Facebook y la privacidad: Un oxímoron

Facebook and privacy: An oxymoron

Recibido: Julio 19 de 2024 - Evaluado: Agosto 27 de 2024 - Aceptado: Septiembre 30 de 2024

Vanessa Antonio Ortega[1]
Sergio Mauricio Taborda Serna[2]
Jesús David Parra Bermeo[3]

Para citar este artículo
Antonio Ortega, V., Taborda Serna, S. M., & Parra Bermeo, J. D. (2024). Facebook y la privacidad: Un oxímoron. *Revista Crecer Empresarial, 6*(2), 2-23.

Resumen
En la actualidad, la privacidad en el entorno digital suscita intensos debates y preocupaciones entre los usuarios. Facebook, como una de las plataformas más populares y controversiales, enfrenta críticas en torno a su capacidad para proteger la privacidad de sus usuarios, mientras continúa recopilando y utilizando información personal para fines publicitarios y mejoras de su servicio. Esto genera dudas legítimas sobre las intenciones subyacentes de la plataforma. Siguiendo la perspectiva de Alfredo Vela, quien enfatiza la vulnerabilidad de la privacidad en la era digital, es pertinente considerar su afirmación: "En el momento en que algo sale de tu ordenador, deja de ser privado, a veces incluso antes de salir". Históricamente, el concepto de privacidad ha evolucionado de manera significativa, desde sus raíces en la filosofía clásica hasta su aplicación en el contexto digital contemporáneo. Este artículo explora la interrelación entre Facebook y la privacidad, analizando la evolución del concepto, la creación de las redes sociales, casos de vulneración de privacidad en la plataforma, perspectivas de autores relevantes, y la percepción que tienen los usuarios sobre su privacidad en este entorno. El análisis se centra en la contradicción inherente entre la privacidad y el funcionamiento de Facebook, evaluando las medidas implementadas para proteger los datos personales de los usuarios. Los hallazgos indican que Facebook recopila una amplia gama de datos personales, incluyendo información del perfil, historial de navegación y datos de ubicación. Estas vulneraciones a la privacidad plantean riesgos significativos, como el robo de identidad y el ciberacoso, lo que resulta en una creciente desconfianza hacia la plataforma. En conclusión, la protección de la privacidad en plataformas como Facebook es una responsabilidad compartida. Los usuarios deben ser conscientes de las implicaciones y consecuencias de sus publicaciones, reconociendo que cada mensaje, foto o comentario puede

[1] Administradora de Empresas de la Escuela de Administración de Negocios EAN, Posgrado en Responsabilidad Social Corporativa Escuela de Negocios Europea de Barcelona ENEB Universidad Internacional Isabel I de Castilla, Estudiante de Décimo Cuatrimestre de Derecho, Fundación Universitaria Unicervantes. Email: vanessa.antonio@unicervantes.edu.co ORCID: 0009-0002-6679-4272
[2] Administrador Policial de la Policía Nacional de Colombia, Estudiante de Décimo Cuatrimestre de Derecho, Fundación Universitaria Unicervantes. Email: sergio.mauricio@unicervantes.edu.co ORCID: 0009-0008-7896-0462
[3] Contador de la Universidad Surcolombiana, Especialista en Finanzas de la Universidad Libre de Colombia. Estudiante de Décimo Cuatrimestre de Derecho, Fundación Universitaria Unicervantes. Email: jesus.parra@unicervantes.edu.co ORCID: 0009-0002-0043-8742

tener un alcance mucho mayor del que imaginan. A su vez, las empresas deben proporcionar herramientas claras y accesibles para la gestión de la privacidad, y asegurar un uso ético de la información. Solo mediante una colaboración activa entre usuarios y plataformas se podrá crear un entorno digital más seguro y respetuoso, donde todas las partes se sientan valoradas y protegidas.

Palabras clave: Privacidad, redes sociales, protección de datos, vulneraciones de privacidad, ciberseguridad.

Abstract
Privacy in the digital environment is currently the subject of intense debate and concern among users. Facebook, as one of the most popular and controversial platforms, faces criticism about its ability to protect the privacy of its users while continuing to collect and use personal information for advertising and service improvement purposes. This raises legitimate questions about the underlying intentions of the platform. Following the perspective of Alfredo Vela, who highlights the vulnerability of privacy in the digital age, it is pertinent to consider his statement: "The moment something leaves your computer, it is no longer private, sometimes even before it leaves". Historically, the concept of privacy has evolved significantly, from its roots in classical philosophy to its application in the contemporary digital context. This article explores the relationship between Facebook and privacy, analysing the evolution of the concept, the creation of social networks, cases of privacy violations on the platform, the perspectives of relevant authors, and users' perceptions of their privacy in this environment. The analysis focuses on the inherent contradiction between privacy and the functioning of Facebook, and evaluates the measures taken to protect users' personal data. The findings show that Facebook collects a wide range of personal data, including profile information, browsing history and location data. These privacy breaches pose significant risks, such as identity theft and cyberbullying, leading to a growing distrust of the platform. In conclusion, protecting privacy on platforms like Facebook is a shared responsibility. Users need to be aware of the implications and consequences of what they post, recognising that every post, photo or comment can have a far wider reach than they realise. In turn, companies must provide clear and accessible privacy management tools and ensure ethical use of information. Only through active collaboration between users and platforms can a safer and more respectful digital environment be created, where all parties feel valued and protected.

Keywords: Privacy, social networking, data protection, data breaches, cybersecurity.

1. Introducción

En el siglo XXI, la revolución digital ha transformado por completo la forma de nuestra interacción social, permitiendo que plataformas como Facebook conecten a más de 2.96 mil millones de personas en todo el mundo. Este universo digital, donde ideas, imágenes y emociones se intercambian en un instante, nos ofrece la oportunidad de compartir fragmentos de nuestras vidas de maneras nunca imaginadas. Sin embargo, esta conectividad trae consigo una inquietante preocupación: ¿cómo protegemos nuestra privacidad mientras navegamos por este mar de información? A medida que revelamos detalles personales en línea, surge la pregunta fundamental sobre el trato ético y seguro de nuestros datos, tanto por parte de los usuarios como de las corporaciones que prometen su salvaguarda.

Facebook, reconocida como una de las redes sociales más influyentes en el ámbito de la comunicación, ha sido el epicentro de múltiples escándalos de violaciones de datos y el uso indebido de información personal. Esta realidad ha hecho que muchos se cuestionen respecto a la seguridad de sus datos y, por ende, su confianza en esta red social. La noción de privacidad ha experimentado una notable evolución, desde sus raíces filosóficas hasta sus complejas implicaciones en el entorno digital actual. En este contexto, la recopilación masiva de datos y los alarmantes incidentes de ciberacoso, robos de identidad revelan la vulnerabilidad a la que están expuestos los usuarios, riesgos que pueden afectar su bienestar emocional y su confianza en el uso de redes sociales.

Este artículo tiene como propósito analizar la relación entre el uso de Facebook y la percepción de privacidad de sus usuarios, explorando cómo estas dinámicas impactan en la confianza hacia la plataforma y en el comportamiento en línea. A través de este estudio, exploraremos las paradojas de la protección de la privacidad en el ámbito digital y se evaluarán las políticas implementadas para asegurar la información personal en un contexto de creciente interconexión.

2. Perspectiva teórica

2.1 Evolución del concepto de Privacidad

Hoy en día, cada clic y cada publicación que hacemos generan un sinfín de datos que pueden ser analizados y compartidos al instante. En este vertiginoso y conectado entorno, la privacidad se convirtió en un tema crucial en nuestras vidas. Pero ¿cómo llegamos a sentirnos constantemente observados?

