Vulneración al derecho a la intimidad a través de Facebook en Colombia

Juan Felipe Botero Villegas

Trabajo de grado presentado para optar al título de Especialista en Derechos Humanos y Derecho Internacional Humanitario

Universidad de Antioquia
Facultad de Derecho y Ciencias Políticas
Especialización en Derechos Humanos y Derecho Internacional Humanitario
Medellín, Antioquia, Colombia
2023

Cita	(Botero Villegas, 2023)
Referencia **Estilo APA 7 (2020)**	Botero Villegas (2023). *Vulneración al derecho a la intimidad a través de Facebook en Colombia*. [Trabajo de grado especialización]. Universidad de Antioquia, Medellín, Colombia.

Especialización en Derechos Humanos y Derecho Internacional Humanitario, Cohorte XII.

Resumen

En el ámbito digital contemporáneo, la privacidad emerge como un pilar esencial, respaldando la confianza y seguridad en tecnologías y redes, especialmente dada la omnipresencia de estas últimas y el constante intercambio de datos. Esta investigación se centra en la interrelación de privacidad, constitucionalidad, regulación y buen gobierno, poniendo particular atención en Facebook y el contexto colombiano. Se explorará la evolución del derecho a la privacidad desde perspectivas geográficas variadas, incluyendo la Unión Europea con su Reglamento General de Protección de Datos (GDPR), Estados Unidos y Colombia. En el panorama colombiano, se destacará la relación de privacidad con redes sociales, y se examinará el marco legal que rodea dichas plataformas. Además, se reflexionará sobre la importancia de la privacidad en relación con la buena gobernanza en el ciberespacio, enfatizando el papel de Facebook y la emergencia del "derecho blando" para establecer estándares de privacidad, mientras se contempla el equilibrio esencial entre conectividad y protección de datos en nuestra era digital.

Palabras clave: Era digital, derecho a la privacidad, redes sociales, buen gobierno, Facebook.

Abstract

In the contemporary digital environment, privacy emerges as an essential pillar, supporting trust and security in technologies and networks, especially given the omnipresence of the latter and the constant exchange of data. This research focuses on the interrelationship of privacy, constitutionality, regulation and good governance, paying particular attention to Facebook and the Colombian context. It will explore the evolution of the right to privacy from varied geographical perspectives, including the European Union with its General Data Protection Regulation (GDPR), the United States and Colombia. In the Colombian scenario, the relationship of privacy with social networks will be highlighted, and the legal framework surrounding such platforms will be

examined. In addition, it will reflect on the importance of privacy in relation to good governance in cyberspace, emphasizing the role of Facebook and the emergence of "soft law" to establish privacy standards, while contemplating the essential balance between connectivity and data protection in our digital age.

*Keywords***:** Digital age, right to privacy, social networks, good governance, Facebook.

Sumario: Introducción. **1.** La Constitucionalización del derecho a la privacidad: Un análisis a partir de las redes sociales. **1.1.** Constitucionalización de la privacidad en la era digital. **1.1.1.** Caso Unión Europea. **1.1.2.** Caso Estados Unidos. **1.1.3.** Caso Colombia. **1.2.** El Derecho a la privacidad caso Facebook. **2.** Privacidad y Redes Sociales en Colombia: A propósito de Facebook. 2.1. Facebook en Colombia. **2.2.** Legislación sobre redes sociales en Colombia. **3.** El derecho a la privacidad en el ciberespacio: Un acercamiento a partir del buen gobierno. **3.1.** Facultad discrecional de Facebook para hacer uso de la información personal de los usuarios. **3.2.** El derecho blando en la consolidación de tratados multilaterales en pro de la privacidad. **3.3.** Retos y desafíos en materia de privacidad en el ciberespacio. Conclusiones.

Introducción

En la era digital, la privacidad se ha convertido en uno de los pilares fundamentales que sustentan la confianza y seguridad en el uso de tecnologías y redes sociales. La omnipresencia de las redes y el flujo continuo de datos han generado una creciente inquietud sobre cómo se recopila, almacena y utiliza nuestra información personal. Esta exploración temática se adentrará en la intersección entre la privacidad, la constitucionalidad, la regulación y el buen gobierno en el ciberespacio, con un enfoque particular en la plataforma de Facebook y el contexto colombiano.

En un primer momento, se abordará el reconocimiento del derecho a la privacidad en el marco constitucional, haciendo especial énfasis en su manifestación en la era digital. Lo anterior, exponiendo de modo general, como las redes sociales, las cuales representan el reflejo y potenciador de nuestra sociedad hiperconectada, han acentuado la necesidad de abordar y definir este derecho con claridad. A partir de ello, A partir de ello, se desarrolla su alcance constitucional

Luego, la presente revisión documental se traslada al derecho internacional, abarcando la temática desde la Unión Europea, donde el Reglamento General de Protección de Datos (GDPR) ha sentado un precedente significativo en cuanto a la regulación de datos, pasando por Estados Unidos, con un enfoque más fragmentado y orientado al mercado, hasta llegar a Colombia, que busca armonizar sus políticas con estándares internacionales. En paralelo, se desentrañará el caso de Facebook, una entidad que, por su alcance global y posición dominante, ha sido objeto de escrutinio y debate en cuanto a sus políticas de privacidad.

En ese sentido, la construcción de los ejes previamente expuestos, permiten comprender el contexto colombiano, desvelando las particularidades de la relación entre privacidad y redes sociales el país. Facebook, al ser una de las plataformas más utilizadas en Colombia, se erige como un prisma a través del cual se pueden analizar las tensiones y desafíos que presenta la convergencia entre tecnología y privacidad. Además, se abordará el marco legal existente en Colombia respecto a las redes sociales, identificando las medidas adoptadas para proteger a los usuarios y garantizar un uso ético y responsable de los datos.

Es así como, a partir de la construcción temática de esta problemática, el presente artículo se propone una reflexión sobre la relación entre privacidad y buen gobierno en el vasto mundo del ciberespacio. Si bien las plataformas digitales tienen una responsabilidad inherente en la protección de los datos de sus usuarios, es crucial que esta responsabilidad se ejerza con transparencia y equidad (Tapia Hermida, 2021). De manera tal, se analizará cómo Facebook, con su inmensa base de datos y capacidades analíticas, ejerce su facultad discrecional en el manejo de la información personal. Además, se explorará el concepto de "derecho blando" y cómo éste puede servir como herramienta para establecer estándares comunes en la protección de la privacidad, sentando las bases para futuros tratados multilaterales. Ello, supone que se reflexione sobre los desafíos y

obstáculos que enfrenta la garantía de la privacidad en el ciberespacio, considerando la naturaleza cambiante y expansiva de la tecnología.

Por ende, y de acuerdo con los autores Barbosa, Herrera y Rodríguez (2013) el presente trabajo se direccionará bajo una metodología cualitativa, con un enfoque analítico documental, que permite explorar y abordar la temática, de manera tal que a medida que se avance en esta era digital, es vital que exista consciencia del equilibrio entre conectividad y privacidad. Esta exploración busca arrojar luces sobre las múltiples facetas de la privacidad en el ciberespacio, proporcionando un entendimiento profundo de su importancia, los desafíos que presenta y las soluciones viables en pro de un futuro digital más seguro y transparente.

1. La constitucionalización del derecho a la privacidad: un análisis a partir de las redes sociales

El crecimiento exponencial de las redes sociales en las últimas dos décadas ha llevado a un replanteamiento profundo sobre el derecho a la privacidad. Esta explosión comunicativa, que permite a los individuos compartir instantáneamente detalles de su vida, también ha planteado serios interrogantes sobre cómo se protegen, o a menudo se vulneran, los datos e informaciones personales de los usuarios (Toscano, 2017). En este sentido, la constitucionalización del derecho a la privacidad surge como una necesidad imperante para garantizar que las libertades fundamentales no sean eclipsadas por el atractivo magnético de estas plataformas.

