Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), enero-febrero 2026,
Volumen 10, Número 1.

https://doi.org/10.37811/cl_rcm.v10i1

LA PRIVACIDAD DIGITAL EN TIEMPOS DE VIGILANCIA MASIVA

DIGITAL PRIVACY IN TIMES OF MASS SURVEILLANCE

Hoyos Fernandez Nixon
Universidad Cesar Vallejo

Reyna Ferreyros Jose Antonio
Escuela de Posgrado Newman

DOI: https://doi.org/10.37811/cl_rcm.v10i1.22186

La Privacidad Digital en Tiempos de Vigilancia Masiva

Hoyos Fernandez Nixon[1]
nixonhoyosf.22@gmail.com
https://orcid.org/0000-0002-3845-8346
Universidad Cesar Vallejo

Jose AntonioReyna Ferreyros
jrflicenciadosenderecho@gmail.com
https://orcid.org/0000-0002-7730-4841
Escuela de Posgrado Newman

RESUMEN

Este artículo aborda el decimosexto Objetivo de Desarrollo Sostenible que se centra en promover la paz y la justicia mediante instituciones sólidas. Se enfoca en analizar la percepción de los ciudadanos sobre la privacidad digital en un contexto de vigilancia masiva. La metodología empleada es de tipo básica y se enfoca en aspectos cualitativos, con nivel descriptivo. Se utilizo un enfoque basado en la teoría fundamentada y los resultados se basaron en una revisión de artículos académicos y libros relacionados con el tema. En conclusión, la protección de la privacidad en línea es un derecho fundamental que se ve amenazado por la recopilación y supervisión masiva llevadas a cabo por entidades tanto públicas como privadas, lo que ha suscitado preocupaciones sobre el uso de datos y ha planteado cuestiones acerca de la invasión de la privacidad y la violación del derecho a la intimidad y a la libertad de expresión para los ciudadanos. La encriptación se presenta como una medida protectora para preservar estos derechos ante las nuevas capacidades de vigilancia, lo cual hace necesario el establecimiento de legislaciones emergentes para encontrar un equilibrio entre el monitoreo y la preservación de dichos derechos en esta era digital.

Palabras claves: privacidad digital, vigilancia masiva, derecho a la intimidad, derecho a la libertad de expresión, datos personales

[1]Autor principal.
Correspondencia: nixonhoyosf.22@gmail.com

Digital Privacy in Times of Mass Surveillance

ABSTRACT

This article addresses the sixteenth Sustainable Development Goal which focuses on promoting peace and justice through strong institutions. It focuses on analyzing citizens' perceptions of digital privacy in a context of mass surveillance. The methodology used is basic and focuses on qualitative aspects, with a descriptive level. A grounded theory approach was used and the results were based on a review of academic articles and books related to the topic. In conclusion, the protection of online privacy is a fundamental right that is threatened by mass collection and monitoring carried out by both public and private entities, which has raised concerns about data use and raised questions about the invasion of privacy and the violation of the right to privacy and freedom of expression for citizens. Encryption is presented as a protective measure to preserve these rights in the face of new surveillance capabilities, which makes it necessary to establish emerging legislation to find a balance between monitoring and the preservation of said rights in this digital age.

Keywords: digital privacy, mass surveillance, right to privacy, right to freedom of expression, personal data

Artículo recibido: 15 de diciembre 2025
Aceptado para publicación: 22 de enero 2025

INTRODUCCIÓN

En el contexto contemporáneo, la protección de la privacidad digital enfrentó desafíos significativos debido al auge de la vigilancia masiva. En la ciudad de Lima se han planteado preocupaciones significativas sobre el manejo y procesamiento de datos personales por parte de organismos públicos y privados en relación al respeto a la privacidad y la protección de la información personal. La Constitución del Perú del año 1993 garantiza un derecho fundamental en este tema en su art. 2 numeral 6 que establece que: "Cada individuo tiene el derecho a que los servicios informáticos ya sea públicos o privados no divulguen información que afecte a su intimidad personal y familiar". Por lo tanto, este precepto constitucional resulto crucial ya que sirvió como una base legal esencial para proteger la privacidad en un sistema digital cada vez más complejo.

La protección contra la intrusión y la invasion de la privacidad en la vida personal y privada, exteriorizarse se volvió fundamental para proteger la dignidad y la libertad humana. A medida que las empresas y las agencias gubernamentales recopilaban información sensible afectando la reputación, las relaciones y la libertad, la protección del derecho aplicado fue critica y crucial. El art. 2, núm. 6, además de reconocer el derecho a la privacidad, también estableció sus límites y las obligaciones de los servicios que manejaban datos personales, bajo las premisas de legalidad, necesidad y proporcionalidad. Esta regulación devendría un mecanismo crucial para prevenir posibles abusos en la recopilación y manejo de datos, especialmente en el ambiente de la vigilancia masiva.

La privacidad digital, se convirtió en el derecho de los usuarios a proteger sus datos personales mientras navegaban en la red. Así, les otorgaba la facultad de decidir qué información se compartía o pasaba a terceros y cuáles se mantenían resguardadas y confidenciales. Tal derecho, sin embargo, no fue nuevo, en vez estaba íntimamente relacionado con derechos fundamentales, tales como la intimidad de la vida familiar o personal, la libertad de expresión, el honor o la propia imagen.

Todos ellos estaban protegidos y reconocidos en la Carta Magna. Autores Porcelli y Martínez (2020) afirmaban que al ser la red internet una red abierta, no existía ninguna garantía para la intimidad de las personas, es decir, cada vez que un individuo la utilice, va a exponer públicamente y de manera irreversible todo su hacer. Al bajar software o app gratuitas, se está facultando el ingreso a fotos,

archivos y a los contactos personales. En resumen, en la web lo más caro de lo "gratis" eran los datos personales (p. 115).

Del mismo modo, Soler-Martínez (2022) expresaba que el respeto al derecho fundamental de protección de la información en la era digital otorgó sostenimiento a la libertad. Por eso, en un ambiente complejo y dinámico, influenciado por el desarrollo tecnológico, autorizado por la utilización y el destino de la información personal por parte de las personas, el derecho a la confidencialidad y a la seguridad de la información fue un derecho fundamental que aseguró a cada persona el poder sobre sus datos personales identificativos (pp. 101-102).

Los Estados, por consiguiente, debieron haberse asegurado de promulgar "un marco normativo sólido y efectivo para proteger los derechos fundamentales, incluido el derecho a la intimidad". Como el rápido desarrollo tecnológico fue acompañado por lagunas reglamentarias de las normativas sobre leyes débiles y vacíos legales, se pensaba que la legislación "debería haber sido convenientemente armonizada para evitar y prevenir abusos potenciales en sus derechos" (Mormontoy-Pérez, 2024, p. 70).

