



ID del documento: INRM-Vol.2.N.3.001.2024

Tipo de artículo: Investigación

Entre la seguridad y la privacidad: dilemas éticos en la recolección de datos digitales

Between security and privacy: ethical dilemmas in digital data collection

Autores:

Luis David Bastidas González

Pedro Antonio Saltos García

¹Universidad Estatal de Milagro, Ecuador, davidbastidasg1@gmail.com, <https://orcid.org/0000-0003-3060-4342>

²Universidad Estatal de Milagro, Ecuador, psaltosg@unemi.edu.ec, <https://orcid.org/0000-0002-4416-2488>

Corresponding Author: *Bastidas González Luis David*, davidbastidasg1@gmail.com

Reception date: 10-09-2024

Acceptance: 25-09-2024

Publication: 27-09-2024

How to cite this article:

Saltos García, P. A., & Bastidas González, L. D. . (2024). Entre la seguridad y la privacidad: dilemas éticos en la recolección de datos digitales. *Intellectual Network Revista Internacional*, 2(3), 1-15. https://revinde.org/index.php/intellectual_network/article/view/51



Resumen

La era digital ha transformado nuestra percepción de la privacidad y la seguridad de la información. En un entorno interconectado, los datos se han convertido en un recurso valioso, lo que genera dilemas éticos al momento de ser intercambiados y comercializados, complicando la protección de la información personal y corporativa. Cuando se aborda el tema de privacidad, se está tocando cuestiones fundamentales como la libertad, la dignidad y la autonomía personal. Estos principios deben ser protegidos y valorizados en una sociedad cambiante y cada vez más tecnológica, donde la información se presenta con mayor claridad, pero las acciones que se realizan con ella a menudo carecen de la misma transparencia. Este artículo investiga la relación existente entre la seguridad y la privacidad al momento de recopilar datos digitales, analizando las complejas interacciones entre la protección de datos y el respeto a la intimidad individual en un entorno tecnológico que se encuentra en constante evolución. Los resultados muestran que muchos de los usuarios en internet están dispuestos a sacrificar parte de su privacidad a cambio de servicios que se perciben como seguros. Así mismo, las organizaciones priorizan la seguridad por encima de la privacidad, lo que puede llevar a la explotación de datos sin el consentimiento adecuado. Finalmente, se discute la transparencia al momento de recopilar y utilizar los datos, subrayando la urgencia de establecer un enfoque ético que logre equilibrar la seguridad y la privacidad en la recolección de datos digitales.

Palabras Clave: privacidad; seguridad; recolección de datos; dilema ético.

Abstract

The digital age has transformed our perception of privacy and information security. When the issue of privacy is addressed, fundamental issues such as freedom, dignity and personal autonomy are being touched. These principles must be protected and valued in a changing and increasingly technological society, where information is presented more clearly, but the actions that are carried out with it often lack the same transparency. This article investigates the relationship between security and privacy when collecting digital data, analysing the complex interactions between data protection and respect for individual privacy in a technological environment that is constantly evolving. The results show that many Internet users are willing to sacrifice some of their privacy in exchange for services that are perceived as secure. Likewise, organizations prioritize security over privacy, which can lead to data exploitation without proper consent. Finally, transparency in the collection and use of data is discussed, underscoring the urgency of establishing an ethical approach that manages to balance security and privacy in the collection of digital data.

Keywords: privacy; safety; data collection; ethical dilemma.



1. INTRODUCCIÓN

En un mundo cada vez más interconectado y digitalizado, la velocidad del avance tecnológico plantea desafíos sin precedentes para nuestra sociedad. La capacidad de innovar y crear ha superado la velocidad de adaptación de las normativas éticas y legales que deberían regular estas transformaciones. Esta desincronización no solo afecta la manera en que interactuamos, también llega a poner en tela de juicio los valores que guían nuestras relaciones en un entorno que cada vez es más virtual. Ante esto, es importante reflexionar sobre cómo salvaguardar la integridad y la justicia en un mundo donde la tecnología cada vez avanza a pasos agigantados, dejando atrás las estructuras normativas que a lo largo de la historia han guiado nuestras conductas.

La vida contemporánea se caracteriza por una profunda transformación en la forma en cómo percibimos y practicamos la moralidad. Es así que, en un entorno cada vez más digital, el concepto de ética a menudo se minimiza, perdiendo su significado y relevancia. Sin embargo, en medio de esta confusión, la ética puede convertirse en un poderoso medio de conexión, capaz de fortalecer nuestras comunidades y fomentar la cohesión social. A pesar de su potencial y los evidentes avances en nuestros estilos de vida, la era digital también trae consigo desafíos que amenazan con erradicar estos valores fundamentales (Arriola Rosales, 2024).