A lo largo de la historia, el concepto de privacidad ha experimentado una notable evolución. Desde la filosofía clásica de Aristóteles y Platón, quienes la consideraban un derecho natural, hasta la era moderna, donde se reconoce como un derecho fundamental. La privacidad es y seguirá siendo un refugio vital que protege nuestra intimidad. Un momento decisivo en esta evolución se presenta con el artículo “The Right to Privacy”, publicado en 1890 por Samuel D. Warren y Louis D. Brandeis. Este ensayo no solo estableció las bases del concepto contemporáneo de privacidad en el contexto del derecho estadounidense, a través de la noción de “The Right to be Let Alone” (el derecho a ser dejado solo), sino que también abordó las leyes de la calumnia y difamación, para determinar si realmente se salvaguardaba la privacidad individual. En una época en que tecnologías emergentes como la fotografía y la prensa comenzaban a suscitar preocupaciones sobre posibles invasiones a la vida privada, Warren y Brandeis advirtieron sobre el peligro de que estos avances facilitaran la divulgación pública de aspectos íntimos de la vida personal, amenazando lo que consideraban los “recintos sagrados de la vida privada y doméstica”. En la actualidad, este contexto caracterizado por una interconexión global sin precedentes, la relevancia de este mensaje resuena con fuerza, a medida que surgen inquietudes sobre las violaciones a nuestra vida personal. Para autores como como Westin en su obra Privacy and freedom (1967) establecía que la privacidad se podía definir como “la reivindicación de los individuos... para determinar por sí mismos cuándo, cómo y en qué medida se comunica la información sobre ellos”. Al argumentar que los ciudadanos conservaban el control sobre cómo se utilizaban sus datos personales, redefiniendo la privacidad como ese componente esencial de la libertad individual, el cual fue

objeto de diversos debates sobre la tecnología y la libertad personal. Una notable consecuencia de esta evolución fue la formulación de legislaciones enfocadas en el derecho a la privacidad. La década de 1970 fue testigo de un giro crucial en la percepción pública y legal de la privacidad, trayendo consigo leyes que no solo protegían la información personal, sino que también garantizaban a los ciudadanos el derecho a decidir sobre su propio patrimonio informático. Esta tendencia marcó el inicio de un proceso que buscaba establecer límites claros sobre la recopilación y el uso de los datos, sentando precedentes que aún son discutidos en la actualidad.

A continuación, se presenta una tabla que recopila las contribuciones de varios autores a la noción de privacidad, destacando sus obras y el impacto que han tenido en el desarrollo del pensamiento sobre este derecho fundamental. Esta recopilación no solo ilustra la evolución del concepto de privacidad, sino que también resalta la importancia de estas ideas en el contexto contemporáneo, donde las preocupaciones sobre la protección de la información personal son más relevantes que nunca y dónde se refleja la continua búsqueda de un equilibrio entre las innovaciones tecnológicas y los derechos fundamentales de los individuos.

Tabla 1. ***Evolución del concepto de privacidad***

Autor	Obra	Año	Significado de privacidad
Platón	La República	*380 a.C.*	Propone la eliminación de la propiedad privada y la vida familiar entre los guardianes para evitar conflictos de intereses y promover el bien común.
Aristóteles	Política	350 a.C.	Defiende la propiedad y la vida privada como esenciales para la felicidad y el bienestar individual.
Samuel Warren y Louis Brandeis	The Right to Privacy	1890	Artículo que sentó las bases para el concepto moderno de privacidad. Derecho a ser dejado en paz, protección contra la intrusión en la vida personal.
Alan Westin	Privacy and Freedom	1967	Relación entre privacidad y libertad. Privacidad como control sobre la información personal y esencial para la libertad.
John Locke	Dos tratados sobre el gobierno civil	1689	Derecho a la privacidad y no interferencia del Estado. Derecho natural del individuo que el Estado debe respetar.
Jean-Jacques Rousseau	El contrato social	1762	Privacidad como esencial para la libertad individual. Elemento esencial para la libertad y autonomía del individuo.
Immanuel Kant	Fundamentación de la metafísica de las costumbres	1785	Privacidad como derecho fundamental en ética y moralidad. Derecho moral fundamental que debe ser respetado por todos.
Michel Foucault	Vigilar y castigar	1975	Análisis del poder y la violación de la privacidad por el Estado e instituciones. Construcción social que puede ser violada por el poder y las instituciones.
Jurgen Habermas	La esfera pública	1962	Importancia de la privacidad para la libertad individual y la democracia. Esfera esencial para la libertad individual y el funcionamiento de la democracia.
Hannah Arendt	La condición humana	1958	Relación entre privacidad y espacio público, importancia para la creatividad. Espacio necesario para la libertad individual y la creatividad.

Isaiah Berlin	Cuatro ensayos sobre la libertad	1969	Privacidad como esencial para la libertad individual y la autonomía. Condición necesaria para la libertad y la autonomía personal.
Charles Fried	Análisis de la privacidad	1968	Privacidad como esencial para la confianza y la intimidad. Base para la confianza y la intimidad en las relaciones humanas.
Bruce Schneier	Secrets and Lies	2000	Privacidad en la era digital y su importancia para la seguridad. Elemento crucial para la seguridad personal y nacional en la era digital.
Eduardo Bertoni	Privacidad y protección de datos personales	2013	Importancia de la privacidad en América Latina. Derecho fundamental para la libertad y autonomía en el contexto latinoamericano.
Marcelo Thompson	La privacidad en la era digital	2017	Importancia de la privacidad en la era digital en América Latina. Derecho crucial para la libertad y autonomía en la era digital.

Fuente: Elaboración propia.

2.2 Del primer clic a la conexión global: la evolución de las redes sociales

El primer antecedente de las redes sociales modernas se desarrolla en la década de 1970 con la creación de ARPANET, una red de comunicación innovadora utilizada por el Departamento de Defensa de Estados Unidos. Aunque su propósito original era facilitar el intercambio de información en contextos militares, el verdadero potencial de la comunicación en línea comenzó a materializarse en la década de 1990. En esta época, empezaron a surgir plataformas que nos permiten vislumbrar lo que hoy entendemos como redes sociales. Sitios como Classmates.com, lanzado en 1995, e SixDegrees.com en 1997, marcaron el inicio de una nueva era en la que los individuos podían crear perfiles y conectarse entre sí, sentando las bases para la transformación social y su interacción.

A inicios del año 2000, surgen otras plataformas como Friendster (2002), MySpace (2003) y LinkedIn (2002) que revolucionaron radicalmente nuestra manera de relacionarnos. Estas redes no solo ofrecían espacio para conectar amigos y familiares, sino que también permitieron a los usuarios compartir intereses, hobbies y experiencias, creando una comunidad global en la que cada persona podía tener voz.

Sin embargo, este desarrollo tecnológico también trajo consigo nuevos desafíos en torno a la privacidad y la gestión de la información personal. En este contexto, el autor y académico David Rosen, en su obra The Unwanted Gaze (2000), define la privacidad como la capacidad de los individuos para manejar su información personal, protegiéndose de juicios inapropiados que no tienen en cuenta el contexto en el que esa información se presenta. Estas palabras hacen eco, en esta era de redes sociales, donde las interacciones incesantes y la continua exposición a las miradas ajenas es inevitable.

Rosen argumenta que “la privacidad es indispensable para el bienestar humano porque nos permite mantener una esfera personal libre de la mirada intrusiva de otros” (n.p.). Este concepto subraya cómo la violación de la privacidad no solo afecta nuestra dignidad personal, sino que también puede perturbar el tejido esencial de la sociedad, donde cada individuo merece la libertad de ser auténtico, sin prejuicios, sin el peso de la vigilancia constante. Así, la llegada de las redes sociales,

aunque revolucionaría en términos de conexión, nos hace reflexionar: ¿hasta qué punto estamos dispuestos a sacrificar nuestra privacidad en aras de estar conectados?

