global, así como la colección de inteligencia por medios digitales, que tiene un impacto favorable en la seguridad nacional; sin embargo, este impacto se viene cuestionando por las divulgaciones y filtraciones que exponen las formas, medios y plataformas que usan los estados para la vigilancia global.

Hay una tendencia a democratizar y hacer transparente la vigilancia que hacen los estados: organizaciones no gubernamentales y algunos sectores de la población argumentan que hay una vulneración a derechos humanos contra la privacidad permitida con la adquisición de nuevos derechos digitales.

La vigilancia global no es una exclusividad de los gobiernos ni de la función de inteligencia de los estados, esta se ha ampliado hacia otros campos como la actividad industrial y comercial buscando conocer datos, metadatos e identidades digitales que permitan crear patrones, tendencias de consumo y otros aspectos que son utilizados para crear estrategias que permitan generar dinero.

Si bien el gobierno otorga garantías es necesario que exista un profundo secreto en torno a la vigilancia masiva por el interés nacional como la producción de inteligencia, siendo su esencia el secreto, vital para evitar alertar a los actores de amenazas a la seguridad nacional.

Las herramientas de seguimiento y vigilancia global son cruciales para prevenir amenazas como el terrorismo y el crimen organizado; además, ayudan a resolver casos complejos. Así se ha evidenciado –con el gasto militar que involucra tecnología de vigilancia de inteligencia artificial– que se toma en serio a la seguridad y los tomadores de decisiones están dispuestos a invertir importantes recursos. Por tro lado, se destaca que las herramientas son muy similares entre sí; sin embargo, el desarrollo tecnológico ha cambiado la forma en que operan los gobiernos para monitorear y lo que deciden monitorear.

Referencias

Bigo, D. (2016). Digital Surveillance and Everyday Democracy. Leanne Weber; Elaine Fishwick; Marinella Marmo. *The Routledge International Handbook of Criminology and Human Rights, Routledge*,125 - 135, 2016.

Dencik, L., & Wahl-Jorgensen, K. 2017. *Sociedad de Vigilancia y Ciudadanía Digital* – Introducción Revista Internacional de Comunicación, 11, 731-739

Dulzaides Iglesias, M. E., & Molina Gómez, A. M. (2004). Análisis documental y de información: dos componentes de un mismo proceso. *Acimed*, 12(2), 1-21. http://scielo.sld.cu/pdf/aci/v12n2/aci11204.pdf

Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegieendowment. https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en

Hernández-Mosqueda, J. S., Tobón-Tobón, S., & Vázquez-Antonio, J. M. (2014). Estudio conceptual de la docencia socioformativa. *Ra Ximhai*, 10(5), 12. http://www.redalyc.org/pdf/461/46132134006.pdf

Hernández, J. S., & Vizcarra, J. J. (2015). Didáctica para la formación integral en la sociedad del conocimiento. Horson ediciones. México. 2015

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2017). Digital citizenship and surveillance| digital citizenship and surveillance society. *International Journal of Communication*, 11, 9.

Harding, L. (2015). The Snowden Files: The Inside Story of the World's Most Wanted Man. *National Geographic Books*.

Hernández, J. S., & Vizcarra, J. J. (2015). Didáctica para la formación integral en la sociedad del conocimiento. Horson ediciones. México. 2015.

James, A. (2018). *Vigilancia masiva gubernamental y ley en los países de los cinco ojos* (Tesis doctoral, tesis doctoral).

Katz, R. 2015. *El ecosistema y la economía digital en América Latina. Barcelona*: Editorial Ariel; Fundación Telefónica; Editorial Planeta, p.12. http://scioteca.caf.com/handle/123456789/768

Leminen, S., Rajahonka, M., Westerlund, M. y Wendelin R. 2018. El futuro de Internet de las cosas: hacia ecosistemas heterárquicos y modelos de negocio de servicios. *Revista de marketing industrial y empresarial*. 33(6): 749-767.
DOI: https://doi.org/10.1108/JBIM-10-2015-0206

Lu, M. (2023, 18 septiembre). Charted: *The Exponential Growth in AI Computation.* Visual capitalist. https://www.visualcapitalist.com/cp/charted-history-exponential-growth-in-ai-computation

Secretaría de Seguridad y Defensa Nacional - SEDENA (2015). *Doctrina de Seguridad y Defensa Nacion*al.
https://www.esup.edu.pe/wpcontent/uploads/2021/01/8.%20Doctrina%20de%20Seguridad%20y%20Defensa%20Nacional%202015.pdf

Schuster, S., Van Den Berg, M., Larrucea, X., Slewe, T., & Ide-Kostic, P. (2017). Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards & Interfaces*, 50, 76-82. https://doi.org/10.1016/j.csi.2016.09.011

Tobón, S. (2015). *Cartografía conceptual: estrategia para la formación y evaluación de conceptos y teorías*. https://issuu.com/cife/docs/e-book__cartograf__a_conceptual

Tobón, S., Guzmán, C. E., Silvano Hernández, J., & Cardona, S. (2015). Sociedad del conocimiento: Estudio documental desde una perspectiva humanista y compleja. *Paradigma*, 36(2),7-36. https://www.researchgate.net/profile/Sergio_Tobon4/publication/288671205_Sociedad_del_Conocimiento_Estudio_documental_desde_una_perspectiva_humanista_y_compleja/links/568319e508ae1e63f1f01395.pd

Vivas Moreno, A., & Martos García, A. (2010). La cartografía conceptual y su utilidad para el estudio de la lectura como práctica histórico-cultural: El Quijote como ejemplo. *Investigación bibliotecológica*, 24(51), 95-124. http://www.scielo.org.mx/pdf/ib/v24n51/v24n51a5.pdf

Westerlund, M., Isabelle, DA, Leminen, S. (2021). La aceptación de la vigilancia digital en la era del big data. *Revisión de la gestión de la innovación tecnológica*, 11(3): 32-44. http://doi.org/10.22215/timreview/1427

Winter, JS y Davidson, E. 2019. Gobernanza de big data de la información de salud personal y desafíos para la integridad contextual. *La sociedad de la información*, 35(1):36-51

Zajko, M. 2018. Seguridad frente a la vigilancia: la seguridad informática como resistencia a la vigilancia generalizada. *Vigilancia y sociedad* 16(1): 39-52. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

Zuboff, S. (2015). El gran otro: el capitalismo de vigilancia y las perspectivas de una civilización de la información. *Revista de tecnología de la información*, 30, 75–89.