Por eso, las argumentaciones de Martínez-Devia (2019) el legislador era responsable. Era fundamental que los gobiernos e instituciones se mantuvieran actualizadas y aceleraran las regulaciones gubernamentales sobre las normativas legales en la web, ya que el void legal proveniente de la falta de normativa o de la dificultad de aplicar la existente producía la dificultad de sistemática gestión de AI y data (p. 20).

Como señalaron Rivera-Pineda y Maldonado-Ruiz (2023) la protección de la recuperación de la privacidad en línea en normas se basaba en dos principios de la ley, el consentimiento informado y la seguridad de la información. Aseguraron el control de la recuperación de los datos personales y estuvieron equilibrados con políticas de identificación como la seguridad nacional y la penalización, lo que presentó desafíos reglamentarios en torno al acceso a la información en línea y la libertad de expresión (p. 988).

En la actualidad, la vigilancia masiva de medios de comunicación siguió siendo impreciso en el ámbito global y nacional. No se prohibía intervenir en la recuperación la información y la comunicación privada en un Estado de Derecho Social compuesto por una constitución con derecho a la privacidad, intimidad

y la libertad, por lo que no se permitía intervenir en comunicaciones de ámbito privado sin un propósito legítimo, como la seguridad nacional. Subsanar hacia ambos principios legítimos de lo proporcional y necesario era una de las formas de rescatar un derecho a una confidencia personal (Torres-Gómez, 2021, p. 22).

En ese sentido, Espinosa (2020) señaló que la diversificación de la recuperación del sistema de los órganos de inteligencia, fondos y corporaciones, además de la recuperación de la información personal como usuarios, incrementó las violaciones actuales del derecho a la intimidad y la información personal (p. 135). Ademas, Puerto y Sferrazza-Taibi (2018) señalaron que las divulgaciones de Edward Snowden expusieron a nivel mundial la implementacion de programas de vigilancia masiva por parte de Estados Unidos y sus aliados (p. 209).

En sintesis, la vigilancia masiva en la era digital fue la recolección y análisis extensivo de datos sobre individuos mediante tecnologías digitales para monitorear y controlar actividades.

De acuerdo con las directrices establecidas para la investigación, se planteó la siguiente cuestión como problema general, ¿cómo percibían los ciudadanos la privacidad digital en tiempos de vigilancia masiva?; como el problema específico 1, se formuló: ¿cómo se desarrollaba la encriptación de la privacidad digital en el derecho a la intimidad en tiempos de vigilancia masiva?; de igual forma, se tomó como problema específico 2, ¿cómo se evaluaban las medidas de autenticación de la privacidad digital en el derecho a la libertad de expresión en tiempos de vigilancia masiva?

Una justificación teórica del artículo se derivó de la dirección de necesidad para examinar protección de la privacidad digital involucrando vigilancia masiva y entendiendo los cambios en los principios legales fundamentales. La justificación práctica justificó la privacidad digital que demanda protección de la información personal en cambiante entorno y la necesidad de formular políticas y técnicas intrépidas de acuerdo con art. 2, inc. 6 de la Constitución. La justificación metodológica se derivó de uso de plantilla de análisis documental aplicada en la recolección de datos desde fuentes legales y académicas relacionadas.

El objetivo general del artículo fue analizar cómo los ciudadanos percibían la privacidad digital en tiempos de vigilancia masiva. Como objetivo específico 1, se planteó analizar cómo se desarrollaba la encriptación de la privacidad digital en el derecho a la intimidad en tiempos de vigilancia masiva. Y

como objetivo específico 2, analizar cómo se evaluaban las medidas de autenticación de la privacidad digital en el derecho a la libertad de expresión en tiempos de vigilancia masiva.

METODOLOGÍA

El presente articulo utilizó el enfoque cualitativo. En ese sentido, el autor García (2023) definió que la investigación cualitativa se considera un proceso reflexivo de análisis humano que se aplica en un esfuerzo para lograr una comprensión holística de los comportamientos y percepciones en una sociedad con respecto a un problema en particular. Esta metodología incidía en la interpretación de datos y el análisis de manifestaciones sociales y humanas a través del uso de datos de naturaleza no cuantitativa (p. 198).

El enfoque de investigación utilizado fue básico. De acuerdo con los autores Arisque-Alburqueque et al. (2020) esto se refiere a la generación de conocimiento más profundo de la investigación en la interpretación a través de los cimientos principales de los fenómenos y hechos observables y abarca principalmente estudios teóricos y experimentales (p. 62).

El nivel descriptivo fue empleado en este artículo, el cual fue util debido a su objetivo de detallar el planteamiento del problema. Según lo explicado por Escudero y Cortez (2018) la investigación descriptiva, como su nombre sugiere, busca detallar algo, es decir, dibuja la realidad de ciertos eventos, objetos, personas, grupos o realidades y en la que se busca estudiar. Este tipo de metodología se basa en la descripción precisa de los fenómenos observados con el fin de proporcionar una idea clara y completa de lo que es relevante para el objeto de estudio (p. 21).

El diseño aplicado en la redaccion de este artículo fue la teoría fundamentada, ya que se enfocó en la aplicación de varias teorías basadas en fuentes legales y materiales. Se investigó y se trabajó con una variedad de revistas y libros, tanto físicos como electrónicos, relacionados con el tema de la privacidad digital en la época de la vigilancia masiva. La teoría fundamentada fue explicada por De la Espriella y Gómez-Restrepo (2020) como un método de investigación cualitativa que involucra la deriva de conceptualizaciones emergentes a partir de los datos que se descubren y luego se integran en patrones categorizados a través de un análisis comprensivo. Además, los autores comentaron sobre el uso de un sistema de comparación con consistencia y rigor para estructurar y aplicar la información (p. 127).

En el artículo, se había llevado a cabo un estudio exhaustivo e integral en varias fuentes de datos, tanto internacionales como nacionales. Donde puede realizar la busqueda bibliografica y acceder a fuentes primarias, incluyendo las bibliotecas virtuales de las universidades estatales y particulares, al igual que revisar de documentos de interes disponibles en repositorios de datos como SCIELO, DIALNET, SCOPUS, PROQUEST y otras revistas indexadas.

Asimismo, las palabras clave obtenidas al recopilar la informacion se organizaron en categorías y subcategorías para el análisis. Para Baena (2017) las categorías se definieron como conceptos especializados que permitieron precisar y detallar los juicios científicos (p. 93). Los autores, Rueda-Sánchez et al. (2023) definieron una subcategoría como un conjunto de conceptos que se originaba a partir de una categoría más amplia y general (p. 87).

