RELIGACIÓN
REVISTA

La frontera entre privacidad y evasión de responsabilidad: anonimato en internet y desafíos jurídicos

The boundary between privacy and liability avoidance: Internet anonymity and legal challenges

Kenlly Stefanía Molina Párraga, Steven Orley Mendoza Moreira, Javier Andrés Espinoza Suárez

Resumen

El derecho al anonimato es la capacidad de las personas para que su actuación o expresión sea realizada sin la revelación de su identidad. Este derecho se manifiesta en mayor medida en el entorno digital, porque los individuos participan en diferentes actividades en línea. Es un elemental derecho que permite expresar su opinión. también tiene una línea divisoria que debe ser respetada, ser responsable de lo escrito o expresado. El objetivo planteado fue determinar la frontera entre privacidad y evasión de responsabilidad relacionado con el anonimato en internet y desafíos jurídicos. El enfoque metodológico fue cualitativo; mientras el método bibliográfico permitió la revisión de información en repositorios virtuales nacionales e internacionales, de investigaciones asociadas con las variables objeto de estudio; la información se procesó a través del método analítico, realizando un análisis de la información acopiada. Los resultados permitieron profundizar en torno al anonimato enfocado en un contexto holístico, agrupando a la privacidad y la necesidad de responsabilidad legal por las opiniones emitidas. Se concluyó que el anonimato también es utilizado para expresar ideas en contra de personas u organizaciones, y ante aquello los marcos jurídicos permitan seguir acciones legales en contra de quienes las escriben.

Palabras clave: Derecho; privacidad; protección; anonimato; privacidad.

Kenlly Stefanía Molina Párraga
Universidad Laica Eloy Alfaro de Manabí | Manta | Ecuador | e1313632109@live.uleam.edu.ec
https://orcid.org/0009-0002-6219-4720
Steven Orley Mendoza Moreira
Universidad Laica Eloy Alfaro de Manabí | Manta | Ecuador | e1350075832@live.uleam.edu.ec
http://orcid.org/0009-0008-4190-4926
Javier Andrés Espinoza Suárez
Universidad Laica Eloy Alfaro de Manabí | Manta | Ecuador | Javier.espinoza@uleam.edu.ec
https://orcid.org/0009-0000-8126-4400

http://doi.org/10.46652/rgn.v10i47.1496
ISSN 2477-9083
Vol. 10 No. 47 octubre-diciembre, 2025, e2501496
Quito, Ecuador

Enviado: abril 01, 2025
Aceptado: julio 03, 2025
Publicado: agosto 26, 2025
Publicación Continua

CC BY NC ND

RELIGACIÓN CICSHAL
Centro de Investigaciones en Ciencias Sociales y Humanidades desde América Latina

Abstract

The right to anonymity is the ability of individuals to act or express their opinions without revealing their identity. This right is most evident in the digital environment, as individuals engage in various online activities. This basic right to participate and express their opinions also has a dividing line that must be respected, and individuals must be responsible for what they write or express. The objective was to determine the boundary between privacy and evasion of responsibility related to online anonymity and legal challenges. The methodological approach was qualitative; the bibliographic method allowed for the review of information in national and international virtual repositories, including research associated with the variables under study. The information was processed through an analytical method, performing an analysis of the collected information. The results allowed for a deeper understanding of anonymity, focused on a holistic context, encompassing privacy and the need for legal accountability for opinions expressed. It was concluded that anonymity is also used to express ideas against individuals or organizations, and that legal frameworks allow for legal action against those who write them.

Keywords: Law; Privacy; protection; anonymity; privacy.

Introducción

El surgimiento de la internet revolucionó el mundo, no solo cambió la forma en la que se llega a comunicar, también lo hizo con la privacidad y la determinación de responsabilidad. La facilidad de ocultar datos de identificación en completa libertad, permite que naveguen sin ningún contratiempo, sin embargo, esta práctica genera complicaciones cuando se trata de aplicar la norma frente a conductas ilícitas. El internet permite divulgar la información a gran cantidad de internautas, sin restricciones geográficas, pero, ese desarrollo, beneficioso en sus inicios, ha generado la proliferación de conductas inadecuadas.

Lo que en su momento fueron manifestaciones físicas, en la actualidad se ha convertido en actuaciones digitales presentes en foros, blogs o redes sociales sin restricción alguna, en muchos casos, realizados bajo el amparo del anonimato. Cabe indicar que la privacidad, en términos de pronunciamientos o emitir comentarios, también presenta límites. Al realizarse de manera irresponsable, se convierte en abuso, ante lo cual la ley tiene que hacer respetar el derecho de quienes han sido atacados en la web. Bajo esta premisa un elemento presente cada vez en la internet, es el anonimato, de acuerdo con Marx et al. (2018), el anonimato en línea consiste en el ocultamiento de la identidad personal al momento de ejercer una comunicación mediante las diferentes herramientas digitales que puedan servir como medio de identificación.