Entonces, el concepto de "constitucionalización" se refiere a la elevación de un derecho a la categoría de protección constitucional, la cual es un reconocimiento, a nivel del máximo instrumento jurídico de un país, de la importancia y la inviolabilidad de ese derecho (Ramírez-García, 2022). En el caso de la privacidad, se busca salvaguardar la integridad del individuo contra

injerencias externas, especialmente en un mundo digitalizado, pues la presencia de este derecho en las constituciones nacionales impone un deber a los Estados de protegerlo y garantiza a los ciudadanos un recurso legal contra su violación (Rumaldo Calderón, Tupayachi Torres, & Lodeiros Zubiria, 2024).

Por otro lado, las redes sociales, si bien ofrecen múltiples beneficios en términos de comunicación y acceso a la información, también presentan amenazas significativas ya que la recopilación de datos, el monitoreo constante de actividades y la potencial comercialización de la información personal, son aspectos intrínsecos de su modelo de negocio. Estas plataformas, en muchos casos, han sido acusadas de sobrepasar los límites éticos y legales en lo que respecta al manejo de la información, y aquí es donde la protección constitucional entra en juego (Dumortier, 2009).

Sin embargo, la constitucionalización del derecho a la privacidad no es una panacea, puesto que, si bien proporciona un marco legal firme, su eficacia depende de la interpretación de los tribunales, la implementación de leyes secundarias y, sobre todo, la voluntad política de hacerlas cumplir. Además, la naturaleza global de las redes sociales plantea desafíos jurisdiccionales, ya que una plataforma puede operar en múltiples países, cada uno con su propia interpretación del derecho a la privacidad (Puris Cáceres, et al, 2022).

Es fundamental, entonces, que además de las garantías jurídicas, se promueva una cultura de la privacidad entre los usuarios. Esto implica educar a la población sobre sus derechos y cómo ejercerlos. Pues según la Red Iberoamericana de Protección de Datos (2006), también se debe promover la autorregulación y buenas prácticas entre las empresas de tecnología debido a que, solo con una combinación de protección legal y conciencia ciudadana se podrá enfrentar de manera efectiva los desafíos que las redes sociales plantean a la privacidad.

En conclusión, la incorporación del derecho a la privacidad en las constituciones nacionales es un paso crucial hacia la protección de los individuos en la era digital. Sin embargo, es solo el comienzo de una lucha más amplia que involucra a legisladores, tribunales, empresas y, sobre todo, a los propios usuarios, en la construcción de un espacio digital más seguro y respetuoso de los derechos fundamentales.

1.1. Constitucionalización de la privacidad en la era digital

Habría que decir que la era digital, con sus avances tecnológicos y conexiones instantáneas, ha transformado la manera en que la sociedad se comunica y comparte información. Sin embargo, esta revolución digital también ha llevado a desafíos sin precedentes en cuanto a la protección de la privacidad individual, por lo cual, se debe acudir a la constitucionalización de la privacidad, ya que en este contexto, es el proceso de integrar y reconocer la importancia de la privacidad como un derecho fundamental en las constituciones nacionales, garantizando así su protección frente a las amenazas emergentes en el ciberespacio (Ramírez-García, 2022).

Según, Medan (2020) la privacidad, tradicionalmente, ha sido entendida como el derecho a estar solo o a no ser molestado; no obstante, en el entorno digital, su definición se expande para abarcar la protección contra la recolección no autorizada, el almacenamiento, el uso y la divulgación de datos personales. Por lo que, al constitucionalizar este derecho, se le da una posición de prioridad y recalca lo expuesto por autores como Suárez – Manrique (2014) quién reconoce la necesidad de proteger la integridad personal en un mundo donde la información fluye libremente, a menudo sin el conocimiento o el consentimiento explícito del individuo.

Pese a ello, el autor Ramírez - García (2022) resalta como desde la mera inscripción de este derecho en un texto constitucional no es suficiente, por lo que su efectividad reside en la creación

de leyes secundarias, sentencias, reglamentaciones y políticas públicas, las cuales refuerzan su aplicabilidad; así como establecer sanciones claras para su violación (MercoPress. South Atlantic News Agency, 2023). En el mundo digital y el contexto del ciberespacio, lo anterior significa regular a las empresas tecnológicas, plataformas de redes sociales y otros actores digitales que tienen el potencial de acceder, utilizar y, a veces, abusar de la información personal.

Asimismo, Ramírez-García (2022) ha desarrollado desde el concepto de constitucionalización una manera que permite comprender una base sólida para hacer uso de las garantías constitucionales, aplicados al caso específico de la protección de la privacidad. Ello, no es óbice para dar por entendido en primer momento que este concepto ya se encuentra desarrollado y no cuente con retos y desafíos para ser aplicado en la era digital. La naturaleza global y descentralizada del internet plantea problemas jurisdiccionales, ya que las violaciones de la privacidad pueden ocurrir en cualquier parte del mundo, independientemente de dónde esté ubicada la persona afectada (Figueroa G., 2013). Además, la tecnología evoluciona a un ritmo más rápido que la legislación, lo que puede dejar vacíos legales o hacer que ciertas regulaciones se vuelvan obsoletas rápidamente.

En ese sentido, mientras que la era digital ha llevado a la necesidad de redefinir y reforzar la privacidad a nivel constitucional, este es solo el primer paso en un proceso continuo, por lo que, es esencial que las sociedades sigan adaptándose y respondiendo a los desafíos emergentes, equilibrando las oportunidades de la tecnología con la protección inalienable de los derechos individuales. Situación que enmarca la necesidad de abarcar los ejes temáticos desde casos particulares, cómo lo es la Unión Europea, Estados Unidos y finalmente Colombia, lo cual permitirá comprender el Rol de los Estados a la hora de accionar medidas restrictivas a las

compañías y delimitar aquella autonomía y libertad con la que gozan para hacer uso de la información personal que recopilan, almacenan y utilizan.

1.1.1. Caso Unión Europea.

En un primer caso, la Unión Europea ha sido pionera en reconocer y abordar los desafíos de la privacidad en la era digital. Con la proliferación de la tecnología y la expansión del ciberespacio, según los autores Puerto y Sferrazza (2018) la Unión Europea ha entendido que la protección de la privacidad individual no es simplemente una opción, sino una necesidad fundamental para salvaguardar los derechos de sus ciudadanos La constitucionalización de la privacidad, en este contexto, implica la elevación de la privacidad a un derecho fundamental reconocido y protegido a nivel constitucional y supranacional en el bloque europeo (Parlamento Europeo y Consejo de la Unión Europea, 2016).

En este sentido, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, implementado en (2018), es un ejemplo de este reconocimiento, pues más que una simple ley, el GDPR es un marco regulatorio que refleja el compromiso de la Unión Europea con la privacidad de sus ciudadanos en la era digital. No solo establece directrices claras sobre cómo deben ser tratados los datos personales, sino que también otorga a los individuos un conjunto de derechos, como el derecho al olvido y la portabilidad de los datos, que les permite tener un control significativo sobre su propia información (Mejía Cambar, 2019).

Además del GDPR, la Carta de los Derechos Fundamentales de la Unión Europea, que tiene rango constitucional, reconoce explícitamente el derecho a la protección de datos personales. Esta constitucionalización de la privacidad refleja la seriedad con la que la Unión Europea aborda este tema y establece un estándar elevado para que otros países y regiones lo sigan. La combinación del

GDPR y la Carta crean un entorno en el que la privacidad no es solo un derecho esperado, sino una norma legalmente vinculante.

Sin embargo, la implementación y el cumplimiento siguen siendo desafíos pues, aunque el GDPR proporciona un marco robusto, depende de la vigilancia tanto de las autoridades nacionales de protección de datos como de la Comisión Europea para garantizar que las empresas cumplan. Además, con la naturaleza dinámica de la tecnología, la Unión Europea debe estar en constante revisión y adaptación de sus regulaciones para abordar las nuevas amenazas y desafíos a la privacidad (Martínez López-Sáez, 2020).