En el presente artículo, se utilizaron las siguientes categorías y subcategorías en la búsqueda:

Tabla N° 1: Categorias y subcategorias

Categoría 1	
Privacidad digital	
Subcategoría 1 y 2	
Encriptación	**Autenticación**
Categoría 2	
Vigilancia masiva	
Subcategoría 1 y 2	
Derecho a la intimidad	Derecho a la libertad de expresión

Fuente: Elaboración propia (2025)

Dadas la naturaleza del artículo, hemos logrado identificar al análisis documental como la técnica más adecuada. Nos permitía examinar los documentos recopilados, analizando su contenido para llegar a conclusiones basadas en la información que contienen. Los autores Arias y Covinos (2021) señalaron que el análisis documental se definió como un procedimiento que se realiza con el objeto de extraer datos del contenido de los documentos (p. 99).

Por otro lado, el estudio que habíamos realizado se había valido también del método descriptivo. El cual consistió en detallar los resultados de la herramienta utilizada para la recolección de datos, que se basaban solamente en la información que obtenía de las guías de análisis documental. La recolección

de datos se realizó a través de la revisión de la normativa vigente así de como de otros artículos, revistas y libros que estuviera relacionadas con el tema la privacidad digital en tiempos de vigilancia masiva

En relación con el método descriptivo, Guevara-Albán et al. (2020) mencionan que la investigación se considerará descriptiva cuando el investigador conozca a fondo el problema o la realidad, con el fin de narrarla detalladamente consignando o definiendo todos sus componentes. Además, a través de las entrevistas el investigador tuvo la oportunidad de analizar la problematica desde una perspectiva adicional (p. 167).

De acuerdo a Ventura y De Oliveira (2022) la integridad en la investigación era una dimensión emergente de la ética investigativa que guiaba las buenas prácticas científicas y definía los deberes profesionales. Basada en valores como la honestidad, transparencia, respeto, imparcialidad y responsabilidad, esta dimensión abordaba cuestiones esenciales para el ámbito científico y ético (p. 1).

Cabe indicar que la información empleada en el presente trabajo fue recolectada de fuentes pertinentes y verificadas, por cuanto se desarrolló siguiendo los estándares de la institución privada Universidad César Vallejo. Por otro lado, la información fue citada de acuerdo con las normas APA séptima edición, la Resolución Vicerrectorado de Investigación N° 081—2024-VI-UCV y el sistema Turnitin. Por tanto, se pudo garantizar el respeto a los derechos de autor y la integridad académica de acuerdo a la legislación peruana, A fin de asegurar la correcta atribución de fuentes y en consecuencia, evitar el plagio de ideas en el artículo desarrollado.

RESULTADOS Y DISCUSION

RESULTADOS

En esta sección, los resultados de la revisión se presentaron debidamente, incluyendo el tema de la investigación, sus categorías y subcategorías. Se obtuvo información, en donde nos permitió entender de forma integral el tema investigado. En ese sentido, el objetivo general del artículo fue analizar cómo los ciudadanos perciben la privacidad digital en tiempos de vigilancia masiva. La privacidad digital, también considerada privacidad en línea o privacidad de Internet, se refería al derecho de las personas a proteger sus datos personales en la red. Esto incluía la “información confidencial” y la “información personal sensible” solo revelada a amigos cercanos.

El desarrollo tecnológico había agudizado los dilemas relacionados con la privacidad digital, especialmente a partir de la implementación de sistemas de vigilancia cada vez más avanzados. En ese contexto, Mendoza-Armijos (2024) había sostenido que la privacidad digital no debía concebirse como un impedimento para la innovación, si no como un derecho fundamental que requería una protección efectiva en la era de la información (p. 37).

Como afirma, Porcelli (2020) en algunos países iberoamericanos, el derecho a la protección de información personal se ha establecido como un derecho independiente, distinto de la vida privada y el honor. Su objetivo principal ha sido asegurar el control individual sobre la información personal, particularmente en el contexto tecnológico, y proteger otros derechos humanos que podrían verse afectados por intrusiones ilegales o arbitrarias relacionadas con la gestión de datos (p. 469).

Autores como Maqueo y Barzizza (2020) indicaron que el derecho a la protección de datos personales evolucionó con el tiempo para encajar con la tecnología moderna. Aunque se originó en la década de 1970, adquirió una importancia sin precedentes con el surgimiento de Internet: de repente, el mundo se vio invadido por efectos tales como la vigilancia de masas o la aparición del Estado vigilante (p. 28).

Para Cumbreras-Amaro (2020) el derecho a la protección de información personal se extendió más allá del derecho a la intimidad, ya que se activaba en cualquier situación en la que se manejaran datos personales (p. 153). Así, para Casas et al. (2020) el derecho de las personas a resguardar su información personal se manifiesta como la facultad jurídica en virtud de la cual tuvieron la capacidad para disponer y controlar su información personal frente a terceros, autoridades estatales y entidades privadas (p. 11).

En la actualidad, el tratamiento de datos personales preocupa cada vez más, dada la utilización de la inteligencia artificial en este proceso (Murrugarra-Retamozo, 2024, p. 31).

Además, Mendivelso-Jiménez (2024) describieron que la protección y seguridad de la información no solo deben provenir del ámbito jurídico y de las políticas públicas en seguridad digital y criptografía, sino también de la educación preventiva. Esta educación debía incluir el conocimiento de riesgos y métodos de protección, así como experiencias prácticas sobre situaciones de riesgo comunes en la vida cotidiana (p. 7412).

Citando a Delgado-Franco (2019) afirmó que la vigilancia masiva comenzó a ser una realidad concreta a partir de los avances tecnológicos y la creciente importancia de la información porque equivale a una

actividad en contra de la ley del trabajo que rige el derecho humano a la autonomía e invasión a la privacidad y la ley digital bajo la protección de la información. Asimismo, también viola el derecho a la capacidad informativa (pp. 53-54).

Entonces, Rayman-Labrín (2015) manifestó que la vigilancia masiva es un monitoreo sistemático y prolongado de grupos enteros de usuarios en línea porque los usuarios en línea de diversas plataformas web, interacción y generación de grandes volúmenes de datos que son grabados, recopilados, almacenados y analizados para descubrir patrones conductuales, preferencias y rasgos que revelan la identidad de los titulares (p. 206). Desde el punto de vista de Ojeda-Segovia (2020) la vigilancia masiva había representado un riesgo significativamente mayor que cualquier otro mecanismo de control (p. 133).

En diversas ocasiones, los usuarios de plataformas digitales como Facebook o Google aceptaron los términos y condiciones sin comprender que estaban otorgando a estas empresas control sobre su información personal, incluyendo la opción de vender dicha información a terceros. En respuesta a estas situaciones, la Unión Europea estableció la implementación del Reglamento General de Protección de Datos, que exigía a los propietarios de la información un permiso explícito para transferir sus datos.