La evolución tecnológica ha redefinido drásticamente nuestras formas de comunicación y acceso a la información, impactando también los valores éticos que rigen las instituciones y sus interacciones. Sin embargo, las normativas sociales y profesionales parecen no seguir el mismo ritmo, generando una desconexión entre el rápido avance de la tecnología y la capacidad de los códigos éticos para abordar los dilemas emergentes (Arriola Rosales, 2024).

Durán (2022) afirma que la ética profesional actúa como la voz de la conciencia moral, siendo fundamental para la prosperidad social y para la construcción del desarrollo individual de cada profesional. Esta ética impulsa a los individuos a ofrecer servicios a la comunidad que generen beneficios y satisfacción colectiva. Así, se espera que el profesional asuma un compromiso serio, responsable y disciplinado, orientado hacia el bien común en lugar de intereses personales. Este compromiso no solo requiere desarrollar habilidades mentales y emocionales, también se busca dar prioridad a los valores morales en su trabajo.

El derecho a la privacidad, fundamentado en la valoración del individuo, ha sido respaldado por la tradición jurídica que protege la persona y garantiza la inviolabilidad de su domicilio, así como de sus documentos y pertenencias. Esta protección asegura que ningún elemento relacionado con la vida privada de un individuo pueda ser utilizado por terceros sin su consentimiento, enfatizando en la importancia de la autonomía y el respeto hacia la intimidad personal de quienes utilizan el internet (Pfeiffer, 2008).

La digitalización y la gestión masiva de información traen consigo retos complejos en los ámbitos legales y éticos, lo que exige una reflexión sobre cómo se pueden llegar a manejar estos cambios y así proteger los principios fundamentales dentro de la era digital que atravesamos. Es por esto que se cuestiona, ¿Cómo se pueden equilibrar las necesidades de seguridad y la protección de la privacidad en la recolección de datos digitales, considerando los dilemas éticos que surgen de esta? Por lo que este artículo pretende identificar cuáles



son los desafíos éticos que surgen al momento de recopilar y utilizar los datos, así como las repercusiones que trae consigo para los usuarios.

A través de un análisis crítico, se desarrollará un marco teórico que permitirá identificar estos dilemas, al tiempo que se propondrán mejores prácticas y políticas que fomenten un equilibrio entre la seguridad y la protección de la privacidad. Además, el estudio busca aumentar la conciencia social sobre la importancia de la privacidad en la era digital, realizando un debate público informado sobre los derechos individuales. A partir de este trabajo se espera contribuir al desarrollo de prácticas más responsables y equilibradas que promuevan tanto la seguridad como la salvaguarda de los derechos de privacidad, fomentando un entorno digital más ético y transparente.

2. DESARROLLO

Antecedentes Históricos

La protección de datos dentro de la era digital tiene sus orígenes que se remontan en la década de los 60, cuando empezaron a surgir preocupaciones sobre la privacidad y el manejo adecuado de la información personal debido al crecimiento de los sistemas informáticos. En 1968, Suecia aprobó la primera ley de protección de datos, que sentó las bases para el tratamiento de la información personal. En 1970, Estados Unidos también empezó a proteger la privacidad de los datos con leyes, como la Ley de Privacidad de la Educación Familiar (FERPA) y la Ley de Informes de Crédito Justos (FCRA). Sin embargo, la tecnología siguió avanzando, y con la llegada de Internet y el auge de las redes sociales en los años 2000, se hicieron visibles las deficiencias en la protección de datos.

La introducción del Reglamento General de Protección de Datos (GDPR) en la Unión Europea en mayo de 2018 fue un hito crucial en la protección de datos a nivel mundial. Este reglamento estableció un marco regulatorio completo para salvaguardar la información personal de los ciudadanos de la UE, centrándose en el consentimiento informado, la transparencia en el manejo de datos y las obligaciones claras para las empresas que procesan información personal.

En otros países y regiones, como California con la Ley de Privacidad del Consumidor de California (CCPA), han adoptado leyes similares para abordar las preocupaciones con respecto a la privacidad de los datos. Estas regulaciones buscan garantizar que los usuarios tengan más control sobre su información personal y que las empresas sean responsables al momento de usarlas.

Investigaciones Internacionales

La investigación de Vesga (2023) titulado "Delitos informáticos y la vulneración al derecho a la intimidad personal en la Provincia de Barranca, 2023", evalúa cómo los delitos informáticos afectan el derecho a la privacidad en Barranca durante 2023. Este estudio se llevó a cabo en Huacho, Perú, y utilizó una metodología cuantitativa con un enfoque descriptivo y correlacional, además de un diseño no experimental y transversal.