2.3. Facebook: la revolución social que transformó la conexión humana

En febrero de 2004, nace Facebook, marcando un hito en nuestra forma de conectarnos. Creada por Mark Zuckerberg y un grupo de compañeros de Harvard, la plataforma comenzó como un sitio exclusivo para estudiantes universitarios, ofreciendo un espacio donde podían interactuar, compartir fotos y mantener contacto. Su gran popularidad permitió que rápidamente se expandiera a otras universidades y, en 2006, se abriera al público en general. Este giro transformó a Facebook en una de las plataformas más utilizadas a nivel mundial y un referente en la historia de las redes sociales.

Según estadísticas de Statista (2023), Facebook se consolidó como la red social más grande del mundo, con más de 2.96 mil millones de usuarios activos. Para junio del 2024, esta cifra se incrementó en un 1.3% respecto al año anterior, alcanzando los 3.065 millones de usuarios, lo que le permite mantenerse entre las 15 marcas más valiosas del mundo. Este éxito es innegable y ha dado forma a la manera en que nos comunicamos y compartimos nuestra vida cotidiana. Desde momentos importantes hasta detalles triviales, Facebook se ha convertido en un espacio donde las personas comparten fragmentos íntimos de sus vidas, lo que genera preocupaciones significativas sobre la seguridad de la información personal y la privacidad (ver Figura 1).

Figura 1. Facebook en cifras: Análisis del Gigante de las Redes Sociales a Principios de 2024

Con 3.065 millones de usuarios activos mensuales, Facebook continúa su constante evolución y adaptación a los avances tecnológicos y las transformaciones en los hábitos de los usuarios. La plataforma se mantiene como un gigante a nivel global, marcando su huella en la vida digital de millones de personas. Para 2024, se prevé que la incorporación de inteligencia artificial y aprendizaje automático desarrolle la personalización del contenido a nuevos niveles, explorando nuevas fronteras como la realidad aumentada (AR) y la realidad virtual (VR). Estos usuarios, que en promedio dedican cerca de 19 horas y 47 minutos al mes en la plataforma, posicionan a Facebook como la segunda plataforma más utilizada para la búsqueda de información y marcas,

superada solo por YouTube entre los mayores de 24 años. En este escenario, Facebook se enfocará en 2024 en mejorar la privacidad y la seguridad de sus usuarios, implementando mejoras en sus configuraciones que permitirán un mayor control sobre sus datos. De esta forma, la plataforma se adaptará a las nuevas regulaciones internacionales y abordará las preocupaciones de los usuarios en relación con su privacidad.

Desde su lanzamiento, Facebook ha pasado por numerosos cambios, inicialmente restringido a estudiantes de Harvard, se expandió rápidamente a otras universidades, luego a escuelas secundarias y finalmente a cualquier persona mayor de 13 años. En 2006, la introducción del News Feed compiló actualizaciones de amigos en un solo flujo, transformando la interacción en la plataforma. Un año después, Facebook se abrió a los desarrolladores, lo que permitió el crecimiento de juegos en la plataforma, como el famoso Farm Ville.

En 2008, Facebook Chat se lanzó y, en 2009, se introdujo el botón "Me gusta", que se convirtió en la insignia característica de la plataforma. En 2012, Facebook se lanzó en dispositivos móviles y comenzó a enfocarse en la publicidad, ya que más de mil millones de usuarios hacían uso de la plataforma, convirtiéndola en líder de la publicidad en línea. Facebook continúo su expansión al adquirir otras empresas, incluyendo Instagram en 2012, WhatsApp en 2014 y Oculus VR en 2014, ampliando así su alcance y funcionalidad en este universo digital.

2.4 Análisis de la privacidad en Facebook

A medida que los usuarios se sumergen en esta experiencia de hiperconexión, muchos tienen la ilusión de que sus datos están debidamente resguardados. Sin embargo, la realidad desmiente esta creencia, que resulta ser, en gran medida, una ilusión. A través del tiempo, Facebook ha sido escenario de numerosos incidentes que han comprometido gravemente la privacidad de sus usuarios. Desde filtraciones de datos hasta controversias sobre el uso indebido de la información, cada nuevo escándalo resalta lo frágil que puede ser la frontera entre la conexión social y la vulnerabilidad personal.

Facebook ha logrado reunir a miles de millones de personas, fomentando un sentido de comunidad y pertenencia casi inigualable. Pero que sucede con esta promesa de conexión, que tiene un alto precio: el sacrificio de la privacidad. La plataforma ha evolucionado hasta convertirse en un espejo de nuestras vidas, donde compartimos experiencias, pensamientos y sentimientos, lo que plantea preguntas sobre la autonomía y el derecho a gestionar nuestras propias comunicaciones.

La incesante búsqueda de interacción y validación social pueden entrar en conflicto con nuestra necesidad de preservar aspectos íntimos de nuestras vidas. Por ejemplo, la transacción social que se produce al compartir información personal en la plataforma puede no ser tan inocente como parece. Cada "me gusta", cada comentario y cada publicación agregan capas de datos, invisibles para los usuarios, que a menudo subestiman su valor y vulnerabilidad. La cuestión se torna aún más pertinente cuando consideramos que muchos usuarios creen erróneamente que sus datos están completamente protegidos. Cabe resaltar, que la realidad demuestra que, a menudo, la información personal se encuentra en manos de terceros, muchas veces sin el conocimiento o consentimiento explícito del usuario.

Para contextualizar mejor el impacto de estas preocupaciones, a continuación, se ha recopilado información que incluye varios autores relevantes que han analizado las implicaciones de la privacidad en Facebook (ver Tabla 2).

Tabla 2. ***Evolución del concepto de privacidad en redes sociales***

Autor	Obra	Año	Privacidad en redes sociales
Daniel Solove	Understanding Privacy	2008	Privacidad en la era digital, crucial para la libertad individual. Derecho esencial para la libertad y autonomía en la era digital. Analiza cómo las redes sociales afectan la privacidad y la necesidad de regulaciones adecuadas.
Helen Nissenbaum	Privacy in Context	2010	Análisis de la privacidad en contextos sociales. Necesidad de contextualizar la privacidad según el entorno social. Examina la privacidad en redes sociales y propone el concepto de "integridad contextual".
Jeffrey Rosen	The Unwanted Gaze	2000	Importancia de la privacidad en la era digital. Protección contra la vigilancia y la intrusión en la vida personal. Discute cómo plataformas como Facebook pueden invadir la privacidad personal.
Latanya Sweeney	Discrimination in Online Ad Delivery	2013	Privacidad para evitar la discriminación en la publicidad en línea. Herramienta para prevenir la discriminación y proteger la equidad en la era digital. Analiza cómo la publicidad en redes sociales puede violar la privacidad y llevar a la discriminación.
Carlos Affonso Pereira	Privacidad y derechos digitales	2015	Relación entre privacidad y derechos digitales en América Latina. Derecho esencial para la libertad y creatividad en el entorno digital. Explora la privacidad en redes sociales y la protección de datos personales en plataformas como Facebook.

Fuente: Elaboración propia.

Esta tabla es solo una representación de la amplia perspectiva desde varios autores que han contribuido al debate sobre la privacidad en Facebook. En conjunto, estos puntos de vista nos invitan a reflexionar en la importancia de reconsiderar cómo usamos la plataforma y cómo percibimos los riesgos asociados. Las preguntas e interrogantes se amplían: ¿cómo equilibramos la necesidad de conexión con el derecho a la privacidad? ¿Estamos dispuestos a continuar compartiendo en un espacio donde la confianza se ha visto comprometida? ¿Seguiremos brindando segundas oportunidades a la protección de nuestros datos y con ello a la vulneración de nuestra privacidad?