Además, en lo que respecta al objetivo específico 1, se determinó analizar cómo se desarrollaba la encriptación de la privacidad digital en el derecho a la intimidad en el contexto de la vigilancia masiva. En este caso, la encriptación de datos definidos como un proceso en el que la información clara y comprensible se convierte en texto cifrado. Era un proceso esencialmente complejo que tenía por finalidad garantizar la protección de la información sensible para el acceso no autorizado y la confidencialidad de los datos.

La encriptación de los activos de los datos permitió tanto a las personas individuales como a las organizaciones asegurar los datos y otros activos de la intervención y el uso no autorizado de ciberdelincuentes, hackers y otros actores maliciosos. Asimismo, Carvajal-Chavez (2019) describió que la encriptación era un método utilizado para codificar la información con el fin de protegerla de terceros (p. 983).

Aunado a ello, los autores Sánchez-Muñiz et al. (2023) manifestaron que la encriptación y el uso de contraseñas habían sido métodos cruciales para garantizar la privacidad de la información personal (p.

61). Asi también, Giménez-Palomares y Monsoriu (2023) precisaron que, en la era digital resultaba crucial asegurar el manejo adecuado de la información (p. 22).

Por otro lado, Burbano-Ardila et al. (2021) indicaron que, en 2015, la ONU adoptó la resolución "El derecho a la privacidad en la era digital", para que los Estados protegieran y respetaran la privacidad e intimidad. Esta resolución buscó que los Estados establecieran mecanismos para salvaguardar estos derechos en el entorno digital y ofrecieran herramientas para restablecerlos en caso de vulneración (p. 42).

La intimidad fue reconocida por el derecho internacional de los derechos humanos a través de diversos instrumentos legales, como el art. 12 de la Declaración Universal de Derechos Humanos, el art. 17 del Pacto Internacional de Derechos Civiles y Políticos, el art. 16 de la Convención sobre los Derechos del Niño y el art. 14 de la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares. Estos documentos internacionales establecían que el derecho humano a la privacidad había resguardado frente a las intromisiones ilegales o arbitrarias en la vida familiar, privada, la correspondencia o el hogar, garantizando protección frente a tales interferencias. Además, reconocían que este derecho era esencial para la práctica de la libertad de expresión y para mantener opiniones sin interferencias.

En el ámbito americano, este derecho fue recogido en el art. 5 de la Declaración Americana de los Derechos y Deberes del Hombre y en el art. 11 de la Convención Americana sobre Derechos Humanos de 1969. De manera similar, fue contemplado en el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, en el art. 17 de la Carta Árabe de Derechos Humanos, y en el art.10 del Capítulo Africano: Carta sobre los Derechos y el Bienestar del Niño. En el Perú, el derecho a la intimidad había sido consagrado en el art. 2, inciso 7, de la constitución.

En ese contexto, la jurisprudencia, en el Exp. N° 03485-2012-PA/TC, en su fundamento 20, se había indicado que el derecho a la intimidad se reservaba específicamente para los aspectos más personales y privados de un individuo y su familia, abarcando información sumamente sensible. Entre estos datos, sin pretender ser exhaustivo, se incluían aspectos relacionados con la salud, las preferencias sexuales, así como los sentimientos y emociones de los seres más cercanos.

En ese orden de ideas, Cuevas-Orta (2022) manifestó que el derecho a la intimidad había sido un derecho esencial que otorgaba a las personas la facultad de excluir o restringir el acceso a su vida personal. En la era digital, este derecho fue vulnerado debido a la automatización de los datos, lo que permitió la recolección y el tratamiento sistemático de información personal sin autorización, lo que llevó a una divulgación negligente de la privacidad del individuo (p. 125).

Tal como lo señaló Castro-Jaramillo (2016) el derecho a la intimidad en las plataformas sociales había estado estrechamente vinculado con la gestión de bases de datos personales, particularmente en lo que se refería a la información privada de los usuarios. Por ende, este manejo del derecho puede afectar otros derechos, como la autonomía personal. Es más, fue imperativo que las instituciones estatales intervinieran para proteger este derecho y monitorear la forma en que las plataformas de Facebook, Twitter, Instagram y WhatsApp generaban bases de datos (pp. 124-125).

En la era de la vigilancia masiva, el concepto de intimidad como derecho intentó proteger el campo personal frente al proceso de recolección y tratamiento arbitrario de la información personal realizado por el gobierno y el entorno no estatal. Este derecho aseguraba que los individuos mantuvieran el control sobre su información privada y prevenía su exposición sin consentimiento.

En lo que concernía al objetivo específico 2 se estableció analizar cómo se evaluaban las medidas de autenticación de la privacidad digital en el derecho a la libertad de expresión en tiempos de vigilancia masiva, en concordancia con ello, Romero-Castro et al. (2018) definieron la autenticación como un proceso cuyo objetivo era confirmar la veracidad de algo, sin que necesariamente implicara la verificación de un usuario. A menudo, la autenticación se utilizaba para comprobar si un cambio o dato era correcto y no se limitaba únicamente a las personas, sino que también se aplicaba a sistemas, dispositivos y otros elementos (p. 16).

Asi también, Martínez-Molano y Rincón-Cárdenas (2021) expresaron que autenticar significaba que, una vez identificada una persona, se le proporcionaba una credencial de autenticación que le permitía gestionar el acceso, confirmando así su identidad. En otras palabras, se validaba la identidad digital a partir de la credencial de autenticación entregada (p. 257). La Carta Magna había protegido derechos esenciales y el derecho a la libertad de expresión había ocupado una posición destacada, según se establecía en el art. 2, inciso 4.

Teniendo en cuenta a los autores Vasquez-Cerna et al. (2023) se describió que la correcta aplicación de métodos para detectar ataques, el uso de tecnologías avanzadas para la protección y la adopción de regulaciones éticas rigurosas habían sido considerados esenciales para asegurar una autenticación segura y proteger la privacidad de los usuarios (p. 11). Para, Mejía (2020) la libertad de expresión enfrentó retos impuestos por la dinámica social, siendo uno de los más significativos el entorno digital, donde los parámetros tradicionales para protegerla resultaron a menudo obsoletos (p. 95).

El art. 19 de la Declaración Universal de los Derechos Humanos estableció que “todas las personas tenían el derecho fundamental a la libertad de opinión y de expresión” (Valentine-Martínez, 2022, p. 176). Por consiguiente, Calcaneo-Monts (2021) sostuvo que la libertad de expresión es un derecho protegido desde mediados del siglo XX, había servido como defensa contra actos arbitrarios del Estado. Sin embargo, en el siglo XXI, la transición digital y las redes sociales, que se autorregulaban e imponían sus propias normas, habían redefinido este derecho, sometiendo a los individuos tanto a las regulaciones tradicionales como a las establecidas por las empresas de redes sociales (p. 43).