En resumen, la Unión Europea ha dado pasos significativos hacia la constitucionalización de la privacidad en la era digital, estableciendo estándares que muchos ven como ejemplares a nivel mundial. Sin embargo, en un mundo digital en constante evolución, es esencial que la Unión Europea continúe adaptándose y reforzando su compromiso con la protección de los derechos fundamentales de sus ciudadanos. Por lo que, el caso particular de la Unión Europea expone la necesidad de hacerle respectivo control a las compañías desarrolladoras de redes sociales, cómo lo es particularmente Facebook (Grupo Meta), a causa de las vulnerabilidades que se lograron ubicar a priori establecer sanciones para la compañía. Asimismo, la Unión Europea ha sido enfática en promover la protección de los derechos personales, como lo es la privacidad e intimidad, lo cual garantizará un debido equilibrio entre las libertades y el papel del Estado protegiendo estos derechos de terceros.

1.1.2. Caso Estados Unidos

Por otro lado, en Estados Unidos, la concepción y protección de la privacidad en la era digital ha seguido una trayectoria única, reflejando su tradición jurídica y los valores fundamentales en los que se basa su Constitución. Aunque la palabra "privacidad" no aparece explícitamente en la Constitución de Estados Unidos, decisiones de la Corte Suprema han interpretado que ciertas enmiendas, en particular la Cuarta Enmienda, protegen derechos relacionados con la privacidad de los ciudadanos contra injerencias indebidas (Kwon, et al, 2023).

Ahora bien, la Cuarta Enmienda protege a los ciudadanos de búsquedas y confiscaciones irracionales. En el contexto de la era digital, esto ha llevado a debates sobre cómo se aplican estas protecciones a la recolección y el acceso a datos digitales, como correos electrónicos o registros en línea. Aunque existen leyes específicas, como la Electronic Communications Privacy Act (ECPA), que abordan directamente la privacidad digital, la velocidad del avance tecnológico a menudo supera la capacidad del marco legal para adaptarse adecuadamente (De Salve, Mori, Ricci y Di Pietro, 2023).

A nivel estatal, California ha sido líder en la protección de la privacidad digital con la implementación de la California Consumer Privacy Act (CCPA) (Senado del Estado de California, 2018). Esta ley, que algunos comparan con el GDPR de la Unión Europea, otorga a los californianos derechos significativos sobre cómo se recopilan, usan y venden sus datos personales. La existencia del CCPA refleja un movimiento hacia una regulación más estricta de la privacidad digital en Estados Unidos, al menos a nivel estatal.

Sin embargo, a diferencia de la Unión Europea, donde existe un marco regulatorio unificado en toda la región, en Estados Unidos la regulación de la privacidad digital puede variar significativamente de un estado a otro. Esta falta de uniformidad a menudo plantea desafíos tanto

para las empresas, que deben navegar por un mosaico de leyes estatales, como para los ciudadanos, cuyos derechos pueden depender de dónde residen.

Pese a que Estados Unidos ha tomado medidas para proteger la privacidad en el ámbito digital, su enfoque ha sido fragmentado, oscilando entre interpretaciones constitucionales y legislaciones estatales específicas. Mientras que algunos estados avanzan hacia una mayor protección de la privacidad, la nación en su conjunto todavía lucha por encontrar un equilibrio entre la innovación tecnológica y la salvaguarda de los derechos fundamentales en la era digital.

A partir del Caso de la Unión Europea y Estados Unidos en el Estado de California se permite evidenciar un patrón con un propósito y enfoque especifico, que corresponde a salvaguardar la protección de datos personales y protección a la privacidad en el ciberespacio. Por lo que, se llevó a cabo el desarrollo de medidas correctivas para aquellas compañías las cuales vulneran de forma constante aquellas garantías vitalicias al hacer uso de las redes digitales. No obstante, no basta meramente con impulsar medidas correctivas y restrictivas, por el contrario, se requiere buscar una manera armónica en que el Estado pueda intervenir respecto al tratamiento de los datos sin que ello altere la anonimización de estos.

1.1.3. Caso Colombia

Por otra parte, Colombia al igual que muchos países, ha experimentado los desafíos y oportunidades que trae consigo la era digital. Sin embargo, la historia y el contexto legal colombiano han llevado a una evolución particular en la protección de la privacidad en el entorno digital. Aunque la Constitución de 1991 no menciona explícitamente el derecho a la privacidad digital, sí consagra el derecho a la intimidad personal y familiar y a su buen nombre, reconociendo de facto la importancia de la privacidad de los ciudadanos.

A partir de esta base constitucional, Colombia ha adoptado regulaciones específicas para abordar los desafíos de la privacidad en la era digital. La Ley 1581 de 2012 también conocida como la Ley de Protección de Datos Personales, es el principal instrumento que regula la recolección, el tratamiento, y la circulación de datos personales, otorgando a los ciudadanos derechos sobre su información y estableciendo obligaciones para quienes manejan estos datos. Por ende, esta ley, inspirada en parte por modelos europeos, refleja el reconocimiento de Colombia sobre la importancia de proteger los datos personales en el siglo XXI.

Adicionalmente, la Corte Constitucional de Colombia ha jugado un papel activo en la interpretación y protección del derecho a la privacidad en el contexto digital mediante diversas sentencias, como la C – 748 de 2011, en la cual se reforzó la idea de que los derechos fundamentales, incluida la privacidad, deben ser respetados y protegidos, independientemente de los avances tecnológicos. decisiones como esta han proporcionado orientación y han establecido precedentes en casos relacionados con la privacidad y la protección de datos.

No obstante, Colombia enfrenta retos significativos. A pesar de contar con una regulación robusta, la implementación y el cumplimiento son aspectos que requieren constante atención. La rápida evolución de la tecnología y la aparición de nuevas formas de recolectar y procesar datos exigen que tanto el marco legal como las entidades encargadas de su vigilancia estén en constante adaptación y actualización.

Es menester precisar que en el caso de Colombia la privacidad en la era digital no ha sido objeto de controversia, ni tampoco ha escalado política o socialmente como ha ocurrido en el contexto de los Estados que conforman la Unión Europea, o del Estado de California en Estados Unidos. Ello, en parte se debe al desconocimiento social frente a los riesgos de permitir el acceso a información sensible a los terceros. Asimismo, pese a la existencia de las normas en materia de

protección de datos personales e información sensible; Colombia carece de instrumentos institucionales para accionar el aparato judicial y dar fe al debido cumplimiento del ordenamiento jurídico.

Pese a que existen entidades a cargo de dar garantía a los derechos de los consumidores como lo es la Super Intendencia de Industria y Comercio (SIC), que funge como la entidad competente en este caso de velar por la debida protección de la privacidad e información personal recopilada y tratada por terceros, Colombia carece de un margen de acción legal efectivo que permita salvaguardar los derechos fundamentales. A modo de ejemplo, existe el Registro Nacional de Bases de Datos el cual insta a las compañías que operan en Colombia y recopilan información personal a tener dicho registro con el fin de ser vigilados y controlados por la SIC.[1]

En ese sentido, Colombia ha hecho esfuerzos notables para proteger la privacidad de sus ciudadanos en la era digital, apoyándose en su Constitución y desarrollando leyes específicas que aborden el desafío. Pero, si bien ha logrado avances significativos, el país enfrenta el desafío constante de adaptarse a un mundo digital en evolución, garantizando que los derechos fundamentales de sus ciudadanos sean siempre la prioridad.

1.2 El Derecho a la privacidad: caso Facebook

Ahora bien, la revolución digital ha transformado la manera en que nos comunicamos, compartimos y accedemos a la información. Las redes sociales, en particular, han sido protagonistas de esta transformación, siendo Facebook una de las plataformas más influyentes y

[1] Un dato significativo es que no todas las compañías que operan en Colombia o que lo hacen por medio de terceros cuentan con este registro, impidiendo un efectivo control y supervisión respecto a la información que recopilan las compañías sobre sus usuarios, ello, ocurre especialmente con compañías trasnacionales como lo es Facebook.

omnipresentes a nivel global. No obstante, la rápida expansión y penetración de Facebook ha llevado a inquietudes y cuestionamientos sobre cómo esta plataforma maneja y protege la privacidad de sus usuarios (Segado-Boj y Díaz-Campo, 2020).