2.5 Casos de vulneración de privacidad en Facebook

Para comprender la magnitud de las vulneraciones a la privacidad que ha enfrentado Facebook, es crucial retroceder en el tiempo y examinar momentos clave que han marcado su trayectoria. La historia de esta plataforma está controversialmente expuesta a varios escándalos y controversias que no solo impactaron a los usuarios, sino que también plantearon profundas preguntas sobre la ética y la responsabilidad en el manejo de datos personales.

Uno de los cambios más polémicos ocurrió en 2006 con la introducción de la función "News Feed". Muchos usuarios se sorprendieron al descubrir que sus actividades estaban siendo expuestas

sin su consentimiento explícito, lo que desató una ola de críticas que cuestionaba la protección de la información personal en la plataforma. Este episodio no fue un caso aislado, sino una señal de la cultura empresarial que a menudo, por no decir que la mayoría de las veces prioriza la interacción por encima de la privacidad.

En 2007, Facebook lanzó "Beacon", un servicio diseñado para compartir automáticamente las acciones de los usuarios en otros sitios web. La mayoría de los usuarios desconocía por completo que sus acciones estaban siendo monitoreadas y divulgadas, lo que fue considerado una clara violación de su privacidad. Esta falta de información y consentimiento llevó al creciente descontento entre los usuarios.

A medida que pasaba el tiempo, las preocupaciones por la privacidad solo crecían. En 2010, Facebook modificó su configuración de privacidad, haciéndola más compleja y confusa. Esto resultó en que muchos compartieran más información de la que realmente pretendían, lo que avivó las críticas sobre la falta de claridad en las políticas de la empresa. Tal confusión no solo generó frustración, sino que también puso de manifiesto la responsabilidad de Facebook en guiar a sus usuarios de una manera clara y sencilla en la gestión de su información.

Un año después, en 2011, Facebook se vio obligado a revisar sus políticas de privacidad y aceptó someterse a auditorías tras múltiples denuncias. Estas acciones fueron el resultado de una queja presentada en 2009 por varias organizaciones ante la Comisión Federal de Comercio (FTC), que acusaron a la red social de infringir leyes de protección al consumidor, resaltando la necesidad de un marco regulatorio que salvaguarde los derechos de los usuarios.

En el año 2013 fue un año crítico. Revelaciones indicaron que aplicaciones de terceros podían acceder a datos personales incluso sin el consentimiento de los usuarios. Además, el excontratista de la NSA, Edward Snowden, hizo públicas varias filtraciones sobre el programa de vigilancia PRISM, que implicaba la recolección masiva de datos de usuarios, incluyendo a Facebook. Aunque Zuckerberg negó la colaboración con dicho programa, la confianza del usuario ya estaba quebrantada.

En el año 2014, el profesor George E. Panichas en su artículo "An Intrusion Theory of Privacy" sostuvo que la privacidad implica estar libre de diversas formas de intrusión, que abarcan aspectos tanto epistemológicos como psicológicos. Su principal preocupación giraba en torno al uso no autorizado de imágenes y datos personales, resaltando la imperiosa necesidad de salvaguardar la dignidad y la autonomía de las personas ante tales violaciones.

En el mismo año, un estudio titulado "Experimental Evidence of Massive_Scale Emotional Contagion Through Social Networks", publicado en la revista Proceedings of the National Academy of Sciences, investigó el fenómeno del "contagio emocional masivo virtual" en Facebook. Realizado por investigadores de la Universidad de Cornell, la Universidad de California y Facebook, el experimento manipuló el contenido de noticias presentando a aproximadamente 690.000 usuarios. Los resultados mostraron que los usuarios expuestos a contenido positivo tendían a compartir mensajes optimistas, mientras que aquellos que veían contenido negativo replicaban esa negatividad en sus publicaciones.

El caso de Cambridge Analytica en 2016 supuso un golpe devastador para la privacidad en Facebook. Se hizo evidente cómo los datos de millones de usuarios fueron recopilados y utilizados sin consentimiento, influyendo en decisiones políticas y manipulación en las elecciones presidenciales (Pew Research Center, 2022). Este escándalo, que afectó a aproximadamente 87 millones de usuarios, despertó una preocupación ya a nivel global acerca de la privacidad y la ética en el uso de datos (Granville, 2018).

La implementación del Reglamento General de Protección de Datos (RGPD) en 2018 representó un intento significativo de abordar estos problemas en Europa, estableciendo requisitos más estrictos para la recopilación y manejo de datos, pero la complejidad de las políticas de privacidad y la falta de claridad en su comunicación dificultaron que los usuarios comprendieran sus derechos. No obstante, desde 1974 existe la Ley de Privacidad (Privacy Act of 1974), la cual estableció principios para la recopilación y uso de información personal por parte del gobierno federal en Estados Unidos. Otorgando a los ciudadanos derechos sobre sus datos, incluyendo acceso y corrección de información. Además de la prohibición de la divulgación sin consentimiento, promoviendo la transparencia y responsabilidad. Su relevancia se ha ampliado al debate contemporáneo sobre la privacidad en plataformas digitales como Facebook.

En julio de 2019, la Comisión Federal de Comercio (FTC) de Estados Unidos impuso a Facebook una multa récord de 5 mil millones de dólares por violaciones a la privacidad de los usuarios, marcando la sanción más alta en la historia de la FTC y una de las más significativas en el país. Esta sanción se debió al incumplimiento por parte de Facebook de un acuerdo de privacidad establecido en 2012, en el cual la empresa se comprometió a proteger adecuadamente la información de los usuarios y a ser más transparente sobre el uso de estos.

A pesar de las sanciones y cambios legislativos, la vulnerabilidad de los datos en Facebook continúo. En 2021, se conoció que más de 500 millones de usuarios habían visto comprometida su información personal, que terminó en manos de hackers, un incidente global, que afectó a personas en más de 106 países (Fernández, 2022) . La divulgación de información privada no solo suscitó preocupaciones sobre la privacidad de los usuarios, sino que también incrementó el riesgo de que fueran blanco de campañas de phishing y otros fraudes en línea, evidenciando así la vulnerabilidad persistente de nuestras interacciones en redes sociales.

El caso más reciente se produjo en septiembre de 2024, cuando la Comisión de Protección de Datos de Irlanda (DPC) impuso una multa de 91 millones de euros a Meta, la empresa matriz de Facebook, por almacenar contraseñas de usuarios en texto plano y sin el cifrado adecuado. Este fallo de seguridad, descubierto en 2019, reveló una grave vulnerabilidad en la gestión de datos personales, que Meta notificó a la DPC tras darse cuenta del problema. Se determinó que Meta había violado varios artículos del Reglamento General de Protección de Datos (RGPD), entre ellos:

Artículo 5. Falta de implementación de medidas técnicas y organizativas adecuadas para asegurar la seguridad de las contraseñas.
Artículo 32. Incumplimiento en garantizar un nivel adecuado de seguridad frente a riesgos.
Artículo 33. Falta de comunicación del problema en un tiempo razonable.

La magnitud de estos incidentes es alarmante no solo por la cantidad de información que está en juego, sino también por las implicaciones que tienen para la autonomía y dignidad de las personas. En este sentido, se vuelve imperativo que los usuarios tomen un papel activo en la protección de su propia privacidad, elevando su conciencia sobre el manejo de sus datos personales.

En la siguiente tabla se resumen algunos de los incidentes más significativos en la historia de Facebook relacionados con la vulneración de la privacidad.