La libertad de expresión en redes y plataformas digitales tendía a invadir la intimidad y el buen nombre como derechos de las personas (Guillermo-Jiménez y Meneses Quintana, p. 300). En ese sentido, Mejía-Navarrete (2021) describió que la modernidad digital promovió por parte de las corporaciones tecnológicas la apropiación del derecho a la libertad de expresión, creando un "ciudadano-cliente" sumiso a la lógica del mercado. Esto condujo al surgimiento de una “cibercracia”, un régimen digital autoritario dirigido por unas pocas corporaciones como Facebook, Apple, Microsoft, Amazon y Google, las cuales habían dominado la libertad de expresión en las plataformas sociales (pp. 120-121).

La libertad de expresión permitía a las personas expresar sus pensamientos y opiniones de cualquier manera. Existencial tanto a nivel individual como social, la libertad de expresión se manifestaba con mayor frecuencia en el ciberespacio y las redes sociales. En las sociedades democráticas, los ciudadanos tenían el derecho a expresarse sin miedo a ser acosados, censurados, o castigados (Díaz-Giunta, 2023, p. 111).

En los tiempos de la vigilancia masiva, el derecho a la libertad de expresión había sido un derecho fundamental ya que los ciudadanos debían ser capaces de expresar libremente sus pensamientos y opiniones; este derecho protegía la privacidad autónoma en todas las áreas de su vida. Por otro lado, la

encriptación en la privacidad digital es el proceso de codificación de información vital en un formato no legible por personas sin la clave privada adecuada para descifrar los datos.

DISCUSIÓN

Con respecto al objetivo general, se puede señalar que los ciudadanos consideran la privacidad digital en la era de la vigilancia masiva como una seria amenaza para la protección de los derechos fundamentales a la privacidad y la intimidad. En cuanto a esto, Bouzas-Mendes (2023) establece que, el mundo ha cambiado con el desarrollo publicitado de la tecnología, con muchas áreas de la sociedad que aún se pueden ver como mejoradas, pero el lado oscuro de la luna se volvió perceptible en la forma de delitos en línea y amenazas cibernéticas para la ley y el orden (p. 142).

Por su parte Quijano (2022) subraya que la privacidad enfrenta amenazas no solo por parte de entidades públicas, sino también por organizaciones privadas, que pueden tener un poder y capacidad de invasión mayores que los gobiernos debido a su acceso a información personal y su influencia en la interacción social (p. 120).

Por otro lado, Mendoza (2023) señala que, frecuentemente, al hablar del derecho a la salvaguarda de la información personal, se considera que es un derecho reciente que surge con el uso de Internet, la economía digital y el rápido avance de las Tecnologías de la Información y Comunicación (p. 184). Asi también, Ojeda-Bello y Cutié-Mustelier (2021) indican que definir los componentes básicos del derecho a la protección de datos personales es esencial para clarificar su contenido fundamental. Este procedimiento garantiza, así como su aplicación e implementación correctas y establece que los ciudadanos puedan usar y ejercer este derecho (p. 255).

Citando a Barzola-Plúas y Núñez-Ribadeneyra (2025) señalan que la protección de datos personales en la era digital plantea desafíos legales complejos, los cuales exigen una adaptación continua de las normativas y una concienciación activa por parte de los actores involucrados, ya que resulta fundamental para resguardar los derechos fundamentales y garantizar que el desarrollo tecnológico no vulnere la privacidad ni la seguridad de las personas (p. 33).

Sin embargo, para Sánchez-Diaz (2023) afirma la era digital facilita la protección de los derechos humanos. En este sentido, el autor enfatiza que la protección de los derechos humanos afecta la protección en el mundo real y la protección en el mundo virtual. Afirma de inmediato que las

regulaciones y prácticas judiciales actuales son inadecuadas para proteger a las personas en respuesta al rápido aumento del uso de tecnologías y del espacio para compartir información personal y consideran que los usuarios suelen convertirse en productos (p. 13).

De acuerdo con Barreno-Salinas (2024) sostiene que el derecho a la privacidad afronta retos emergentes en el contexto digital, originados por el avance tecnológico, la recolección masiva de datos y las prácticas de vigilancia tanto estatales como corporativas. Aunque existen marcos normativos nacionales e internacionales orientados a la protección de la información personal, persisten vacíos legales, limitaciones en la aplicación efectiva de las leyes y una creciente desigualdad de poder entre la ciudadanía y las entidades encargadas del tratamiento de datos (p. 143).

Para, Castro-Gonzales y Planas-Woll (2024) la vigilancia estatal es legítima cuando se realiza en función del interés general. Sin embargo, la vigilancia no debe emplearse para reprimir o violar la libertad de los individuos. Los sistemas internacionales, entre ellos los de inteligencia artificial fundamentan en el ámbito de la vigilancia global la prevención del terrorismo y la resolución de casos complejos, justificando importantes inversiones (p. 32).

Por consiguiente, Moret-Millás y Sánchez-Gil (2022) afirman que muchas plataformas de redes sociales ofrecen beneficios significativos en diversos sectores. Aunque generan nuevas amenazas a la democracia y los derechos humanos, como el crimen cibernético, la propagación de información engañosa, el retiro de contenido y la vigilancia masiva (p. 288).

De hecho, con respecto al primer objetivo específico, la importancia de la encriptación para la era de la vigilancia masiva inteligente del siglo XXI radica en el hecho de que la encriptación es intrínsecamente un medio vital de cómo la gente mantiene el derecho a la privacidad en lo que ahora se llama a menudo el equilibrio de la vida digital mediante el uso de los datos a través de los gobiernos y entidades privadas. Al mismo tiempo, se debe señalar que este proceso es desafiante, ya que estos documentos digitales modernos no solo son encriptados, sino que también pueden ser controlado por tecnologías avanzadas y porque se debe encontrar el equilibrio correcto entre la seguridad y la privacidad en la misma.

En general, la encriptación en la privacidad digital es el proceso mediante el cual lo que es confidencial en los documentos se convierte en algo prácticamente ilegible para cualquiera que no sea la persona o la entidad.

Por otro lado, Angles-Yanqui (2020) argumenta que el derecho a la intimidad es el derecho de un individuo a proteger su espacio personal para mantener la protección de su existencia, vida familiar e íntima, sin la invasión de terceros. A pesar de su independencia, el derecho a la privacidad se ve afectado por las tecnologías emergentes, como el análisis del big data y el avance de la IA, en cuanto al almacenamiento y la transmisión electrónica, dados los procesos de internet y la interoperabilidad de información dentro de las instituciones nacionales como la transnacional (p. 197).

De acuerdo con esto, Corrales-Melgarejo (2023) arguye que el derecho a la intimidad entrega al derecho a la confidencialidad y el secreto de la información personal. A pesar de que el derecho a la privacidad mantiene la autonomía en el almacenaje y la transmisión digital, los avances tecnológicos influyen en este derecho en lo que respecta al almacenamiento y transmisión electrónica (p. 269).