Siguiendo lo anterior, la red social Facebook en su esencia, facilita la conexión y el intercambio de información entre individuos de todo el mundo. Sin embargo, su modelo de negocio, basado en la monetización de datos de sus usuarios para publicidad dirigida, ha sido objeto de escrutinio y crítica. A lo largo de los años, diversos escándalos relacionados con la filtración, uso indebido y venta no autorizada de datos personales han arrojado dudas sobre el compromiso real de la empresa con la protección de la privacidad (Martorell, do Nascimento, y Garrafa, 2016). Uno de los casos más notorios fue el de Cambridge Analytica, donde se reveló que los datos de millones de usuarios fueron utilizados sin su conocimiento explícito para influir en campañas políticas.

Por otro lado, las regulaciones, como el GDPR en la Unión Europea o la Ley de Protección de Datos Personales en Colombia, han establecido estándares y expectativas sobre cómo deben ser tratados los datos personales (Roncancio Bedoya, Vélez Jaramillo, y Agudelo Taborda, 2022). Aunque Facebook ha adaptado sus políticas y ha realizado cambios en respuesta a estas regulaciones, la naturaleza fundamental de su modelo de negocio sigue generando tensiones inherentes entre la monetización de datos y el derecho a la privacidad.

Por otra parte, la respuesta legal y regulatoria a las prácticas de Facebook refleja una lucha global entre las libertades individuales y las ambiciones corporativas en la era digital (Kumar et al, 2023). A nivel de usuario, esta situación ha llevado a un creciente escepticismo y conciencia sobre la importancia de proteger su información personal (Lemay, Doleck y Bazelais, 2017). Se ha

incentivado la adopción de prácticas y herramientas que promueven una mayor privacidad y el control sobre los datos propios (Estella y Martínez, 2022).

Sin embargo, el caso de Facebook también subraya la necesidad de un marco regulatorio global coherente que aborde los desafíos de la privacidad en la era digital. La protección de la privacidad no debe depender de la jurisdicción o de la benevolencia corporativa, sino ser reconocida y garantizada como un derecho fundamental en todo el mundo (Martorell, do Nascimento y Garrafa, 2016).

Es así como, el caso de Facebook se ha convertido en un referente en el debate sobre la privacidad en la era digital, evidenciando la tensión entre el crecimiento empresarial y los derechos individuales. La solución a este dilema requerirá una combinación de regulación efectiva, innovación tecnológica orientada a la privacidad y una mayor conciencia y empoderamiento de los usuarios (Eadicicco, 2019).

2. El fenómeno de la Minería de Datos y la fuga de información: Caso Facebook.

La minería de datos, un fenómeno omnipresente en la era digital ha generado crecientes preocupaciones en relación con la privacidad de los usuarios. En este contexto, el caso de Facebook se destaca como un ejemplo paradigmático de la intersección entre la minería de datos y la fuga de información personal. Teniendo en cuenta que, la gigantesca red social, hoy conocida como Meta, ha sido objeto de escrutinio debido a sus prácticas de recopilación y utilización de datos de usuarios para fines publicitarios y comerciales (De Salve, Mori, Ricci, & Di Pietro, 2023).

En el centro de la controversia se encuentra el uso de la información personal de los usuarios de Facebook con el objetivo de ofrecer publicidad personalizada. La plataforma ha sido criticada por su capacidad para segmentar a los usuarios de manera precisa, utilizando datos sensibles como

preferencias, comportamientos en línea y ubicaciones. Según autores como (Hernández Peña, 2022), esta práctica ha suscitado preocupaciones sobre la invasión de la privacidad y ha planteado preguntas fundamentales sobre quién controla realmente la información personal en el entorno digital.

El escenario se complica aún más con la problemática de la fuga de información, ilustrada de manera destacada por incidentes como el escándalo de Cambridge Analytica en 2018. En este caso, datos de millones de usuarios de Facebook fueron recopilados sin su consentimiento y utilizados con fines políticos. Este episodio evidenció las vulnerabilidades en las políticas de privacidad y seguridad de la plataforma, así como la necesidad de regulaciones más estrictas para proteger la información personal de los usuarios (Ortutay & The Associated Press, 2023).

A medida que la minería de datos evoluciona, es imperativo abordar no solo la transparencia en la recopilación de datos, sino también la ética en su uso. La necesidad de regulaciones más robustas y de un mayor control por parte de los usuarios sobre sus datos personales se ha convertido en un tema crucial en la agenda global. En ese sentido, interconexión entre la minería de datos y la fuga de información plantea desafíos fundamentales que requieren respuestas tanto a nivel empresarial como gubernamental para salvaguardar la privacidad en el paisaje digital en constante cambio.

2.1. Brechas de seguridad digital

En la era digital, las brechas de seguridad se han convertido en un desafío persistente y preocupante. Estas brechas, a menudo resultado de vulnerabilidades en sistemas informáticos, representan una amenaza directa para la integridad y confidencialidad de la información almacenada en línea. Por lo que, las brechas de seguridad no solo afectan a las grandes

corporaciones, sino que también ponen en riesgo a pequeñas y medianas empresas, así como a usuarios individuales. Los atacantes aprovechan diversas técnicas, como la ingeniería social, el phishing y la explotación de vulnerabilidades en software desactualizado. En ese sentido, autores como (Puris Cáceres, y otros, 2022) instan por el desarrollo de herramientas cibernéticas que permitan no solo entender la sofisticación de estos ataques, sino que por el contrario permite reforzar aquellas debilidades existentes dentro del ciberespacio; lo que permite resaltar la necesidad crítica de medidas proactivas para fortalecer la seguridad digital.

El riesgo de brechas de seguridad se intensifica con la creciente interconexión de dispositivos en el Internet de las cosas (IoT). Según, (Chib, Bentley, & Wardoyo, 2019) a raíz de la proliferación de dispositivos conectados presenta un panorama amplio y complejo que aumenta las superficies de ataque, requiriendo una atención especial para garantizar la seguridad de los datos y la privacidad del usuario, que en este caso nos da a entender que no nos encontramos expuestos meramente desde aquellos espacios digitales que ofrecen las redes sociales, y por el contrario, aquel mundo metafísico se ha trasladado a nuestras realidades, lo que supone entonces mayores probabilidades de estar expuestos a terceros. La gestión adecuada de contraseñas, actualizaciones regulares de software y la conciencia constante sobre las amenazas digitales son elementos esenciales en la defensa contra las brechas de seguridad.

Por tanto, el impacto de las brechas de seguridad va más allá de la pérdida de datos personales; también puede afectar la confianza del público en las plataformas en línea y en la capacidad de las organizaciones para proteger la información sensible. A medida que la tecnología avanza, la ciberseguridad se convierte en un componente esencial de la sociedad moderna, y la colaboración entre sectores público y privado se vuelve fundamental para abordar este desafío y mitigar las brechas de seguridad digital en constante evolución.

Así las cosas, al traer a colación casos particulares en materia de recopilación y tratamiento de datos por parte del Grupo Meta (Anteriormente Facebook), es factible denotar aquellas prácticas poco garantistas debido a la falta de claridad en las políticas de privacidad, junto con la extensa recopilación de datos para fines publicitarios, ha planteado inquietudes sobre la transparencia y la auténtica autonomía del usuario en el control de su información. Autores como (Bibri, Alexandre, Sharifi, & Krogstie, 2023) plantean la necesidad de un equilibrio más ético entre la búsqueda de ingresos a través de la publicidad personalizada y el respeto a la privacidad individual sigue siendo un tema candente en el debate sobre la responsabilidad corporativa en la era digital (Valero, y otros, 2023).

2.2. La venta de información personal a terceros: Un enfoque desde la protección a la privacidad en la era digital

En el contexto de la era digital, la venta de información personal a terceros, como lo evidencia el caso de Facebook, plantea cuestiones cruciales sobre la protección de la privacidad en línea. La gigantesca red social, a lo largo de los años, ha sido objeto de críticas y escrutinio por sus prácticas de recopilación y comercialización de datos de usuarios. Este fenómeno no solo resalta la complejidad de la privacidad en el entorno digital, sino que también subraya la necesidad de enfoques más rigurosos para salvaguardar la información personal de los usuarios.

La preocupación radica en cómo Facebook utiliza los datos personales de sus usuarios para generar ingresos a través de la publicidad personalizada (Dumortier, 2009). Este modelo de negocio ha suscitado preguntas significativas sobre el consentimiento informado de los usuarios y sobre quién tiene realmente el control sobre sus datos. Por ende, la transparencia en la recopilación y uso de datos se convierte en un pilar esencial para abordar las inquietudes de privacidad en la era digital.