Tabla 3. ***Casos de vulneración de privacidad en redes sociales***

Año	Incidente	Descripción
2006	Introducción de "News Feed"	Las actividades de los usuarios fueron expuestas sin su consentimiento explícito, generando críticas sobre la protección de la información personal.
2007	Lanzamiento de "Beacon"	Servicio que compartía automáticamente las acciones de los usuarios en otros sitios web sin su conocimiento, considerado una violación de la privacidad.
2010	Cambios en configuración de privacidad	Modificaciones que complicaron el control de la información por parte de los usuarios, resultando en una mayor exposición de datos personales.
2011	Auditorías de privacidad	Facebook aceptó someterse a auditorías tras denuncias de múltiples organizaciones sobre infracciones a las leyes de protección al consumidor.
2013	Acceso de terceros a datos personales	Revelación de que aplicaciones de terceros podían acceder a datos personales sin autorización explícita de los usuarios.
2013	Revelaciones de PRISM	Documentos publicados por Edward Snowden mostraron que Facebook estaba involucrado en un programa de vigilancia masiva de la NSA, recolectando comunicaciones de usuarios.

Fuente: Elaboración propia.

2.6 Privacidad como derecho fundamental

La privacidad es reconocida como un derecho humano fundamental, consagrado en diversos instrumentos internacionales que establecen su importancia en la protección de la dignidad y autonomía de las personas. Por ejemplo, el artículo 12 de la Declaración Universal de Derechos Humanos (1948) establece que "nadie será objeto de injerencias arbitrarias en su vida privada, en su familia, su domicilio o su correspondencia", mientras que el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966) refuerza esta idea al afirmar que "toda persona tiene derechos a la protección de la ley contra tales injerencias o ataques".

Desde el año 2013, el derecho a la privacidad en el contexto digital ha tomado relevancia en el ámbito internacional. La Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos han adoptado diversas resoluciones sobre este tema, resaltando la necesidad de salvaguardar la privacidad frente a las crecientes amenazas que surgen con la era digital. La resolución más reciente, identificada como A/HRC/RES/42/15 aprobada en septiembre de 2019, enfatiza que es responsabilidad de los Estados garantizar que cualquier intervención en el derecho a la privacidad cumpla con los principios de legalidad, necesidad y proporcionalidad. Este enfoque

es indispensable para proteger a los individuos frente a abusos y garantizar que su información personal no se vea comprometida.

Además, la resolución destaca que los derechos fundamentales, incluido el derecho a la privacidad, deben ser resguardados en el entorno digital, considerando el impacto de tecnologías emergentes, como la inteligencia artificial, que podría afectar la realización de este derecho y otros derechos humanos. Las recomendaciones contenidas en el documento están dirigidas tanto a los Estados miembros como a las empresas, instándolos a cumplir con sus obligaciones en el respeto y la protección del derecho a la privacidad en esta nueva era digital.

La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) ha destacado que el derecho a la privacidad es esencial para el ejercicio y el disfrute de los derechos humanos tanto en línea como fuera de línea. Este derecho es uno de los cimientos de una sociedad democrática, ya que facilita la realización de diversas libertades esenciales, como la libertad de expresión, la capacidad de asociarse y reunirse, así como el acceso a derechos económicos y sociales. La ACNUDH también señala que cualquier violación del derecho a la privacidad puede tener efectos desproporcionados, afectando especialmente a ciertos grupos o individuos, lo que puede incrementar la desigualdad y la discriminación. Por lo tanto, es vital que tanto los gobiernos como las empresas asuman una responsabilidad proactiva en la salvaguarda de la privacidad, asegurándose de que las políticas y prácticas digitales promuevan y respeten estos derechos fundamentales, contribuyendo a una sociedad más justa y equitativa.

Según el informe de la ONU sobre el derecho a la privacidad en la era digital, este derecho no solo es un mecanismo de defensa contra injerencias arbitrarias, sino que también empodera a las personas al brindarles control sobre su información personal y su utilización en la esfera digital. La protección de la privacidad está estrechamente vinculada al respeto de la identidad individual y la dignidad humana, aspectos que son esenciales para mantener el resguardo de la vida privada y las comunicaciones personales. En este sentido, la promoción de normas de privacidad robustas es un imperativo no solo legal, sino moral, que busca avanzar en una sociedad donde se respete plenamente el derecho de cada individuo a gestionar su información sin temor a abusos o violaciones (ONU, 2021).

2.7 Estadísticas y percepción de privacidad

El informe del Pew Research Center titulado “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information” pone de manifiesto una creciente inquietud entre la población estadounidense respecto a la seguridad de sus datos personales. Según el estudio, un 70% de los adultos opinan que su información es menos segura hoy en día en comparación con hace cinco años. Esta sensación de vulnerabilidad refleja un escepticismo creciente acerca de cómo las empresas y el gobierno gestionan la recolección de datos. De hecho, el 81% de los encuestados considera que los riesgos asociados con la recopilación de información por parte de las empresas son mayores que sus beneficios, mientras que un 66% siente lo mismo respecto a las acciones del gobierno. Esta atmósfera de desconfianza se acentúa por el comportamiento de muchos usuarios, ya que aproximadamente el 36% admite que nunca se detiene a leer las políticas de privacidad antes de aceptarlas, lo que sugiere una falta de conciencia o interés en entender lo que están aceptando con su consentimiento.

Ante estas preocupaciones, es notable que un 79% de los participantes en la encuesta se muestre escéptico sobre la capacidad de las empresas para manejar correctamente su información. Esto plantea un desafío para las organizaciones, que deben trabajar arduamente para recuperar y fortalecer la confianza del consumidor en este crítico panorama.

El informe también revela diferencias significativas en la percepción de la privacidad según distintos grupos demográficos, como la edad, la etnia y la educación. Esto indica que las estrategias de protección de datos necesitan adaptarse para ser más efectivas y representativas de la diversidad de la sociedad.

En el caso de Facebook, la plataforma ofrece alternativas para las configuraciones de privacidad, pero su compleja interfaz puede dificultar que los usuarios manejen adecuadamente su seguridad. La información crucial se encuentra dispersa en diferentes secciones, lo que puede generar confusión o porque no decirlo, quien quiere leer 22 páginas de políticas de configuraciones. Es de resaltar, que por ejemplo la función de "borrar historial" no elimina permanentemente los datos, sino que simplemente los desvincula de la cuenta del usuario, nada es secreto en las redes y tampoco se puede borrar por completo nuestro rastro.

Aunque Facebook ha eliminado algunas funciones controvertidas, como el reconocimiento facial, los usuarios aún tienen la opción de etiquetarse en publicaciones, permitiendo ajustar quién puede ver dichas publicaciones y exigir aprobación antes de que estas sean visibles para otros. Sin embargo, el control de los usuarios sobre su propia información sigue siendo limitado. A pesar de que la plataforma permite a los usuarios revisar su "Actividad fuera de Facebook", esto no significa que puedan eliminar sus datos de forma definitiva.

A pesar de ello, curiosamente con todas las inquietudes sobre la privacidad, la mayoría de los usuarios de Facebook continúan activamente en la plataforma. Un 54% ha ajustado sus configuraciones de privacidad, y un 81% expresa su preocupación por cómo las empresas utilizan sus datos personales. Esta dinámica revela una paradoja atractiva: los usuarios eligen sacrificar parte de su privacidad por los beneficios sociales y el sentido de pertenencia que la plataforma les proporciona, en un mundo complejo, donde el deseo de conexión y comunidad puede superar el anhelo de proteger la información personal.

Al parecer las personas, no comprenden la dimensión y las consecuencias que conlleva la vulneración de la privacidad en el ámbito digital. Una de las consecuencias más comunes es el acoso en línea, donde los acosadores pueden acceder a información personal obtenida a través de redes sociales para hostigar, amenazar o difamar a sus víctimas. Este tipo de hostigamiento puede generar efectos perjudiciales significativos en la salud mental de las personas, como ansiedad, depresión e, incluso, en casos extremos, el suicidio.