En ese orden de ideas, Monroy-Ramírez (2024) define la intimidad como el derecho a mantener un espacio privado inaccesible a tercero sin consentimiento. Significa la capacidad de elegir y comunicar información y protegerse de la intromisión de terceros (p. 5). En resumen, concluimos que el derecho a la intimidad está amenazado de manera radical en estos tiempos de vigilancia masiva, cuando la cantidad de información recopilada y manipulada por gobiernos multinacionales está en aumento. Por lo que, la idea de vigilancia masiva, el cual es el control o monitoreo generalmente detallado de tales individuos, comunicaciones y comportamientos, pone en peligro el derecho a la intimidad, otorga acceso a la vida privada de las personas a otros individuos sin el consentimiento adecuado.

Finalmente, en términos del segundo objetivo específico, se evalúan las medidas de autenticación de la privacidad digital y se gestiona la influencia de tales mecanismos en el derecho a la libertad de expresión en la era de la vigilancia masiva. Aunque tal tecnología mejora la privacidad y las prácticas de manufactura, se ha demostrado que las medidas de seguridad masiva pueden dañar la libertad de expresión restringiendo el acceso a Internet o debilitando el anonimato.

Por ende, los autores Marmolejo-Corona et al. (2023) comentan que la autenticación es un componente clave de la seguridad en esta modalidad de protección, el código de autentificación es esencial para proteger los datos y sistemas de los usuarios (p. 42). Asimismo, Mendoza-Arteaga et al. (2020) sostienen que la autenticación es el primer filtro en un modelo de seguridad estándar y demuestra la prohibición legal de los sistemas de datos de un individuo (p. 3).

Además, Barata-Mir (2022) menciona que la libertad de opinión se defiende y protege a nivel mundial, lo que tiene connotaciones obvias para Internet, la plataforma le proporciona a la era tecnológica y la comunicación masiva ofrece una plataforma global y accesible para expresar y recibir puntos de vista muy distintos de la televisión, la radio y los medios impresos (p. 90).

En ese contexto, Olguín-Meza (2023) describe la libertad de opinión como la facultad de expresarse libremente acerca de derecho de expresar opiniones sin discriminación sobre asuntos públicos y privados, el cual es un pilar fundamental en un mundo interconectado y diverso que faculta el ejercicio pleno de los derechos sin restricciones en la transmisión y divulgación de información (p. 39).

Según, Placín-Vergillo (2024) la libertad de expresión es considerada el acceso a internet a las personas la oportunidad de expresar y compartir sus opiniones de manera ágil. La capacidad de compartir contenido a nivel mundial abre una nueva forma de influir este derecho en donde tiene sus pros y contras (p. 90). El desafío del derecho a la libertad de expresión en una era de vigilancia masiva presenta desafíos importantes ya que una vigilancia exhaustiva puede reprimir la comunicación abierta y fluida, generar autocensura. Es fundamental encontrar un equilibrio entre la seguridad y la libertad de expresión.

CONCLUSIONES

La protección de la privacidad digital se consideró un derecho fundamental comprometido en un contexto de épocas de vigilancia masiva. La recopilación masiva y la administración del uso de los datos por parte de las entidades gubernamentales y privadas aumentaron la percepción de los ciudadanos de que su vida privada era vulnerable al acceso no autorizado. Es más, si su información personal es utilizada sin su consentimiento o expuesta sin las debidas precauciones, vulneraria derechos básicos como la libertad de expresión e incrementando la autocensura y limitándolos a utilizar la comunicación en la red.

En los últimos años el avance de la tecnología de encriptación ha sido crucial para proteger la privacidad digital y el derecho a la intimidad en una era de vigilancia masiva enfocándose en preservar la confidencialidad frente al constante monitoreo y recolección de datos personales. Sin embargo, las sofisticadas funciones de vigilancia y control presentaron retos importantes poniendo en duda la

eficiencia de estas medidas de seguridad en un contexto donde la violación de la privacidad se había vuelto cada vez más común.

En tiempos de vigilancia masiva, la eficacia de las medidas de protección de la privacidad digital en relación al derecho a la libertad de expresión se analizaba principalmente en función de su capacidad para preservar dicho derecho ante la recopilación y seguimiento detallado de datos. Estas medidas se centraban en garantizar que la información privada y las comunicaciones de los usuarios estuvieran protegidas contra accesos no autorizados para fomentar una expresión libre sin miedo a represalias o a la censura. Se evaluaba la efectividad de métodos de autenticación como la autenticación multifactor y el cifrado punto a punto para salvaguardar la confidencialidad de las comunicaciones y restringir el acceso a datos sensibles solo a los titulares legítimos.

REFERENCIAS BIBLIOGRÁFICAS

Angles-Yanqui, G. H. (2020). TikTok: La ineficacia del derecho a la intimidad en la era digital en tiempos de Covid -19 y el "famoso" derecho al olvido en Perú. REVISTA DE DERECHO, 5(1), 194-204. https://doi.org/10.47712/rd.2020.v5i1.61

Arias, J y Covinos, M. (2021). *Diseño y Metodología de la Investigación (Vol. 1).* Arequipa - Perú: Enfoques Consulting EIRL.

Arispe-Alburqueque, C. M; Yangali-Vicente, J. S; Guerrero-Bejarano, M. A; Lozada de Bonilla, O. R; Acuña-Gamboa, L. A y Arellano-Sacramento, C. (2020). *La Investigación Científica. Una aproximacion para los estudios de posgrado.* Guayaquil - Ecuador: Universidad Internacional del Ecuador .

Baena, G. (2017). *Metodología de la investigación (3a. ed).* Mexico : Grupo Editorial Patria.

Barata-Mir, J. (2022). Libertad de expresión regulacion y moderacion privada de contenidos. *Teoría & Derecho. Revista De Pensamiento jurídico*(32), 88-107 . https://doi.org/10.36151/TD.2022.039

Barreno-Salinas, M. M. (2024). El derecho a la privacidad en la era digital: Desafios y garantías frente a la vigilancia masiva desde una perspectiva de derechos humanos. *VISUAL REVIEW, 17*(1), 235 - 245.

https://doi.org/10.62161/revvisual.v17.5769

Barzola-Plúas, Y. G & Núñez-Ribadeneyra, R. A. (2025). Desafíos legales en la protección de datos personales en la era digital. *Multidisciplinary Collaborative Journal, 3*(1), 31 - 43. https://doi.org/10.70881/mcj/v3/n1/44

Bouzas-Mendes, R. E. (2023). El reto de la privacidad en la era de internet. *Revista de Derecho de la UNED (RDUNED)*(31), 113-148. https://doi.org/10.5944/rduned.31.2023.37949

Burbano-Ardila, A; Navia-Lopez, A y Diaz-Losada, S. L. (2021). Surveillance systems and their effect on the right to privacy from the security discourse. *Revista Latinoamericana de Derechos Humanos, 33*(1), 33-51. https://doi.org/10.15359/rldh.33-1.2