Cuñas (2021) centró su investigación en "Los datos personales en las redes sociales y el derecho a la intimidad personal", analizando cómo se viola el derecho a la intimidad según



el artículo 178 del Código Orgánico Integral Penal de nuestro país en Facebook. Este estudio combinó un análisis legal y doctrinal del derecho a la intimidad con un examen de 13 casos de divulgación de datos personales. El autor utilizó una metodología cualitativa para revisar las fuentes y realizó encuestas entre abogados en Riobamba. Los resultados mostraron que la incidencia de delitos en redes sociales en Ecuador es baja y que los delitos que se sancionan suelen ser de poca gravedad, lo que llevó a la formulación de propuestas y recomendaciones.

Por otro lado, Zamora (2020) llevó a cabo una investigación titulada "Los delitos informáticos y el derecho a la intimidad en el Código Orgánico Integral Penal", con la finalidad de analizar jurídicamente los delitos informáticos, sus sanciones y su impacto en la intimidad de los usuarios de internet. El autor implementó el método científico, recopiló información bibliográfica y documental, y realizó un estudio de campo que incluyó encuestas a abogados en ejercicio. Los resultados terminaron confirmando la hipótesis de que los delitos informáticos afectan el derecho a la intimidad.

Por otro lado, Palacios (2021) realizó una investigación titulada "Los delitos informáticos contra datos y su vulneración al derecho de la intimidad personal en la ciudad de Ayacucho, 2020". El autor busca determinar cómo los delitos informáticos impactan el derecho a la intimidad en Ayacucho durante ese año. La investigación se basó en el enfoque cualitativo y descriptivo, con la participación de 6 abogados. Los resultados destacaron que los delitos informáticos contra la recopilación de datos vulneran claramente el derecho a la intimidad personal, exigiendo una mayor atención y una adecuada aplicación de la normativa.

BASES TEÓRICAS

Ética digital

Una ética digital, como ética aplicada, busca orientar el comportamiento y las relaciones de las generaciones digitales al establecer referentes éticos para su actuar, vivir y convivir (Floridi y otros, 2019). La ética digital es entendida como una ética aplicada que busca guiar el comportamiento moral dentro de los entornos virtuales, promoviendo los valores a nivel personal, social y profesional (de Broglie, 2016). Desde esta perspectiva, esta ética debe ayudar a los profesionales de internet y tecnología a manejar la información que circula en línea, evaluando su veracidad, definiendo qué se puede publicar y qué información debe ser cuestionada por ser distorsionada o falsa, legitimando así la información a través del valor de la comunicación.

Otro enfoque de la ética digital se centra en identificar los deberes y derechos que se debe tener al momento de utilizar el internet. Desde una perspectiva de responsabilidad como valor ético en el mundo digital, se proponen varios deberes: como el deber de conexión, el deber de transparencia, el deber de equidad, de participación y el de protección (UNESCO, 2019).

Datos personales

Se define como cualquier información que identifica o puede identificar a una persona natural, ya sea de forma directa o indirecta, en el presente o en el futuro. Esto incluye también datos inocuos, metadatos y fragmentos de datos que puedan identificar o hacer identificable a un individuo (Ecuador, 2019).





El reciente Reglamento General de Protección de Datos (RGPD) se basa en la Directiva Europea sobre datos personales de 1995, estableciendo seis principios fundamentales para el tratamiento de datos personales:

- Deben ser procesados de manera legal, justa y transparente.
- Su recolección debe tener fines específicos, legítimos y claramente definidos.
- Deben ser adecuados, pertinentes y limitados a lo necesario para los propósitos para los cuales se utilizan.
- Es imprescindible que sean precisos y se mantengan actualizados.
- Deben conservarse de forma que se pueda identificar a los interesados únicamente durante el tiempo necesario para cumplir con los objetivos del tratamiento.
- Su manejo debe asegurar la protección y seguridad de la información.

Privacidad

La privacidad permite al individuo decidir de forma selectiva qué información compartir o revelar. El tipo de información que una persona se siente libre de compartir varía según la naturaleza de la relación, la cual influye en el tipo y nivel de conocimiento que se considera apropiado entre las partes.