A medida que la venta de información personal a terceros se vuelve más prevalente, surge la necesidad urgente de regulaciones más sólidas. En este sentido, el caso de Facebook destaca la importancia de establecer límites claros sobre cómo las plataformas digitales pueden recopilar, compartir y utilizar los datos de los usuarios. Por lo que, la implementación de regulaciones como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea marca un paso significativo hacia la protección de la privacidad en la era digital; máxime teniendo en cuenta las vulnerabilidades en el ciberespacio.

En ese sentido, la ética en el manejo de datos también se convierte en un tema central. La venta de información personal plantea preguntas éticas fundamentales sobre la responsabilidad de las empresas en el uso de los datos de los usuarios (Martínez López-Sáez, 2020). En un entorno digital en constante evolución, donde la tecnología avanza rápidamente, se necesita un equilibrio delicado entre la innovación y la protección de la privacidad para garantizar un tratamiento ético de la información personal en línea.

La participación constante por parte de los usuarios es otro aspecto crucial en la protección de la privacidad digital. La educación sobre la importancia de la privacidad, así como la comprensión de las configuraciones de privacidad disponibles, empoderan a los usuarios para tomar decisiones informadas sobre cómo desean compartir su información en línea. La conciencia y la participación pública son esenciales para impulsar cambios en las prácticas de recopilación de datos y garantizar un mayor respeto por la privacidad en la era digital.

Por ende, el enfoque desde la protección a la privacidad en la era digital debe abordar de manera integral la venta de información personal a terceros. Así es como, el caso de Facebook destaca la urgencia de medidas que equilibren la innovación tecnológica con la protección de los derechos individuales, subrayando así la necesidad de regulaciones claras, ética en el manejo de

datos y la participación de los usuarios en la construcción de un entorno digital más seguro y respetuoso con la privacidad.

2.3. La ética empresarial en el manejo de los datos personales: Un acercamiento a partir de los entornos digitales

La ética empresarial en el manejo de datos personales se ha vuelto fundamental en la era digital, donde la recopilación y uso de información personal son prácticas comunes. Las empresas, especialmente en el ámbito digital, enfrentan la responsabilidad de garantizar que sus prácticas de manejo de datos sean éticas y respetuosas con la privacidad de los individuos. Este enfoque ético no solo fortalece la confianza del usuario, sino que también se ha vuelto esencial en un contexto global donde la privacidad es cada vez más valorada.

En entornos digitales, donde la recopilación masiva de datos es una realidad, las empresas deben ser transparentes acerca de cómo recopilan, almacenan y utilizan la información personal. La transparencia se convierte en un pilar ético crucial para construir la confianza del usuario y garantizar que los individuos estén informados sobre el destino de su información. Así las cosas (Estella & Martínez, 2022), se entiende el papel de las políticas de privacidad, en el sentido que estás seas claras y comprensibles son esenciales para comunicar estas prácticas de manera efectiva.

La protección de datos personales debe ir más allá del cumplimiento de regulaciones y leyes. Las empresas éticas adoptan un enfoque proactivo para salvaguardar la privacidad de los usuarios, implementando medidas de seguridad robustas y asegurándose de que la recopilación de datos se realice de manera justa y legítima. Este enfoque ético implica también la toma de decisiones conscientes en situaciones donde la rentabilidad y la ética pueden entrar en conflicto (Chib, Bentley, & Wardoyo, 2019).

La ética empresarial en el manejo de datos también implica la responsabilidad social corporativa. Las empresas deben considerar el impacto social y ético de sus prácticas, y contribuir positivamente a la comunidad. Según (Mejía Cambar, 2019), esto puede incluir iniciativas para educar a los usuarios sobre la importancia de la privacidad y la seguridad de los datos, así como la participación en la formulación de estándares éticos en la industria.

En ese sentido, la ética empresarial en el manejo de datos personales en entornos digitales es esencial para construir relaciones sólidas con los usuarios y preservar la confianza en la era digital. Las empresas éticas adoptan medidas proactivas para proteger la privacidad de los individuos, promueven la transparencia en sus prácticas y contribuyen de manera positiva a la sociedad. Este enfoque ético no solo es un requisito esencial en el mundo empresarial actual, sino que también es esencial para el desarrollo sostenible y la integridad a largo plazo de las organizaciones.

3. El derecho a la privacidad en el ciberespacio: Un acercamiento a partir del buen gobierno

En la era de la digitalización, el ciberespacio se ha convertido en un vasto dominio donde la información fluye constantemente, transformando la manera en que nos comunicamos, trabajamos y socializamos. A medida que las tecnologías avanzan y penetran más en nuestra vida cotidiana, surgen desafíos inherentes en la protección de la privacidad y la integridad de los datos personales. En este contexto, el concepto de buen gobierno emerge como una herramienta esencial para equilibrar la innovación tecnológica y los derechos fundamentales de los individuos.

El buen gobierno es entendido como la gestión pública transparente, eficaz y orientada hacia el bienestar de la ciudadanía (Roncancio Bedoya, Velez Jaramillo, & Agudelo Taborda, 2022), tiene un papel crucial en el ámbito digital. La protección de la privacidad no es solo una

cuestión de establecer barreras tecnológicas; requiere una estructura legal y reguladora robusta que respalde y garantice estos derechos. Países como Colombia, por ejemplo, han avanzado en la implementación de leyes de protección de datos, y la intervención de sus tribunales ha fortalecido los derechos digitales de los ciudadanos.

No obstante, más allá de las leyes, el buen gobierno implica una actitud proactiva hacia la educación digital, puesto que las autoridades, en colaboración con la sociedad civil y el sector privado, deben promover la alfabetización digital, capacitar a los ciudadanos sobre sus derechos y responsabilidades en línea y fomentar una cultura de privacidad y seguridad en el ciberespacio (Eadicicco, 2019). Las redes sociales, ejemplificadas en plataformas como Facebook, son espacios donde la privacidad se encuentra en constante tensión con la monetización de datos. Un buen gobierno reconoce esta dinámica y trabaja con estas empresas para asegurar prácticas transparentes y justas, al tiempo que protege a los ciudadanos de posibles abusos. El diálogo y la cooperación entre el sector público y privado son esenciales para lograr un equilibrio en el ciberespacio (Jia & Ruan, 2020).

Además, el buen gobierno en el ámbito digital también abarca la implementación de infraestructuras tecnológicas seguras y confiables (Yanliu Lin, 2018). Los gobiernos deben invertir en sistemas y tecnologías que no solo faciliten la interacción digital, sino que también garanticen la protección de datos y la privacidad de los usuarios. En ese sentido, el derecho a la privacidad en el ciberespacio es un desafío multidimensional que requiere una respuesta coherente y holística (Álvarez Goyoaga, 2019). A través del buen gobierno, es posible forjar un ciberespacio donde la innovación y la protección de derechos coexistan en armonía, garantizando un futuro digital más seguro y equitativo para todos.

3.1. Facultad discrecional de Facebook para hacer uso de la información personal de los usuarios

El modelo de negocio de Facebook se basa, en gran medida, en la recopilación y análisis de datos de sus usuarios para dirigir publicidad específica y personalizada. Al aceptar los términos y condiciones cuando una persona se registra en la plataforma, los usuarios otorgan a Facebook cierta discreción para usar su información (Martorell, do Nascimento, & Garrafa, 2016). Sin embargo, la amplitud y opacidad de estas cláusulas han generado inquietudes sobre hasta qué punto la compañía puede llegar en su uso de datos sin violar derechos fundamentales, como el derecho a la privacidad.