Calcaneo-Monts, M. A. (2021). Internet, redes sociales y libertad de expresión. *Revista Mexicana De Derecho Constitucional, 1*(44), 37-54. https://doi.org/10.22201/iij.24484881e.2021.44.16157

Carvajal-Chávez, C. A. (2019). The encryption of business data: advantages and disadvantages. *RECIMUNDO, 3*(2), 980-997. https://doi.org/10.26820/recimundo/3.(2).abril.2019.980-997

Casas, E; Requejo, J; Piñar, J; Pérez, M y García, I. (2020). *El Derecho a la Proteccion de Datos Personales en la Sociedad Digital.* Madrid - España: Editorial Centro de Estudios Ramón Areces S.A. https://www.fundacionareces.es/recursos/doc/portal/2018/03/20/el-derecho-a-la-proteccion-de-datos-personales.pdf

Castro-Gonzalez, L y Planas-Woll, E. F. (2024). Ecosistemas digitales de vigilancia e inteligencia global y su impacto en la Seguridad y Defensa Nacional. *Revista De Ciencia E Investigación En Defensa ,, 5*(2), 30-46. https://doi.org/10.58211/6q7w0g73

Castro-Jaramillo, A. M. (2016). Derecho a la intimidad en las redes sociales de internet en Colombia. *Novum Jus, 10*(1), 113-133

. https://doi.org/10.14718/NovumJus.2016.10.1.5

Corrales-Melgarejo, E. R. (2023). Entre los derechos a la intimidad y protección de los datos personales en el trabajo y el poder fiscalizador del empleador: las cámaras de videovigilancia. *Revista Oficial del Poder Judicial, 15*(19), 261-277. https://doi.org/10.35292/ropj.v15i19.739

Cuevas-Orta, V. (2022). Los derechos fundamentales en la era digital. *Derechos Fundamentales a Debate/Comisión Estatal de Derechos Humanos Jalisco*, 116-133. http://historico.cedhj.org.mx/revista%20DF%20Debate/articulos/revista_No18/ADEBATE-18-art6.pdf

Cumbreras-Amaro, M. (2020). La seguridad de los datos personales y la obligación de notificar las brechas de seguridad. *Revista de Derecho, Empresa y Sociedad (REDS)*, 151-162. https://dialnet.unirioja.es/servlet/articulo?codigo=7631166

De la Espriella, R y Gomez-Restrepo, C. (2020). Metodología de investigación y lectura crítica de estudios. Teoría fundamentada. *Revista Colombiana de Psiquiatría, 49*(2), 127-133. http://www.scielo.org.co/pdf/rcp/v49n2/0034-7450-rcp-49-02-127.pdf

Delgado-Franco, C. (2019). Ensayo ganador del X premio Enrique Ruano Casanova. Vigilancia masiva y el derecho a la protección de los datos personales. *Foro. Revista de Ciencias Juridicas y sociales, 22*(1), 17-57. https://revistas.ucm.es/index.php/FORO/article/view/66632/4564456554331

Díaz-Giunta, R. (2023). El derecho a la libertad de expresión y las redes sociales. *Athina*(015), 91-114. https://doi.org/10.26439/athina2023.n015.6487

Escudero, C. y Cortez, L. (2018). *Técnicas y métodos cualitativos para la investigación científica.* Machala - Ecuador: UTMACH. https://repositorio.utmachala.edu.ec/bitstream/48000/12501/1/Tecnicas-y-MetodoscualitativosParaInvestigacionCientifica.pdf

Espinosa, P. (2020). MASS SURVEILLANCE Conflict between national security, right to data protection and private life. *Revista Cálamo, 13*, 123–137. https://doi.org/10.61243/calamo.13.167

García, G. (2023). Investigación cualitativa desde el método de la investigación acción. *Revista de Artes y Humanidades UNICA, 24*(51), 196-210. https://doi.org/10.5281/zenodo.10048464

Giménez-Palomares, F y Monsoriu, J. A. (2023). Una propuesta de practica informatica: aritmetica modular y encriptacíon de imágenes. *Modelling in Science Education and Learning, 16*(1), 21-27. https://doi.org/10.4995/msel.2023.18520

Guevara-Alban, G. P; Verdesoto-Arguello, A. E y Castro-Molina, N. E. (2020). Metodologias de pesquisa educacional (descritiva, experimental, participativa e de ação). *Revista Científica Mundo de la Investigación y el Conocimiento Recimundo, 4*(3), 163-173. https://doi.org/10.26820/recimundo/4.(3).julio.2020.163-173

Guillermo-Jiménez, W y Meneses-Quintana, O. (2023). Libertad de expresión en internet y redes sociales vs. Derechos a la intimidad y el buen nombre. Prevalencia, colisión y ponderación en el Derecho constitucional (1992-2019). *Revista derecho del Estado*(56), 275-304. https://doi.org/10.18601/01229893.n56.10

Maqueo, M y Barzizza, A. (2020). *Democracia, privacidad y proteccion de datos personales.* México: Instituto Nacional Electoral. https://www.ine.mx/wp-content/uploads/2021/02/CDCD-41.pdf

Marmolejo-Corona, I. V; Bautista-Aguila, F. A; Santiago-González, Y. F y Serrano-Manzano, G. A. (2023). Security in Authentication Systems: Vulnerability Analysis and Mitigation Strategies. *XIKUA Boletín Científico De La Escuela Superior De Tlahuelilpan, 11*(22), 39-43. https://doi.org/10.29057/xikua.v11i22.10802

Martínez-Devia, A. (2019). La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? *Revista La Propiedad Inmaterial*, 5-23. https://doi.org/10.18601/16571959.n27.01

Martínez-Molano, V y Rincón-Cárdenas, E. (2021). Problemas y desarrollo de la identidad en el mundo digital. *Revista Chilena De Derecho Y Tecnología, 10*(2), 251-276. https://doi.org/10.5354/0719-2584.2021.59188

Mejia, A. (2020). La libertad de Expresion en Jaque el Panoptico del Siglo XXI. Big Data como amenaza para la Democracia. A propósito del caso Cambridge Analytica. *UNIVERSITAS. Revista De Filosofía, Derecho Y Política*(32), 79-105. https://doi.org/10.20318/universitas.2020.5512

Mejía-Navarret J. (2021). Libertad de expresión, redes sociales y modernidad. *Revista de la Universidad Ricardo Palma, Tradición, Segunda época*(21), 111-122 https://doi.org/10.31381/tradicion.v0i21.4485

Mendivelso-Jiménez, J. (2024). Security and privacy in digital time, the age of liquid information. *Ciencia Latina Revista Cientifica Multidisciplinar, 8*(2), 7398-7420. https://doi.org/10.37811/cl_rcm.v8i2.11136