Otra de las graves consecuencias, el robo de identidad, dónde los delincuentes utilizan información personal expuesta para llevar a cabo actividades fraudulentas, como abrir cuentas bancarias, solicitar dinero, tarjetas de crédito a nombre de la víctima. Situaciones que no solo pueden acarrear pérdidas financieras considerables, sino que también es evidente el riesgo en la reputación de la persona afectada. No olvidemos, las más de 530 millones de cuentas de Facebook que fueron

expuestas en una violación de datos en 2019 (Krishnan, 2021). Esta brecha expuso datos sensibles como números de teléfono, nombres completos, ubicaciones, fechas de nacimiento y direcciones de correo electrónico, lo que facilitó el robo de identidad y otros fraudes.

El estudio realizado por la firma McKinsey & Company (2020) destacó que el 60% de los consumidores están dispuestos a cambiar sus hábitos de consumo si sienten que una marca está comprometida con la protección de su privacidad. Este hallazgo subraya la importancia de que las empresas no solo implementen políticas de privacidad, sino que también comuniquen de manera clara su compromiso con la protección de los datos de los usuarios.

2.8 ¿Cómo proteger tu privacidad en Facebook?

La protección de la privacidad en Facebook es esencial en un mundo donde millones de personas comparten constantemente información personal. A continuación, se detallan algunos consejos prácticos de empresas expertas en ciberseguridad y protección de datos, para mantener la información segura y privada en esta plataforma social.

Optimizar la seguridad de la cuenta
Creación de una contraseña fuerte: Utilizar contraseñas únicas y robustas para cada cuenta. Combinación de letras mayúsculas, minúsculas, números y caracteres especiales. Evitar datos personales como fechas de nacimiento o nombres de mascota. Apoyarse en generadores de contraseñas.
Habilitar la autenticación de dos factores (2FA): Activar esta función para añadir una capa extra se seguridad. Con 2FA, se necesitará un código adicional para acceder a la cuenta, reduciendo significativamente el riesgo de acceso no autorizado.

Configurar la privacidad del perfil
Revisar y Ajustar la Configuración de Privacidad: Limita quién puede ver la información y las publicaciones. Definir opciones predeterminadas para las publicaciones y asegurarse que solo los amigos o conexiones de confianza puedan acceder a nuestro perfil.
Decide Quién Puede Ver las Publicaciones: Al crear una nueva publicación, elegir quién puede ver el contenido. Seleccionar entre las opciones como “Público”, “Amigos”, o “Sólo yo”.

Monitorear sesiones y ajustes de preferencias
Revisa los inicios de sesión: Regularmente, revisar desde dónde se ha accedido a la cuenta y cerrar sesiones desconocidas. Esto se puede hacer en la sección de “Seguridad e inicio de sesión”.
Recibe alertas de inicios de sesión sospechosas: Configura las notificaciones para que llegue el aviso sobre inicios de sesión no reconocidos, esto permite reaccionar rápidamente antes este tipo de actividades.

Cautela con la información que compartes
Limita la información personal compartida: No publicar información sensible, como ubicación, horario, datos relevantes que puedan ser usados con otros fines.
Desconfiar de mensajes sospechosos: Siempre verificar la autenticidad de mensajes o enlaces inesperados, ya que podrían ser intentos de phishing o malware.

Actualización de software
Actualizar regularmente los dispositivos: Asegurar que el software y aplicaciones se encuentren actualizados para aprovechar las funcionalidades de protección y parches de seguridad. Según datos, solo el 42% de los usuarios de smartphones en Estados Unidos, actualizan automáticamente el software.

Educar a nuestro entorno sobre seguridad en línea
Compartir Conocimientos: Hablar con los familiares y amigos, sobre la importancia de la seguridad en redes sociales. Una comunidad informada puede ayudar a prevenir ataques.
Configura Opciones de Seguridad en Otros Dispositivos y Aplicaciones: No limitarse a Facebook, estas medidas de seguridad aplican en todas las redes sociales y dispositivos.

Revisar y controlar aplicaciones conectadas
Desvincular Aplicaciones No Utilizadas: Revisar las aplicaciones y servicios conectados a la cuenta de Facebook y eliminar aquellos que ya no se utilicen.
Gestionar Preferencias de Anuncios: Revisar qué información se utiliza para dirigirte anuncios y ajustas las preferencias para limitar la publicidad basada en los datos personales.

3. Metodología

En este artículo de investigación, se emplearon fuentes sociojurídicas, fuentes primarias y secundarias para la recopilación de datos, lo que permite obtener una visión integral y fundamentada de la problemática de la privacidad en el contexto de la plataforma Facebook. Esta aproximación metodológica garantiza una compresión profunda de la evolución del concepto de privacidad a lo largo de la historia, desde las perspectivas de diferentes autores, las preocupaciones y comportamientos de los usuarios en relación con la protección de su información personal.

3.1 Tipo de investigación

La presente investigación se clasifica como un estudio descriptivo y analítico. Se enfoca en examinar la relación de Facebook con la privacidad, analizando cómo la plataforma maneja la información personal de los usuarios y las implicaciones que esto tiene en su percepción de privacidad. Dado el enfoque propuesto, está investigación no busca establecer relaciones causales entre variables, sino más bien describir y analizar el estado actual y las preocupaciones de los usuarios en torno al tema de la privacidad en el entorno digital.

3.2 Diseño de la investigación

El diseño metodológico adoptado para esta investigación es de tipo documental descriptivo. Esto implica la recopilación y análisis de la información secundaria obtenida de fuentes confiables, como informes de organizaciones, estudios estadísticos como Statista, Pew Research Center, legislación y organizaciones de defensa del consumidor que han investigado la privacidad en Facebook, más la literatura académica relevante. Este enfoque permite un análisis crítico de la información existente sobre la privacidad en Facebook.

3.3 Fuentes de información

Para la recolección de datos, se han utilizado las siguientes fuentes:

Fuentes primarias que incluyen, la información crucial sobre los derechos humanos en el mundo digital, enfocado principalmente en el derecho a la privacidad y la protección de datos, informes y documentos elaborados por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), que ofrecen un marco normativo que permite contextualizar la situación de la privacidad de los usuarios en plataformas como Facebook.

De igual manera, informes que abarcan la percepción de los usuarios sobre la privacidad de su información en Facebook. Se examinan sus preocupaciones, el nivel de conocimiento que tienen sobre las políticas de privacidad de la plataforma y las acciones que llevan a cabo para proteger sus datos. Esta información se obtiene a través de una revisión de estudios previos, informes como Statista, Pew Research Center, Kolsquare y literatura existente que abordan esta perspectiva.

Fuentes secundarias dónde se abarcaron, las normas internacionales relativas a la privacidad digital, de la Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos, que han aprobado numerosas resoluciones referentes al derecho a la privacidad en la era digital. Estas normas establecen directrices sobre la protección de datos y la privacidad en plataformas digitales, incluyendo Facebook, y son fundamentales para entender el marco normativo que rige la recopilación y el uso de datos personales en el ámbito digital.

De igual manera la regulación de la Unión Europea, la General Data Protection Regulation (GDPR), la cual establece normas estrictas sobre la protección de datos personales y la privacidad, influyendo directamente en las prácticas de Facebook al tener que adaptar su manejo de datos de usuarios europeos, marcando así una protección de privacidad digital para toda la industria tecnológica.