> La información que recopilamos y tratamos sobre ti depende de la forma en la que usas nuestros **PRODUCTOS**. Por ejemplo, recopilamos información diferente si vendes muebles en Marketplace o si publicas un reel en Instagram. Recopilamos cierta información sobre ti cuando utilizas nuestros Productos (…) A través de nuestros, puedes enviar mensajes, tomar fotos y grabar videos, comprar o vender artículos y mucho más. Llamamos "actividad" a todo lo que puedes hacer a través de nuestros Productos. Recopilamos tu actividad a través de nuestros Productos y la información que proporcionas. (Grupo Meta Platforms, 2023) (Negrilla fuera de texto)

Esta situación pone en evidencia la falta de contenido explicativa desde las políticas de privacidad y el uso que se le da a la información por parte de la compañía, toda vez que no delimita su capacidad discrecional y por el contrario deja en el aire el entendido de la información utilizada por la compañía para sectorizar a sus usuarios. Diversos escándalos, como el caso de Cambridge

Analytica[2] (Ortutay & The Associated Press, 2023), han puesto en evidencia los riesgos asociados con la facultad discrecional de la plataforma. En situaciones donde la información de los usuarios fue utilizada sin un consentimiento explícito o de maneras no previstas, se evidenció la necesidad de un marco regulador más estricto y transparente que proteja a los usuarios contra el uso indebido de sus datos.

A raíz de estas preocupaciones, Facebook ha realizado cambios en sus políticas y prácticas, buscando ofrecer mayor claridad y control a los usuarios sobre cómo se utilizan sus datos. La plataforma ha implementado herramientas que permiten a los usuarios revisar y ajustar sus preferencias de privacidad, y ha intensificado sus esfuerzos de comunicación para explicar cómo se recopilan y utilizan los datos (Al-Ghuwairi, y otros, 2023).

Sin embargo, la confianza una vez quebrantada es difícil de restaurar. A pesar de los esfuerzos de la compañía, persiste un debate global sobre el alcance de la facultad discrecional de plataformas como Facebook y sobre cómo equilibrar las ventajas de la personalización con el respeto a la privacidad (Valero, y otros, 2023).

En conclusión, la facultad discrecional de Facebook en el uso de la información personal de los usuarios es una cuestión compleja que reside en la intersección de la tecnología, la ética y el derecho. Mientras la plataforma sigue desempeñando un papel fundamental en la vida digital de

[2] El caso de Cambridge Analytica y Facebook, que salió a la luz en 2018, reveló una seria vulneración de la privacidad y generó un amplio escándalo. La consultora política Cambridge Analytica obtuvo ilegalmente datos personales de aproximadamente 87 millones de usuarios de Facebook a través de una aplicación de encuestas. Aunque solo unas decenas de miles de personas utilizaron la aplicación, la aplicación también recopiló información de amigos de los usuarios sin su conocimiento o consentimiento. Asimismo, estos datos fueron utilizados para crear perfiles psicográficos y personalizar mensajes políticos durante las campañas electorales, incluida la elección presidencial de Estados Unidos en 2016. La revelación de esta práctica desencadenó una cascada de críticas hacia Facebook, planteando preocupaciones sobre la gestión de la privacidad y la seguridad de los datos de sus usuarios. Este incidente subrayó la necesidad de una mayor supervisión y regulación en el manejo de datos personales por parte de las plataformas digitales.

muchas personas, es imperativo que continúe evolucionando y adaptándose a las demandas y expectativas cambiantes de sus usuarios en relación con la privacidad y la seguridad de los datos.

3.2. El derecho blando en la consolidación de tratados multilaterales en pro de la privacidad

En el complejo panorama internacional, según el autor Goyoaga (2019) el derecho blando (o "soft law" en inglés) ha emergido como una herramienta valiosa para facilitar la cooperación entre Estados en temas de interés común, incluida la protección de la privacidad (López-Lemus, Carranza, Schmitt-Revilla, & López-Lemus, 2024). A diferencia del derecho duro, que se refiere a normas vinculantes como tratados y convenios, el derecho blando abarca instrumentos no vinculantes como declaraciones, principios y directrices. Aunque no son legalmente obligatorios, estos instrumentos desempeñan un papel crucial en la formulación y consolidación de normas y prácticas internacionales.

La privacidad, en el contexto de un mundo cada vez más digitalizado y globalizado, es un desafío transfronterizo. La naturaleza interconectada de la tecnología significa que las acciones en un país pueden tener repercusiones en otro. En este escenario, los instrumentos de derecho blando se convierten en medios efectivos para establecer estándares y prácticas comunes, permitiendo a los países colaborar sin necesariamente comprometerse a obligaciones legales fijas (Medan, 2020).

Los tratados multilaterales vinculantes en materia de privacidad son desafiantes debido a las diferencias en las culturas jurídicas, valores y prioridades nacionales. El derecho blando permite una aproximación más flexible y adaptativa, facilitando el consenso y promoviendo la adopción voluntaria de buenas prácticas. Por ejemplo, las directrices y principios establecidos en foros internacionales pueden influir en la legislación nacional y en la conducta de actores estatales y no estatales, estableciendo de facto estándares que se adhieren y respetan (Ali, 2023).

Además, el derecho blando puede servir como precursor para tratados vinculantes. Una vez que se haya establecido un consenso a través de instrumentos no vinculantes, los países pueden sentirse más cómodos y preparados para entrar en acuerdos formales, convirtiendo estas normas suaves en compromisos legales duros. Es un proceso gradual que refuerza la cooperación y la confianza entre los Estados.

En conclusión, el derecho blando juega un papel vital en la consolidación de tratados multilaterales en pro de la privacidad. Aunque no tiene la fuerza vinculante del derecho duro, su flexibilidad y capacidad para fomentar el consenso lo convierten en un medio esencial para abordar desafíos globales en el ámbito de la privacidad y más allá.

3.3 Retos y desafíos en materia de privacidad en el ciberespacio

En la era digital contemporánea, el ciberespacio se ha convertido en una extensión vital de nuestras vidas, pero con su expansión han surgido desafíos inéditos en relación con la privacidad. Uno de los principales retos es la naturaleza transfronteriza del ciberespacio. La información fluye libremente, sin respetar las fronteras nacionales, lo que dificulta la implementación y cumplimiento de normativas de privacidad que varían de un país a otro. Además, las jurisdicciones a menudo chocan cuando se trata de definir y sancionar violaciones a la privacidad en línea (Bibri, Alexandre, Sharifi, & Krogstie, 2023).

En consecuencia, la evolución tecnológica constante presenta otro desafío significativo. Según los autores (Bibri, Alexandre, Sharifi, & Krogstie, 2023) Con la proliferación de dispositivos conectados (IoT), la inteligencia artificial y las tecnologías de análisis de grandes datos, la cantidad y variedad de información personal recopilada y procesada es asombrosa. Esto plantea preocupaciones sobre el consentimiento, la transparencia en la recolección y uso de datos, y la

seguridad de estos datos contra posibles brechas y mal uso. Las organizaciones y plataformas, grandes y pequeñas, enfrentan la presión de proteger la información de los usuarios mientras innovan y evolucionan.

Paralelamente, el ciberespacio es también escenario de una creciente sofisticación en amenazas cibernéticas. Actores malintencionados, ya sean individuos, grupos o incluso naciones, emplean tácticas avanzadas para acceder ilegalmente a datos sensibles (Pons Gamón, 2017), lo que intensifica la necesidad de infraestructuras de seguridad robustas y actualizadas. Esta situación se agrava con la falta de conciencia o educación digital en amplios segmentos de la población, quienes pueden no estar plenamente informados sobre cómo proteger su privacidad en línea (Figueroa, 2023). Es así como, la privacidad en el ciberespacio enfrenta una serie de retos multidimensionales que demandan respuestas colaborativas y adaptativas. Es esencial que gobiernos, industria y sociedad civil trabajen conjuntamente para desarrollar soluciones que protejan los derechos individuales, mientras se mantenga el dinamismo y potencial del mundo digital.

Conclusiones

La privacidad es un derecho fundamental que ha cobrado especial relevancia en la era digital. Las redes sociales, encabezadas por plataformas como Facebook, han transformado nuestra manera de comunicarnos, pero también han elevado las preocupaciones sobre la privacidad de los datos y la seguridad de la información.