Al considerar la privacidad en Internet, es importante no confundir el término con intimidad, más bien, se refiere a una dimensión diferente de la privacidad: la autonomía individual y la capacidad de elegir y tomar decisiones informadas. En este contexto, la privacidad implica el control sobre diversos aspectos de nuestra vida. Específicamente, en el ámbito digital, esta autonomía se traduce en autodeterminación informativa. Internet maneja enormes volúmenes de datos sobre las personas, que a menudo se divulgan, comparten y utilizan de múltiples maneras. Así, la autonomía individual se encuentra estrechamente vinculada a la gestión de la información personal. (Terwangne, 2012).

Derecho a la intimidad personal

Para (Muñoz, 2018) el derecho a la intimidad personal es un concepto esencial en los derechos humanos, que asegura a las personas el control y privacidad sobre sus vidas y la información compartida. Este derecho protege a los individuos de la intromisión no autorizada en sus asuntos personales, su vida privada y su espacio personal. Está reconocido en muchas constituciones y existen tratados internacionales de derechos humanos.

Era digital

En el siglo XIX, la Revolución Industrial transformó la concepción del ser humano como entidad social y cultural. Con la llegada de la era digital y las nuevas tecnologías, hemos experimentado un crecimiento tecnológico sin precedentes, al punto que algunos consideran que estamos viviendo una Segunda Revolución Industrial. Esta era tecnológica no solo ha mejorado la calidad de los servicios, sino que también ha incrementado notablemente su diversidad.

La implementación de estas innovaciones está impactando lo que antes se conocía como sociedad industrial, dando paso a lo que hoy llamamos sociedad de la información o del conocimiento (Franco, 2005). Las técnicas introducidas en esta nueva etapa digital comprenden un conjunto de tecnologías que amplían las posibilidades de la comunicación





humana. La sinergia de estas nuevas tecnologías influirá en los procesos productivos y comunicacionales a nivel global, lo que se conoce como la Revolución Digital o Era Digital.

La Privacidad En El Entorno Digital

El entorno digital amplía considerablemente el desafío de la privacidad, llevándolo más allá del simple control de los datos personales. La creciente importancia de este concepto refleja su naturaleza dinámica y expansiva (de Pisón Cavero J. M., 2016). El alcance de la privacidad se ha ampliado, con un aumento en los aspectos de la vida que pueden ser observados o manipulados, así como en las formas de recopilación de datos y la tendencia a compartir información personal en redes públicas.

El derecho a la privacidad es más reciente que el de la intimidad y surge principalmente por la capacidad de las Tecnologías de la Información y la Comunicación (TIC) para manejar grandes cantidades de datos de una persona, relacionándolos con otras fuentes y creando perfiles muy detallados. Estos perfiles pueden revelar gustos, hábitos, aficiones e incluso ideologías o creencias religiosas. Este es el motivo por el que se ha intentado proteger el derecho a la privacidad a nivel internacional implementándose artículos y convenios, como el Convenio 108 del Consejo de Europa de 1981, pasando por la Directiva Europea 95/46/CE de 1995, hasta la Carta Europea de Derechos Fundamentales, que en su artículo 8 establece lo siguiente:

1. Toda persona tiene el derecho a la protección de sus datos personales que la conciernan.
2. Estos datos se tratarán de manera justa, con fines específicos y basados en el consentimiento de la persona afectada o en otro fundamento legítimo previsto por la ley. Además, toda persona tiene derecho a acceder a los datos que la conciernan y a solicitar su rectificación.
3. El cumplimiento de estas normas estará sujeto al control de una autoridad independiente.

Protección de datos personales

En 1980, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), en colaboración con el Consejo de Europa, publicó una serie de directrices para salvaguardar la privacidad y facilitar los flujos transfronterizos de datos personales, basándose en los siguientes principios (OECD, 2013):

1. Establecer límites claros en la recolección de datos.
2. Asegurar que los datos sean pertinentes para el propósito previsto.
3. Definir de manera explícita el uso que se dará a los datos antes de solicitarlos.
4. No utilizar los datos para fines diferentes a los inicialmente establecidos sin el consentimiento de los interesados.
5. Proteger los datos contra accesos no autorizados o actos de piratería.
6. Garantizar que las prácticas y políticas sobre el uso de datos sean transparentes y accesibles.
7. Asegurar que las personas cuyos datos han sido recolectados tengan derecho a acceder a ellos y a solicitar modificaciones o su eliminación definitiva.

Consentimiento y autonomía



El ser humano, por su naturaleza, es ontológicamente autónomo, lo que significa que su autonomía proviene de sí mismo. Cada persona es verdaderamente autónoma solo si se gobierna a sí misma de dos maneras: en primer lugar, sin coacciones que limiten su capacidad individual para seguir normas de conducta siguiendo a Emanuel Kant, y teniendo la capacidad de elegir voluntariamente un curso de acción según John Stuart Mill.