La Ley de Privacidad del Consumidor de California (CCPA), que es una de las legislaciones más estrictas en materia de privacidad en los Estados Unidos, con un impacto significativo en cómo Facebook debe manejar los datos de los usuarios que residen en California. Esta ley contribuye al empoderamiento de los consumidores respecto al uso de sus datos y la responsabilidad que tienen las plataformas en el tratamiento de esta.

A través de esta combinación de fuentes primarias y secundarias, la investigación busca proporcionar un análisis exhaustivo y crítico sobre la relación entre Facebook y la privacidad, revelando la complejidad y los desafíos que enfrentan los usuarios en el entorno digital actual.

3.4 Instrumentos de recolección de información

Dado que la investigación se basa en un enfoque documental, no se diseñaron instrumentos de recolección de datos convencionales como encuestas o entrevistas. En su lugar, se aplicó una estrategia de revisión comparativa sistemática de literatura. Se realizó un análisis crítico de las fuentes de datos seleccionadas, con el objetivo de extraer información relevante y estadística que apoyara la comprensión de problemática relacionada con la privacidad en Facebook.

Para llevar a cabo esta tarea, se consideraron categorías de información:

Percepciones sobre la privacidad: Se recopilaron datos que reflejan las opiniones y sentimientos de la población respecto a cómo se maneja la privacidad en Facebook. Esto incluye la percepción de la seguridad y las preocupaciones relacionadas con el uso de sus datos personales.

Datos demográficos: Se analizaron estadísticas que brindan un contexto sobre los diferentes perfiles de usuarios que manifiestan inquietud por la privacidad. Esta información facilita la identificación de patrones y tendencias en las preocupaciones de distintos grupos demográficos.

Impacto de incidentes de vulneración de privacidad y protección de datos: Se revisaron informes y estudios que documentan como escándalos significativos, como la filtración de datos de Cambridge Analytica, han influido en la confianza de los usuarios hacia la plataforma. Este análisis permite entender el efecto de tales eventos en la percepción colectiva de la privacidad.

Medidas de protección recomendadas: Se llevó a cabo un análisis de las sugerencias y recomendaciones proporcionadas por expertos en ciberseguridad y organizaciones dedicadas a la protección de datos. Esta información destaca las estrategias propuestas para mejorar la gestión de la privacidad en Facebook y empoderar a los usuarios.

Este enfoque metódico y riguroso garantiza que la investigación examine a fondo la situación de la privacidad en Facebook, utilizando fuentes primarias y secundaras confiables, sin la necesidad de realizar encuestas directas. Así, se logra mantener un alto estándar en el tratamiento de los datos existentes y en la obtención de conclusiones significativas del tema.

3.5 Análisis de la información

El análisis de la información recopilada se llevó a cabo siguiendo estos pasos:

1.Clasificación de Datos: Se organizaron los datos extraídos de las diversas fuentes en categoría temáticas que reflejan la evolución del concepto de privacidad, aspectos de la privacidad en Facebook.

2. Análisis Cualitativo: Se examinó el contenido de los informes y estudios a partir de una lectura crítica que permite identificar patrones, temas recurrentes y percepciones de los usuarios. Se consideraron las citas de autores relevantes sobre la temática, reflexionando sobres sus implicaciones en el contexto de Facebook.

3. Análisis Cuantitativo: Se interpretaron las cifras y estadísticas extraídas de los informes, evaluando tendencias y diferentes aspectos relacionados con la percepción de los usuarios sobre la privacidad.

4. Síntesis de Resultados: Finalmente, se elaboró un resumen de los hallazgos más relevantes, integrando las conclusiones obtenidas tanto en el análisis cualitativo como cuantitativo.

4. Resultados

Los hallazgos de la investigación indican que la mayoría de los usuarios de Facebook están preocupados por su privacidad, con un 70% expresando desconfianza en cómo se manejan sus datos personales. A pesar de esta preocupación, solamente un 54% ha ajustado sus configuraciones de privacidad, lo que sugiere que, aunque reconocen los riesgos, buscan formas de mantener cierta medida de control sobre su información.

Además, estudios como el de Pew Research Center revelan que un 70% de los adultos en Estados Unidos creen que su información personal es menos segura que en años anteriores. El comportamiento de los usuarios representa un 36% que admite no leer las políticas de privacidad, evidencia una desconexión entre la percepción y las acciones a concretar que podrían mitigar los riesgos asociados. El informe de la ACNUDH señala la falta de transparencia y rendición de cuentas asociada con la recopilación y el uso de datos, lo que profundiza la desconfianza de los usuarios.

Los incidentes de vulneración de privacidad, como el caso de Cambridge Analytica, pusieron de manifiesto los peligros del uso de datos sin el consentimiento informado del usuario, llevando a una mayor desconfianza hacia Facebook. La investigación también resalta cómo la complejidad de las configuraciones de privacidad en la plataforma dificulta que los usuarios gestionen efectivamente su seguridad, ocasionando efectos adversos en su bienestar emocional y sentido de pertenencia.

El informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos revela la preocupación con la integración de tecnología de inteligencia artificial en plataformas digitales, a medida que estas se vuelven cada vez más comunes y los usuarios deben estar cada vez más conscientes de las implicaciones negativas que pueden surgir.

5. Discusión

La relación entre los usuarios y plataformas como Facebook presenta una paradoja significativa: la promesa de conectividad y la preocupación creciente por la privacidad. A pesar de que cada vez más usuarios expresan inquietudes sobre el manejo de sus datos personales, muchos eligen seguir utilizando la plataforma, priorizando sus necesidades sociales sobre la protección de su información.

Este dilema se ve reflejado en un informe reciente que indica que el 79% de los encuestados desconfían de la capacidad de las empresas para gestionar adecuadamente su información, lo que nos lleva a cuestionar cómo llevar esta línea tan delgada entre conexión y privacidad.

La discusión en torno a la evolución del concepto de privacidad y su enfoque a través del tiempo resalta la necesidad de educar a los usuarios sobre el manejo responsable de sus datos. La literatura académica respalda la idea de que los derechos de privacidad son fundamentales para la libertad y bienestar en la era digital. Sin embargo, a medida que las redes sociales continúan creciendo y evolucionando, es vital que las regulaciones se ajusten y que las plataformas adopten mecanismos más transparentes y responsables en el tratamiento de datos.

La percepción de inseguridad en torno a la privacidad apunta a un diálogo necesario entre los usuarios y las plataformas sociales, donde ambas partes deben colaborar proactivamente. La falta de confianza generada a partir de escándales pasados debe ser abordada no solo a través de cambios en políticas, sino también mediante la creación de un entorno donde los usuarios se sientan con el poder de ejercer el control sobre su información personal.

Conclusiones

En el umbral de esta nueva era digital, la relación entre Facebook y la privacidad se revela como un fuerte dilema psicosocial que apuesta por nuestra esencia misma como seres humanos. Mientras navegamos por la vastedad de esta plataforma, nos encontramos atrapados en una encrucijada donde el deseo de conexión social y validación personal choca con la necesidad inalienable de proteger nuestra información y dignidad. Aunque la alerta sobre las vulneraciones a la privacidad ha sonado en múltiples ocasiones, el hechizo adictivo de la "dopamina digital" nos mantiene cautivos, dejando en las sombras nuestras preocupaciones en pro de la interacción constante.

Las estadísticas apuntan al crecimiento exponencial de Facebook, resaltando la tentación irresistible de una comunidad virtual, que, aunque puede conectarnos y acercarnos, también entreteje los riesgos profundos para nuestra privacidad. El bombardeo constante de funciones de interacción sólo intensifica este fenómeno, reforzando preferencias de uso y sumiendo a los usuarios en un ciclo de gratificación instantánea.