Mendoza-Armijos, H. E. (2024). Regulación jurídica de la privacidad en el entorno digital y sus desafios actuales. *Science Journal, 2*(1), 28 - 40. https://doi.org/10.63618/omd/isj/v2/n1/31

Mendoza-Arteaga, A. G; Bolaños-Burgos, F; Cedeño-Sarmiento, C y Saltos-Rivas, W. R. (2020). La importancia de la autenticación multifactor para el usuario final en unentorno financiero. *Revista de Tecnologías de la Informática y las Comunicaciones, 4*(1), 42-51. https://doi.org/10.33936/isrtic.v4i1.2347

Mendoza-Enríquez, O. A. (2021). The personal data protection right in artificial intelligence systems. *Revista del Instituto de Ciencias Jurídicas de puebla IUS, 15*(48), 179-207. https://doi.org/10.35487/rius.v15i48.2021.743

Monroy-Ramírez, M. C. (2024). El derecho a la intimidad o privacidad como derecho humano. *Revista Académica CUNZAC, 7*(1), 1-11. https://doi.org/10.46780/cunzac.v7i1.112

Moret-MillásV y Sánchez-GilI, I. (2022). Una aproximación de Derecho Comparado a la regulación de las plataformas de redes sociales. *Revista De Las Cortes Generales*(112), 287-316. https://doi.org/10.33426/rcg/2022/112/1664

Mormontoy Pérez, J. J. (2024). Sobre la privacidad en las tecnologías de la información: ¿una ventana sin cortinas? *Chornancap Revista Jurídica, 1*(2), 53–72.

https://doi.org/10.61542/rjch.40

Murrugarra-Retamozo, B. I. (2024). Inteligencia artificial y privacidad en internet: amenazas para los datos personales de los usuarios. *Revista Científica Multidisciplinaria Ogma, 3*(2), 30-48. https://doi.org/10.69516/9dp8ap45

Ojeda-Bello, Z y Cutié-Mustelier, D. (2021). El derecho a la protección de datos perso-nales en Cuba desafíos en la era digital. *Revista del Instituto de Ciencias Jurídicas de Puebla, 15*(48), 243-257. https://doi.org/10.35487/rius.v15i48.2021.689

Ojeda-Segovia, L. (2020). Vigilancia tecnológica versus derecho a la privacidad-intimidad. El caso de la pandemia. *Textos Y Contextos, 1*(21), 123 - 134. https://doi.org/10.29166/tyc.v1i21.2513

Olguín Meza, M. de J. (2023). La Libertad de Expresión en la Sociedad del Conocimiento. *Con-Ciencia Boletín Científico De La Escuela Preparatoria, 10*(20), 39-42. https://doi.org/10.29057/prepa3.v10i20.10575

Placin-Vergillo, F. (2024). Internet en el ejercicio de la libertad de expresión del sistema europeo de derechos humanos. *IUS ET SCIENTIA, 10*(1). https://doi.org/10.12795/IESTSCIENTIA.2024.i01.04

Porcelli, A. M y Martínez, A. N. (2020). La reformulación del derecho a la privacidad y el reconocimiento de los nuevos derechos en el entorno digital en tiempos de COVID-19. *Red Sociales, Revista del Departamento de Ciencias Sociales, 7*(7), 109-125.

Porcelli, A. M. (2020). La Protección de los Datos Personales en el Entorno Digital. Los Estándares de Protección de Datos en los Países Iberoamericanos. *Revista Quaestio Iuris, 12*(2), 465-497. https://doi.org/10.12957/rqi.2019.40175

Puerto, M. I y Sferrazza-Taibi, P. (2018). La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. *Revista derecho del Estado*(40), 209–236. https://doi.org/10.18601/01229893.n40.09

Quijano, C. (2022). *Derecho a la privacidad en internet.* México: Editorial Tirant lo blanch.

Rayman-Labrín, D. (2015). Chile: Surveillance and the right to privacy on internet. *Revista Chilena de Derecho y Tecnologia, 4*(1), 187-232. https://doi.org/10.5354/0719-2584.2015.36007

Rivera-Pineda, Y. M y Maldonado-Ruiz, L. M. (2023). Vulneración del derecho a la privacidad dentro de la era digital en el Ecuador. *Polo del Conocimiento, 8*(10), 982-1009. https://doi.org/10.23857/pc.v8i10.6172

Romero-Castro, M. I; Figueroa-Morán, G. L; Vera-Navarrete, D. S; Álava-Cruzatty, J. E; Parrales-Anzúles, G. R; Álava-Mero, C. J; Murillo-Quimiz, A. L y Castillo-Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Editorial Área de Innovacion y Desarrollo S.L. https://irp.cdn-website.com/c4d16642/files/uploaded/Seguridad-inform%C3%A1tica.pdf

Rueda-Sánchez, M. P; Armas, W. J y Sigala-Paparella, S. P. (2023). Qualitative a priori category analysis: data reduction for management studies. *Ciencia y Sociedad, 48*(2), 83-96. https://doi.org/10.22206/cys.2023.v48i2.pp83-96

Sánchez-Díaz, M. F. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana De Derecho Administrativo, 10*(1), 1-21. https://doi.org/10.14409/redoeda.v10i1.12626

Sánchez-Muñiz, J. J., Delgado-Pionce, E. A., & Cobos-Villafuerte, A. M. (2023). Análisis de los algoritmos criptográficos modernos y su efectividad en la protección de datos personales. *Revista Cientifica: Journal TechInnovation, 2*(1), 57-61. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.57-61

Soler-Martínez, J. A. (2022). Protección constitucional de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías. *Revista Anuario de Derecho Canónico*, 93-126. https://dialnet.unirioja.es/servlet/articulo?codigo=8661053

Torres-Gómez, E. (2021). Mass surveillance technologies and the right to privacy: when the need for security threatens fundamental rights. *Saberes Jurídicos, 1*(2), 15-23. https://umapp002.unimagdalena.edu.co/index.php/saberesjuridicos/article/view/4436

Valiente-Martinez,F. (2022). La Libertad de Expresión y las Redes Sociales de la Doctrina de los Puertos Seguros a la Moderación de Contenidos. *DERECHOS Y LIBERTADES: Revista De Filosofía Del Derecho Y Derechos Humanos*(48), 167-198. https://doi.org/10.20318/dyl.2023.7343

Vásquez-Cerna, J. J; Solano-Quicho, L. M y Mendoza de los Santos, E. C. (2023). The Vulnerability of Biometric Technologies in Authentication. *Ingeniería Investiga, 5*, 1-14. https://doi.org/10.47796/ing.v5i0.866

Ventura, M y De Oliveira, S. C. (2023). Integridade e ética na pesquisa e na publicação científica. *Scielo*, 1-5. https://doi.org/10.1590/0102-311X00283521