3. METODOLOGÍA

Este estudio de revisión bibliográfica empleó un enfoque sistemático basado en las siguientes etapas:

Definición del alcance del estudio:

El objetivo principal del artículo es analizar los dilemas éticos relacionados con la seguridad y la privacidad en la recolección de datos digitales. Esto incluye explorar las interacciones entre la protección de datos y el respeto a la privacidad en un entorno tecnológico dinámico.

Criterios de selección de fuentes:

Se establecieron los siguientes criterios para la selección de los documentos:

- Publicaciones científicas revisadas por pares, informes técnicos, y documentos normativos relacionados con la seguridad y privacidad en la era digital.
- Fuentes publicadas entre 2017 y 2024 para garantizar la relevancia temporal de los datos.
- Textos disponibles en inglés y español, para abarcar una perspectiva global y regional.
- Inclusión de estudios que aborden aspectos éticos, tecnológicos, legales y sociales.

Búsqueda de información:

La búsqueda de literatura se realizó en bases de datos académicas como Scopus, Web of Science, IEEE Xplore, y Google Scholar. Las palabras clave empleadas fueron:

- "Seguridad de datos digitales"
- "Privacidad en internet"
- "Dilemas éticos en la recolección de datos"
- "Protección de la información"
- "Transparencia en el manejo de datos".

Criterios de inclusión y exclusión:

Se incluyeron trabajos que:

- Discutan dilemas éticos relacionados con la privacidad y la seguridad.
 - Presenten análisis teóricos o estudios de caso relevantes.
- Se excluyeron artículos con un enfoque exclusivamente técnico sin implicaciones éticas.



Análisis y síntesis de la información:

Los documentos seleccionados se analizaron utilizando un enfoque cualitativo, categorizando los datos en temas principales:

- Dilemas éticos entre seguridad y privacidad.
- Transparencia en la recolección de datos.
- Prioridades organizacionales en la gestión de datos.

Evaluación crítica:

Se evaluaron las implicaciones éticas, legales y sociales de los hallazgos en la literatura seleccionada. Además, se identificaron áreas de consenso y discrepancia en las perspectivas sobre la privacidad y seguridad.

Limitaciones del estudio:

Este análisis está limitado a las fuentes disponibles en las bases de datos seleccionadas, lo que podría excluir literatura relevante publicada en otros idiomas o plataformas no académicas.

4. RESULTADOS

En este artículo se ha creado y estructurado una tabla que sintetiza una selección de estudios fundamentales sobre la ética en la era digital, con especial atención en la privacidad y seguridad del usuario al momento de recopilar datos digitales. Cada estudio fue seleccionado por su pertinencia y aporte a la comprensión de este tema.

Tabla 1 Matriz de Revisión Documental

#	Título	Nombre Del Autor	Año	Resumen	DOI completo
1	La ética en la era digital	Arriola, C.	2024	Es articulo analiza que, aunque la tecnología avanza rápidamente, la adaptación de las normativas éticas y legales ocurre a un ritmo mucho más lento.	10.46734/revcientifica.v7i1.81
2	¿Dónde y con quién comienza la ética digital?	Durán, J.	2019	El texto aborda la ética en la era digital, destacando la necesidad de que la inteligencia artificial complemente al ser humano, respetando principios éticos y promoviendo el bienestar colectivo.	10.29236/sistemas.n153a7



3	Internet de las cosas y la ética en la manipulación de datos.	Castillo, V. Barreto, J. Chóez, J. & Villacreces, C.	2022	Este artículo ofrece información sobre la ética informática relacionada con la manipulación de datos en diversas plataformas, conocida como "data mining".	10.47230/Journal.TechInnovation.v1.n1.2022.55-65
4	La Encrucijada Ética de la Recopilación de Datos Personales.	Tamayo, D; Tayo, M; Corrales, A & Pazmiño, A.	2023	El texto analiza la revolución tecnológica actual, destacando la convergencia de IA, TIC y datos, y su impacto en la sociedad y la ética.	10.56294/sctconf2023400
5	Los valores detrás de la privacidad	Turégano, I.	2020	El artículo busca distinguir los valores de la privacidad, argumentando que la privacidad es un bien colectivo fundamental para una sociedad democrática, por lo que su protección debe basarse en normas públicas en lugar de la autogestión individual.	10.14198/DOXA2020.43.10
6	Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales.	Enríquez, L.	2017	El foro subraya la urgencia de implementar una ley de protección de datos personales en Ecuador para regular el manejo de datos por instituciones nacionales y extranjeras. El artículo analiza las deficiencias del proyecto actual de ley y propone ajustes para crear una legislación alineada con normativas globales y con las realidades de las tecnologías de la información, asegurando la protección de los derechos de los ciudadanos.	ISSN 1390-2466
7	Protección de datos personales, privacidad y vida privada: la inquietante	Maqueo, M; Moreno, J & Recio, M.	2017	El texto analiza la necesidad de establecer estándares comunes de protección de datos personales a nivel internacional, proponiendo	10.4067/S0718-09502017000100004