Sin embargo, en esta revolución digital, donde las regulaciones como el GDPR y la CCPA parecen ser insuficientes, emerge con fuerza la imperiosa necesidad de educar y empoderar a los usuarios. La responsabilidad no puede recaer solo en el ente regulador o en las plataformas, sino que debe ser un esfuerzo colectivo que involucre a todos los actores de este universo digital. Al fomentar la sensibilización sobre los riesgos y promover buenas prácticas de seguridad, podemos empoderar a los usuarios a tomar decisiones informadas.

El desafío de equilibrar la conectividad con la privacidad no es solo una cuestión técnica, sino un compromiso moral, social y ético. Requiere que repensemos la privacidad, no solo como un derecho individual, sino como el pilar esencial para la dignidad y autonomía en este nuevo mundo digital. La frase de Xavier Báez encapsula esta complejidad: "Las redes sociales son como un gran evento que nunca termina; mientras más lo usas, más te conocen". A medida que nos adentramos en este megaverso, es vital que cultivemos una conciencia crítica, demostrando que podemos coexistir en armonía, el entorno digital sin comprometer nuestra dignidad individual, manteniendo intacta la esencia de lo que significa ser humano en esta era digital.

Referencias

AFP. (2024, septiembre 27). La UE multa a Meta con 91 millones de euros por almacenar las contraseñas de sus usuarios sin medidas de seguridad. ABC.es. https://www.abc.es/tecnologia/ue-multa-meta-millones-euros-almacenar-contrasenas-20240927170723-nt.html?ref=https%3A%2F%2Fwww.abc.es%2Ftecnologia%2Fue-multa-meta-millones-euros-almacenar-contrasenas-20240927170723-nt.html

Auxier, B. (2019, noviembre 15). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Auxier, B. (2021, abril 7). Social media use in 2021. Pew Research Center. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Delgado, A. (2024, septiembre 27). Irlanda multa a Facebook (Meta) con 91 millones de euros por almacenar contraseñas en texto plano. GEEKNETIC. https://www.geeknetic.es/Noticia/32785/Irlanda-multa-a-Facebook-Meta-con-91-millones-de-euros-por-almacenar-contrasenas-en-texto-plano.html

Facebook. (s/f). Facebook.com. https://es-la.facebook.com/help/155833707900388/

Facebook MAU worldwide 2023. (s/f). Statista. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Garcia, E. (s/f). El Derecho a la Privacidad (de Samuel Warren y Louis Brandeis). Datalawrd.com. https://datalawrd.com/el-derecho-a-la-privacidad-de-samuel-warren-y-louis-brandeis/

GDPR: Lo que debes saber sobre el reglamento general de protección de datos. (s/f). Powerdata.Es. https://www.powerdata.es/gdpr-proteccion-datos

Global social media statistics — DataReportal – global digital insights. (s/f). DataReportal – Global Digital Insights. https://datareportal.com/social-media-users

La ciberseguridad en redes sociales: los riesgos y cómo mantenerse a salvo - Revista Seguridad 360. (2023, noviembre 14). Redacción Revista Seguridad 360. https://revistaseguridad360.com/noticias/ciberseguridad-en-redes-sociales/

La FTC impone penalidad de $5 mil millones y nuevas restricciones de privacidad de gran envergadura a Facebook. (2019, julio 23). Comisión Federal de Comercio. https://www.ftc.gov/es/noticias/la-ftc-impone-penalidad-de-5-mil-millones-y-nuevas-restricciones-de-privacidad-de-gran-envergadura

La manipulación emocional es el último intento de Facebook de usar a sus usuarios. (2014, julio 3). MIT Technology Review. https://www.technologyreview.es/s/4299/la-manipulacion-emocional-es-el-ultimo-intento-de-facebook-de-usar-sus-usuarios

Mohsin, M. (2020, noviembre 19). 10 Facebook statistics you need to know in 2023 [new data]. Oberlo. https://www.oberlo.com/blog/facebook-statistics

Newberry, C. (2024, agosto 21). Seguridad en redes sociales: riesgos, buenas prácticas y herramientas [2024]. Social Media Marketing & Management Dashboard. https://blog.hootsuite.com/es/riesgos-de-seguridad-en-redes-sociales/

Osman, M. (2019, febrero 6). Datos y Estadísticas Locas e Interesantes de Facebook 2024. Kinsta®; Kinsta. https://kinsta.com/es/blog/estadisticas-facebook/

Países más afectados por las filtraciones de datos de Facebook de abril de 2021. (s/f). Statista. https://es.statista.com/estadisticas/1227472/ciberdelincuencia-paises-mas-afectados-las-filtraciones-de-datos-en-facebook/

Panichas, G. E. (2014). An intrusion theory of privacy. Res Publica (Liverpool, England), 20(2), 145–161. https://doi.org/10.1007/s11158-014-9240-3

Pérez, A. (2022, noviembre 9). 25 Datos y Estadísticas de Facebook esenciales para 2024. Reactiva Online. https://www.reactivaonline.com/estadisticas-facebook/

Qué dicen los 7 principios de privacidad de Facebook que la red social acaba de revelar por primera vez (y cómo aprovecharlos). (2018, enero 31). BBC. https://www.bbc.com/mundo/noticias-42873573

Ramírez, H. (2023, marzo 31). 10 grandes casos en los que la privacidad digital se vio vulnerada. Grupo Atico34; Ático34 Protección de datos para empresas y autónomos. https://protecciondatos-lopd.com/empresas/casos-privacidad-digital/

Rivera, M. G. (2024, enero 17). Platón y Aristóteles: Visiones Económicas Contrastantes. Economía Histórica. https://economiahistorica.com/platon-y-aristoteles-economia/

Rosen, J. (2000). The unwanted gaze: The destruction of privacy in America. Random.

Ruiz, P. A. (2014, junio 30). Así manipuló Facebook las emociones de sus usuarios. Ediciones EL PAÍS S.L. https://elpais.com/elpais/2014/06/30/icon/1404123574_764889.html

Skelton, S. K. (2019, agosto 7). El dilema de Facebook: a pesar del escándalo, la privacidad no paga. ComputerWeekly.es; TechTarget. https://www.computerweekly.com/es/cronica/El-dilema-de-Facebook-a-pesar-del-escandalo-la-privacidad-no-paga

Thornton, N. (2023, septiembre 6). Guard Your Secrets: Unveiling the consequences of ignoring online privacy. PrivacyEnd. https://www.privacyend.com/consequences-ignoring-online-privacy/

United Nations. (s/f). La Declaración Universal de los Derechos Humanos | Naciones Unidas. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Vanguardia, L. (2021, abril 3). Alerta en la red: Filtrados los datos de 11 millones de cuentas de Facebook en España. La Vanguardia.

https://www.lavanguardia.com/tecnologia/20210403/6625798/facebook-hackeo-pirateo-cuentas-informacion-datos-robo.html

Walker, M. (2021, septiembre 20). News consumption across social media in 2021. Pew Research Center. https://www.pewresearch.org/journalism/2021/09/20/news-consumption-across-social-media-in-2021/

Westin, A. F. (1967). Privacy and freedom ([1st ed.]). Atheneum.

(S/f-a). Ohchr.org. https://www.ohchr.org/es/calls-for-input/2021/right-privacy-digital-age-report-2021

(S/f-b). Ohchr.org. https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

(S/f-c). Ohchr.org. https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy

(S/f-d). Congress.gov. https://www.congress.gov/bill/93rd-congress/house-bill/16373

(S/f-e). Pewresearch.org. https://www.pewresearch.org/2022/01/20/the-state-of-privacy-in-america/

(S/f-f). Reuters.com. https://www.reuters.com/technology/more-than-530-million-facebook-accounts-exposed-data-breach-2021-04-08/

(S/f-g). Mckinsey.com. https://www.mckinsey.com/featured-insights/consumer-and-retail/the-consumer-data-gap