En ese sentido, el análisis a partir de las redes sociales nos muestra que la constitucionalización del derecho a la privacidad es esencial para proteger a los ciudadanos en la era digital. La Unión Europea, con su Reglamento General de Protección de Datos (GDPR), ha establecido un estándar que otorga a los ciudadanos control sobre sus datos. En contraste, Estados

Unidos, con su enfoque orientado al mercado, carece de una legislación federal unificada, lo que lleva a desafíos en la coherencia y aplicación de políticas. Colombia, por su parte, ha realizado esfuerzos para alinear su normativa con estándares internacionales, buscando un equilibrio entre la protección de datos y el fomento de la innovación (Red Iberoamericana de Protección de Datos, 2017).

En el caso de Facebook, la plataforma ha sido centro de debate por su manejo de datos personales. A pesar de las herramientas de privacidad ofrecidas, persisten preocupaciones sobre la transparencia y el consentimiento en la utilización de datos para fines publicitarios. Que posteriormente permiten analizar el contexto colombiano desde las redes sociales, y bajo el caso particular de Facebook, este juega un papel fundamental, conectando a millones de persones y sirviendo como plataforma de interacción social y económica. Sin embargo, la legislación sobre redes sociales en Colombia todavía enfrenta desafíos en cuanto a su aplicación y claridad. Permitiendo denotar que, es esencial fortalecer el marco legal y social incorporando principios de transparencia, responsabilidad y respeto por la privacidad, al tiempo que se promueve la educación y conciencia digital entre los usuarios.

Es por ello necesario que se construyan políticas públicas focalizadas en pro del buen gobierno, el cual desde la doctrina se ha desarrollado y diferentes Estados se han encargado de regularlo, siendo este clave para garantizar el debido funcionamiento del Estado, que en este caso particular tendría que velar por salvaguardar el derecho la privacidad en el ciberespacio. Las plataformas, como Facebook, deben ejercer su facultad discrecional de manera responsable, siendo transparentes en el uso de la información personal y ofreciendo a los usuarios opciones claras sobre la gestión de sus datos.

Asimismo, la discusión no debe plantearse meramente desde la perspectiva del ordenamiento jurídico interno; por el contrario se debe extender y llevar a un campo más amplio, desde el cual se aborde el contexto legal internacional, pero sobre todo desde la perspectiva social, donde claramente a causa de las redes sociales se pueden dar grandes afectaciones a las personas; ello, teniendo en cuenta que el "derecho blando", a través de directrices y principios no vinculantes, puede ser una solución viable para establecer estándares comunes en la protección de datos. Estos instrumentos, aunque no obligatorios, pueden guiar a los países en la adopción de mejores prácticas y servir como base para tratados multilaterales vinculantes en el futuro.

Permitiendo concluir la necesidad de intervención de diferentes actores entre los cuales sin duda se encuentran los Estados, así como la sociedad civil, y se tenga la capacidad de dar garantía a los usuarios respecto al uso de su información por parte de compañías tecnológicas, como lo es el caso de Facebook que, a causa de la constante evolución tecnológica, las amenazas cibernéticas y la globalización exigen soluciones colaborativas y adaptativas. Existe la necesidad latente de desarrollar y reforzar medios adecuados y expeditos para la debida protección de la privacidad en la era digital, que actualmente es un imperativo que requiere esfuerzos conjuntos a nivel local, nacional e internacional. Solo a través de la cooperación, la innovación y la educación podremos navegar con éxito por el ciberespacio, garantizando un futuro digital seguro y beneficioso para todos.

Referencias

Akbari, Y., Al Maadeed, S., Elharrouss, O., Ottakath, N., & Khelifi, F. (2024). Hierarchical deep learning approach using fusion layer for Source Camera Model Identification based on video taken by smartphone[Formula presented]. *Expert Systems with Applications, 238*, 1-10. doi:https://doi-org.iue.basesdedatosezproxy.com/10.1016/j.eswa.2023.121603

Al-Ghuwairi, A. R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A., & Algarni, A. (2023). Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. *Journal of Cloud Computing, 12*(127). doi:https://doi.org/10.1186/s13677-023-00491-x

Ali, S. (2023). Information We Can Extract about a User from 'One Minute Mobile Application Usage'. *IEEE INFOCOM 2023 - Conference on Computer Communications Workshops, INFOCOM WKSHPS 2023*. doi:10.1109/INFOCOMWKSHPS57453.2023.10225869

Álvarez Goyoaga, G. (2019). Incidencia actual del derecho "blando" en el Derecho Internacional. *Revista Diplomática - 2ª Época, 1*(2), 1- 189. Retrieved from https://acortar.link/0KK72x

Barbosa Chacón, J. W., Barbosa Herrera , J. C., & Rodríguez Villabona, M. (2013). Revisión y análisis documental para estado del arte: una propuesta metodológica desde el contexto de la sistematización de experiencias educativas. *Investigación bibliotecológica, 27*(61), 83-105. Retrieved from https://www.scielo.org.mx/scielo.php?pid=S0187-358X2013000300005&script=sci_abstract&tlng=pt

Beade, G. (2022). Endangerment crimes and constitutional proportionality: a reconstruction of criminal responsibility under the basic guidelines of the principle of proportionality. *Ius et Praxis, 28*(3), 191- 201. doi:10.4067/S0718-00122022000300191

Bibri, S., Alexandre, A., Sharifi, A., & Krogstie, J. (2023). Environmentally sustainable smart cities and their converging AI, IoT, and big data technologies and solutions: an integrated approach to an extensive literature review. *Energy Informatics, 6*(1), 1- 39. doi:10.1186/s42162-023-00259-2

Chib, A., Bentley, C., & Wardoyo, R.-J. (2019). Distributed digital contexts and learning: Personal empowerment and social transformation in marginalized populations. *Grupo Comunicar Ediciones, 27*(58), 51- 60. doi:10.3916/C58-2019-05

Congreso de Diputados de España. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* Madrid: Boletín Oficial del Estado. BOE número 294, de 6 de diciembre de 2018, ~~páginas 119788 a 119857~~ (~~70 págs.~~). Retrieved from https://www.boe.es/eli/es/lo/2018/12/05/3

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan

integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. 5 de enero de 2009. Diario Oficial No. 47.223. http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ley 1480 de 2011. Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. 12 de octubre de 2011. Diario Oficial No. 48.220. http://secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales**.** Diario Oficial No. 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Consejo Nacional de Política económica y social. (2019). *Documento CONPES 3975. Política para la Transformación Digital e Inteligencia Artificial.* Bogotá D.C: Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3975.pdf

Corte Constitucional de Colombia. (2011). Proceso C - 748/11. M. P. Jorge Ignacio Pretelt Chaljub; 6 de octubre de 2011. from https://www.corteconstitucional.gov.co/relatoria/2011/C-748-11.HTM

De Salve, A., Mori, P., Ricci, L., & Di Pietro, R. (2023). Content privacy enforcement models in decentralized online social networks: State of play, solutions, limitations, and future directions. *Computer Communications, 203*, 199-225. doi:https://doi.org/10.1016/j.comcom.2023.02.023

Dumortier, F. (2009). Facebook y los riesgos de la «descontextualización» de la información. *IDP. Revista de Internet, Derecho y Política*(9), 25- 41. ~~Retrieved from~~ http://www.redalyc.org/articulo.oa?id=78813254009

Eadicicco, L. (2019, agosto 8). *A new lawsuit accuses Apple of violating user's privacy by allegedly allowing Siri to record without consent*. ~~Retrieved from INSIDER:~~ https://acortar.link/RTGa93

Estella, F., & Martínez, A. (2022). Derecho a la Competencia vs Privacidad: ¿El Gran Dilema en los Nuevos Mercados Digitales? *Revista Cuadernos de Derecho Transnacional*, *14*(1), 169-195. doi: https://doi.org/10.20318/cdt.2022.6682

Figueroa G., R. (2013). El derecho a la privacidad en la jurisdicción de protección. *Revista Chilena de Derecho, 40*(3), 859- 889. doi: http://dx.doi.org/10.4067/S0718-34372013000300005.