búsqueda de un equilibrio global necesario			abordar las asimetrías normativas y jurisprudenciales en el derecho a la protección de datos.	
--	--	--	---	--

El análisis de los artículos seleccionados nos permite centrar en temas cruciales como la privacidad, la inteligencia artificial, la manipulación de datos y la necesidad de marcos normativos adecuados. A continuación, se presentará un análisis comparativo y descriptivo de cada artículo en el contexto del tema central.

El estudio de Arriola (2024) destaca la importancia de señalar la gran diferencia existente entre el rápido progreso de la tecnología y la lenta adaptación de las leyes y normas éticas en todo el mundo. Mientras la tecnología avanza a pasos agigantados, las regulaciones, que deberían guiar su uso y proteger a las personas, no se adaptan ni van al mismo ritmo. Mientras que la tecnología avanza rápidamente, las normativas siguen sin actualizarse, generando un vacío en donde los derechos de privacidad llegan a verse comprometidos y vulnerados.

Arriola sitúa su análisis en la era digital, un periodo caracterizado por tener avances tecnológico acelerados, incluyendo la inteligencia artificial, la recopilación masiva de datos (Big Data) y la digitalización de procesos, siendo fundamental en el estudio ya que la tecnología al día de hoy afecta en la vida cotidiana de cada uno de nosotros, afectando a los derechos y libertades del individuo. El autor destaca que las nuevas tecnologías, como la inteligencia artificial, pueden llegar a traer ventajas, pero también carecen de regulaciones que protejan los datos personales y la privacidad, lo que puede llevar a su explotación y a su vez puede ser usado sin conciencia en las consecuencias.

Arriola (2024) también enfatiza en su artículo que la privacidad se ha convertido en un bien escaso dentro de la era digital, donde la recopilación de datos, muchas veces sin el conocimiento o consentimiento del individuo, pone en riesgo la autonomía personal. Por otro lado, Durán (2019) plantea dilemas éticos sobre la vigilancia y el consentimiento, donde enfatiza la importancia de que el desarrollo de Inteligencias Artificiales y el internet en general debe ser guiado por principios éticos que tengan relación directa entre la ética, seguridad y privacidad. Durán (2019) nos plantea varios dilemas éticos en cuestión con la recolección y el uso de datos, como el consentimiento y la falta de transparencia al momento de recopilar y utilizar los datos, llevando a la violación de la privacidad.

Así mismo, propone que la ética digital debe ser integrada en todos los niveles del desarrollo tecnológico, sugiriendo que los profesionales en tecnologías que se dedican a la creación de IA y recopilación de datos reciban formación en ética para que comprendan el impacto que puede generar sus decisiones.

Este estudio es especialmente relevante en nuestro artículo, ya que proporciona un marco ético y enfatiza en la importancia de este al momento de recopilar y usar datos en un contexto digitalizado donde la privacidad puede verse amenazada. Al abogar por un enfoque centrado en el ser humano, se refuerza la idea de que la seguridad de los datos no debe comprometer la privacidad individual.



Castillo (2022) destaca cómo la recolección y análisis de datos pueden llevar al mal uso de la información personal, esto genera un conflicto entre la necesidad de seguridad al momento de utilizar los datos y el derecho a la privacidad establecido mundialmente en los derechos humanos. El autor da un punto importante dentro de nuestro estudio, argumentando que la manipulación de datos o el “data mining” a menudo se realizan sin consentimiento claro, lo que plantea preguntas sobre la autonomía del usuario dentro del internet y su derecho a la privacidad.

El artículo de Castillo (2022) y Tamayo (2023) discuten cómo a medida que se acumulan más datos, el riesgo de violentar la seguridad y privacidad del usuario también aumenta, explorando los dilemas éticos que surgen de la revolución tecnológica actual, destacando la unión de la inteligencia artificial (IA) con las tecnologías de la información y la comunicación (TIC) y la recopilación de datos. Estos dos autores subrayan la falta de claridad al momento de obtener el consentimiento y cómo llegan a comprometer la autonomía del usuario, enfatizando en cómo la recopilación de datos masivos puede llevar a la creación de perfiles detallados de los usuarios, siendo preocupante en temas sobre la vigilancia y la pérdida de privacidad.

Turégano (2020) cuestiona y afirma que la privacidad debe ser entendida no solo como un derecho individual, sino como un bien colectivo indispensable para el funcionamiento de una sociedad democrática. Esto implica que su protección debe recaer en normas públicas y no solo en la autogestión del individuo. Este enfoque refuerza la idea de que la privacidad es un componente fundamental de la democracia, donde la autonomía y el respeto a la intimidad son necesarios para el desarrollo de relaciones sociales equilibradas. La investigación enfatiza que, en un entorno digital, la privacidad individual cobra un nuevo significado, convirtiéndose en una cuestión de interés público que debe ser protegida por medio de regulaciones estatales y no dejada al arbitrio de cada usuario.

En el contexto de nuestro país, Enríquez (2017) aborda las deficiencias en la legislación de protección de datos, resaltando la necesidad urgente de una Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. La investigación identifica una brecha entre la normativa nacional y las tendencias internacionales, destacando la importancia de una legislación que se alinee con estándares globales y considere las realidades del entorno digital actual. Esto es crucial para proteger los datos personales frente al uso desmedido de la tecnología y las prácticas de recopilación de información. La propuesta de Enríquez se orienta a fortalecer las normativas ecuatorianas, haciéndolas congruentes con las necesidades de la era digital y asegurando que tanto instituciones nacionales como extranjeras se rijan bajo principios éticos y responsables.

Maqueo, Moreno & Recio (2017) abordan el desafío de establecer estándares globales para la protección de datos personales, destacando la falta de coherencia normativa y jurídica en distintos países. La investigación argumenta que estas asimetrías dificultan la creación de un equilibrio entre la privacidad y la seguridad a nivel internacional, generando vulnerabilidades para los usuarios de plataformas digitales. Esta falta de armonización legislativa permite que los datos personales puedan ser utilizados de forma indebida, dependiendo de la jurisdicción en la que se encuentren. El estudio concluye que un marco regulador global, que considere las disparidades normativas y responda a los desafíos de la era digital, es esencial para garantizar una protección adecuada de los datos en todas las regiones.





5. DISCUSIÓN

El análisis presentado en el artículo destaca la creciente tensión entre la seguridad y la privacidad en la recolección de datos digitales, un dilema ético central en la era digital. Con el avance de la tecnología, la recopilación masiva de datos se ha convertido en una práctica común que desafía las normas tradicionales de privacidad, un derecho fundamental que permite a las personas mantener el control sobre su información personal. Sin embargo, en el afán de garantizar la seguridad, muchas organizaciones priorizan la protección de sus sistemas, a menudo sacrificando la privacidad del usuario.

Los estudios revisados muestran una tendencia preocupante: la recolección de datos se realiza frecuentemente sin el consentimiento explícito o el pleno conocimiento del usuario, lo que puede ser interpretado como una falta de transparencia y responsabilidad ética. Por ejemplo, la recopilación y el uso de datos personales en plataformas digitales a través de técnicas como el “data mining” plantean un desafío para la autonomía del usuario, quien puede llegar a verse expuesto a una vigilancia constante sin un claro consentimiento. Estos problemas resaltan la necesidad de una ética digital robusta que promueva principios como el consentimiento informado y la equidad en el manejo de la información.

La normativa ética y legal avanza a un ritmo más lento que la tecnología, lo que crea vacíos regulatorios que pueden ser explotados por entidades con acceso a grandes volúmenes de datos. Esto señala la urgencia de desarrollar políticas públicas y marcos éticos sólidos que equilibren la seguridad y la privacidad en la era digital, protegiendo los derechos de los usuarios mientras se aprovechan los beneficios de la tecnología.

6. CONCLUSIÓN

La era digital ha transformado radicalmente la percepción de la privacidad, enfrentándonos al desafío de equilibrar la protección de esta con la seguridad en la recolección de datos. A medida que el entorno tecnológico evoluciona, las prácticas de recopilación de datos masivos y el uso de la inteligencia artificial plantean riesgos cada vez mayores para la autonomía y la privacidad individual. La revisión de literatura evidencia que, aunque existen regulaciones avanzadas como el GDPR en Europa, aún se necesita un esfuerzo global para desarrollar marcos normativos que protejan de manera efectiva la privacidad y respeten el derecho a la intimidad personal.