Figueroa, A. (2023). Legitimacy of self-defense of police officers. The “Juggler of Panguipulli” case. *Ius et Praxis, 29*(1), 276- 288. doi: http://dx.doi.org/10.4067/S0718-00122023000100276

Hernández Peña, J. C. (2022). Campañas Electorales, Big Data y perfilado ideológico. Aproximación a su problemática desde el Derecho Fundamental a la Protección de Datos. *Revista Espanola de Derecho Constitucional, 2022*(124), 41- 73. doi: http://doi.org/10.18042/cepc/redc.124.02

Grupo Meta Platforms. (2023 de junio de 2023). Política de privacidad ¿Qué es la política de privacidad y qué cubre? https://acortar.link/vFTtIF

Ho, F., Ho-Dac, N., & Huang, J. , S. (2023). The Effects of Privacy and Data Breaches on Consumers’ Online Self-Disclosure, Protection Behavior, and Message Valence. *SAGE Open, 13*(3). doi: https://doi.org/10.1177/21582440231181395

Jia, L., & Ruan, L. (2020). Going Global: Comparing Chinese Mobile applications´ data and user privacy governance at home and abroad. *Internet Policy Review, 9*(3), 1- 22. doi: https://doi.org/10.14763/2020.3.1502

Kumar, V., Preeti, Saheb, S., Kumari, S., Pathak, K., Chandel, J., . . . Kumar, A. (2023). A PLS-SEM Based Approach: Analyzing Generation Z Purchase Intention Through Facebook's Big Data. *Big Data Mining and Analytics, 6*(4), 491-503. doi: https://doi.org/10.26599/BDMA.2022.9020033

Kwon, T., Song, J., Jung, H., Chun, S., Lee, H., Kang, M., . . . Cho, E. (2023). How to decentralize the internet: A focus on data consolidation and user privacy. *Computer Networks, 234*, 1-17. doi: https://acortar.link/JhNXXb

Lemay, D., Doleck, T., & Bazelais, P. (2017). “Passion and concern for privacy” as factors affecting snapchat use: A situated perspective on technology acceptance. *Computers in Human Behavior, 75*, 264- 271. doi:https://doi.org/10.1016/j.chb.2017.05.022

López-Lemus, J. A., Carranza, M., Schmitt-Revilla, M., & López-Lemus, J. (2024). The Role of Social Media and Innovation in Mexican Industrial Entrepreneurship. *Innovar, 34*(92), 1-23. doi:https://doi.org/10.15446/innovar.v34n92.98533

Martínez López-Sáez, M. (2020). La garantía del derecho al olvido: protección de datos, retos futuros y propuestas de regulación de situaciones de vulnerabilidad en la Unión Europea. *(Tesis Doctoral, Universidad de Valencia.)* 1- 812. https://hdl.handle.net/10550/75363

Martorell, L., do Nascimento, W., & Garrafa, V. (2016). Social networks, privacy, confidentiality and ethics: Exhibition of pictures of patients on Facebook. *Interface: Communication, Health, Education, 20*(56), 13- 23. doi: https://doi.org/10.1590/1807-57622014.0902

Medan, S. (2020). Violación del derecho a la privacidad electrónica en el derecho internacional público. *Revista Opcion, 36*(27), 663- 683.

Mejía Cambar, O. (2019). Análisis al reglamento General de Protección de Datos en la Unión Europea: Un Vistazo a la Actualidad de la Era Digital. *La Revista de Derecho, 40*(1), 93- 104. doi:https://doi.org/10.5377/lrd.v40i1.8909

MercoPress.South Atlantic News Agency. (2023, mayo 24). *Multa récord de Unión Europea a Meta por desconocer norma de protección de datos europeos*. Retrieved from Multa récord de Unión Europea a Meta por desconocer norma de protección de datos europeos: https://acortar.link/trCBSH

B., & The Associated Press. (2023, julio 26). *Facebook users have just a month left to apply for part of a $725 million privacy settlement over Cambridge Analytica*. https://fortune.com/2023/07/26/facebook-privacy-settlement-appliy/

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (Unión Europea) 2016/679.* Bruselas: Diario Oficial de la Unión Europea. Retrieved from https://www.boe.es/doue/2016/119/L00001-00088.pdf

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito,ciberterrorismo,legislación y ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, 80- 93. doi:https://doi.org/10.17141/urvio.20.2017.2563

Presidencia de la República de Colombia. (2013). Decreto Reglamentario 1377. *Diario Oficial. ~~Año CXLIX. N. 48834.~~*, ~~1- 10. Retrieved from~~ https://acortar.link/7rg6J9

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

Puris Cáceres, A. Y., Florencia Toala, A., Hernández Palacios, R., Zhuma Mera, E., Torres Quijije, Á., & Oviedo Bayas, B. (2022). Estudio de Técnicas de Minería de datos para la detección de ataques en el conjunto de datos NSL-KDD. *Universidad y Sociedad, 14*(1), 428- 437. https://rus.ucf.edu.cu/index.php/rus/article/view/2645

Ramírez-García, H. (2022). La constitucionalización de la persona: un marco de la relación entre el Estado de derecho y los derechos humanos. *Revista Cuestiones Constitucionales, 47*, 367- 395. doi: https://doi.org/10.22201/iij.24484881e.2022.47.17533

Red Iberoamericana de Protección de Datos. (2006). Autorregulación y Protección de Datos Personales. *Documento Elaborado por el Grupo de Trabajo reunido en Santa Cruz de la Sierra – Bolivia. Los días 3 a 5 de mayo*.

Red Iberoamericana de Protección de Datos. (2017). Estándares de Protección de Datos Personales para los Estados Iberoamericanos. *XV Encuentro Iberoamericano de Protección de Datos*, 1- 34. https://www.redipd.org/es/documentos/estandares-iberoamericanos

Roncancio Bedoya, A. F., Velez Jaramillo, E. A., & Agudelo Taborda, S. (2022). Dinámicas sobre el Buen Gobierno alrededor de la Regulación del Acceso a las TICS en Colombia: El Internet como Mediador de Derechos Sociales. *Verba Iuris*, 107- 117. doi:https://doi.org/10.18041/0121-0021/verbaiuris.47.2022.XXXX

Rumaldo-Calderón, C., Tupayachi-Torres, Y., & Lodeiros-Zubiria, M. L. (2024). Netflix: Comparison of the Impact of Social Media Content on Social Media Engagement Behaviour Between Followers of the Series and the Platform. *Smart Innovation, Systems and Technologies, 344*, 241-255. doi: https://doi.org/10.1007/978-981-99-0333-7_19

Segado-Boj, F., & Díaz-Campo, J. (2020). Social media and its intersections with free speech, freedom of information and privacy. An analysis. *Scientific Association Icono14, 18*(1), 231- 255. doi: https://doi.org/10.7195/ri14.v18i1.1379

Senado del Estado de California. (2018). Title 1.81.26. Security of Connected Devices. *Califronia Privacy Protection Agency*, 01 - 66. https://acortar.link/GLsI38

Suárez-Manrique, W. Y. (2014). La constitucionalización del derecho en el ordenamiento jurídico colombiano. *Vniversitas, 63*(129), 319 - 354. doi:https://doi.org/10.11144/Javeriana.VJ129.cdoj

Tapia Hermida, A. J. (2021). La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento. *Revista Ibero-Latinoamericana De Seguros, 30*(54), 107-146. doi:https://doi.org/10.11144/Javeriana.ris54.rcdu

Tavares, A., & Bitencourt, C. (2021). Diálogo entre o Direito e a Engenharia de Software para um novo paradigma de transparência: controle social digital. *Revista Eurolatinoamericana de Derecho Administrativo, 8*(1), 9- 34. doi:https://doi.org/10.14409/redoeda.v8i1.9676

Toscano, M. (2017). Sobre el concepto de privacidad: la relación entre privacidad e intimidad. *Revista Isegoria*(57), 533-552. doi: https://doi.org/10.3989/isegoria.2017.057.06

Valero, C., Pérez, J., Solera Cotanilla, S., Vega Barbas, M., Suarez Tangil, G., Alvarez Campana, M., & López, G. (2023). Analysis of security and data control in smart personal assistants from the user's perspective. *Future Generation Computer Systems, 144*, 12-23. doi: https://acortar.link/4hkPUr

Yanliu Lin. (2018). A comparison of selected Western and Chinese smart governance: The application of ICT in governmental management, participation and collaboration. *Telecommunications Policy*, *42*(10), 800- 809. doi:https://doi.org/10.1016/j.telpol.2018.07.003