Es imperativo que los gobiernos y las organizaciones prioricen la creación de políticas que garanticen tanto la seguridad como el respeto por los derechos de los usuarios. Esto implica un enfoque ético y legal que permita a los individuos ejercer su autonomía sobre sus datos, exigiendo transparencia en los procesos de recolección y uso de información personal. La educación y formación de profesionales en tecnología sobre ética digital y privacidad también resultan esenciales para promover prácticas responsables y evitar la explotación indebida de datos.

Además, la privacidad debe ser vista como un bien colectivo indispensable para el fortalecimiento de una sociedad democrática, lo que refuerza la necesidad de regulaciones



públicas que protejan este derecho sin depender exclusivamente de la autogestión individual. La implementación de estándares internacionales también se hace necesaria para evitar las disparidades normativas entre países y garantizar una protección consistente de los datos a nivel global.

REFERENCIAS BIBLIOGRÁFICAS

- Durán Chinchilla, C. M. (2022). ÉTICA PROFESIONAL, UNA RESPONSABILIDAD HUMANÍSTICA. *Revista Boletín Redipe*, 11(6), 188-195. <https://doi.org/https://orcid.org/0000-0001-9291-7841>
- Tamayo Salazar, D., Tayo Ugsha, M. G., Corrales Freire, A. S., & Pazmiño Herrera, A. (2023). La Encrucijada Ética de la Recopilación de Datos Personales. *Serie de Conferencias*. <https://doi.org/https://doi.org/10.56294/sctconf2023400>
- Arriola Rosales, C. R. (2024). La ética en la era digital. *Revista Científica Internacional*, 7(1), 135-153. <https://doi.org/https://doi.org/10.46734/revcientifica.v7i1.81>
- Cuñas, E. (2021). Los datos personales en las redes sociales y el derecho a la intimidad personal. *Universidad Regional Autónoma de los Andes: Repositorio institucional UNIANDES*.
- de Broglie, C. (2016). We need to talk about digital ethics. *OCDE*.
- de Pisón Cavero, J. (2016). El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional. *Anuario de filosofía del derecho*, 409-430.
- Ecuador. (2019). POLÍTICA PARA TRATAMIENTO DE DATOS PERSONALES.
- Enríquez Álvarez, L. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Revista de Derecho*(27), 43-61.
- Figueroa Castillo, V. A., Barreto Pin, J. X., Chóez Calle, J. E., & Villacreses Parrales, C. A. (2022). Internet de las cosas y la ética en la manipulación. *Journal TechInnovation*, 1(1), 55-65. <https://doi.org/https://doi.org/10.47230/Journal.TechInnovation.v1.n1.2022.55-65>
- Floridi, L., Cath, C., & Tañadir, M. (2019). La ética digital: su naturaleza y alcance. En *Anuario 2018 del Laboratorio de Ética Digital* (págs. 9-17).
- Maqueo Ramírez, M., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de derecho (Valdivia)*, 30(1), 77-96. <https://doi.org/http://dx.doi.org/10.4067/S0718-09502017000100004>
- Muñoz, L. (2018). Protección penal de la intimidad personal en las redes sociales. *Universidad Nacional del Altiplano, Puno, Perú: Repositorio institucional UNAP*.
- Pfeiffer, M. L. (2008). Derecho a la privacidad. Protección de los datos sensibles. *Revista Colombiana de Bioética*, 3(1), 11-36.



Salgado Seguin, V. (2010). Intimidad, privacidad y honor en Internet. *TELOS: Fundación Telefónica*.

Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *Revista de Internet, derecho y política*, 53-66.

Turégano Mansilla, I. (2020). Los valores detrás de la privacidad. *Cuadernos de Filosofía del derecho*, 43, 255-283. <https://doi.org/https://doi.org/10.14198/DOXA2020.43.10>

UNESCO. (2019). Indicadores de la Unesco sobre la universalidad del Internet.

Vesga Guedes, P. E. (2023). Delitos informáticos y la vulneración al derecho a la intimidad personal en la Provincia de Barranca, 2023. *Repositorio UNJFSC*.

Zamora, J. (2020). Los delitos informáticos y el derecho a la intimidad en el Código Orgánico Integral Penal. *Universidad Técnica de Ambato, Ambato, Ecuador: Repositorio institucional UTA*.

Declaración de Conflicto de Intereses: Los autores declaran que no presentan conflictos de intereses relacionados con este estudio y confirman que todos los procedimientos éticos establecidos por esta revista han sido rigurosamente respetados. Asimismo, garantizan que este trabajo es inédito y no ha sido publicado, ni parcial ni totalmente, en ninguna otra revista académica.