Consecuentemente, dentro de una creciente digitalización, la privacidad y protección de datos se vuelven elementos garantistas de los derechos de los usuarios en internet. Pese a esto, son justamente estas herramientas que, aprovechando el anonimato, es utilizada como un medio para evadir responsabilidades legales cuando cometen infracciones. La posibilidad de realizar interacciones anónimas en internet, crea como desafío la aplicación efectiva de las leyes frente a los actos ilegales que pueden ser cometidas en línea. Por cuanto, la privacidad, así como el anonimato, se convierten en mecanismos de defensa de los usuarios, frente al cometimiento de abusos para evitar repercusiones legales.

Dentro de los antecedentes se indica que, en el ordenamiento jurídico ecuatoriano no existe como tal un derecho así llamado, pese a lo cual, en el Ecuador se encuentran consagrados en la Constitución derechos consagrados en el artículo 66 numeral 6, 7 y 20 que protegen el derecho a opinar, a la rectificación, réplica o respuesta y el derecho a la intimidad respectivamente.

El anonimato en internet ha evolucionado siguiendo la línea de la evolución social, primero se solía manifestar a través de comentarios en blogs o foros, sin embargo, con el avance tecnológico y con la nueva aparición de redes sociales como *Facebook*, *Instagram, Reddit, Twitter* -actual X- o entre las más recientes *Tik Tok*, han requerido que los usuarios se identifiquen a fin de proveer de una mayor "seguridad y confianza" a los demás usuarios. Sin embargo, a pesar de requerir una identificación para poder usarlas esto ha dado origen a la creación de perfiles falsos denominados.

Véliz (2019), establece que, la palabra anonimato deriva del griego "nombra falso", e implica la identificación de un autor mediante una etiqueta que no corresponde a su nombre real de tal forma que no permite que otros vinculen el seudónimo del autor con su nombre real o identidad (p. 651), definiéndolo el autor al seudónimo como un subtipo de anonimato, porque puede bloquear el vínculo entre la autoría y la identidad, guardando estrecha relación.

Incluso Westin (1967, pp. 39-40, citado por Eklund et al., 2022), pionero en el estudio del Derecho a la privacidad, sostiene que el anonimato, surge cuando alguien, a pesar de estar en un lugar público, logra evadir la identificación y el seguimiento; por lo tanto, nos referiremos indistintamente del anonimato tanto del seudónimo ya que ambos no permiten lograr la identificación del autor, en palabras de Hanover "ser anónimo suele referirse a formas de seudónimos o a ser irreconocible" (2021, p. 14).

Según Moore (2018, como se citó en Ossa, 2024), se distinguen tres dimensiones del anonimato en línea:

1. La primera de ellas es la "trazabilidad", que se refiere a la posibilidad de rastrear las contribuciones hasta la identidad o usuario de origen mediante etiquetas de identificación. En este sentido, el anonimato no existe como tal, ya que todo elemente debe ser identificable, a menos que dichas etiquetas sean eliminadas o no se generen, convirtiéndose la trazabilidad en una herramienta que permite rastrear publicaciones o interacciones en distintos portales web a partir de patrones de conducta que una persona desarrolla en un tiempo.

2. La segunda dimensión es la "durabilidad", que depende de la facilidad o dificultad para adquirir y cambiar identidades en el entorno digital, es decir, se relaciona con el esfuerzo de evitar la detección.

3. Por último, el autor menciona la "conectividad", misma que funge como un vínculo entre diferentes plataformas y contextos, influyendo directamente en la reputación y personalidad del usuario, esta última dimensión debe de ser considerada a nivel global, ya que, con un simple clic, es posible interactuar desde cualquier parte del mundo.

El derecho a la privacidad y la protección de datos personales

Un elemento clave dentro de la internet e imprescindible como mecanismo de defensa de los usuarios es la privacidad, establecida en la Declaración Universal de los Derechos Humanos de 1948 en su artículo 12, instaura el derecho a las personas a no ser objeto de injerencias arbitrarias en su vida privada ni ataques a su honra, teniendo el derecho de protección ante dichos ataques, las Naciones Unidas (2018), establece que la privacidad es "esencial para el desarrollo de la personalidad y la protección de la dignidad humana".

Kubli (2017), define el derecho a la privacidad como aquellas disposiciones procedentes dentro de un ordenamiento jurídico tanto nacional como internacional que se refieren a la privacidad de las personas en tres dimensiones. Esto es, aquellos "derechos relacionados con la injerencia mínima del poder público en las relaciones particulares, la protección de los datos personales y el libre desarrollo de la personalidad" (p. 27). Por su parte, Vargas define el derecho a la privacidad como "toda la información y los hechos que el titular del derecho desea excluir de la publicidad" (2023, p. 8).

Pero en sí, ¿qué son los datos personales?, los datos personales (Comisión Europea, s.f.), "son cualquier información relativa a una persona física, viva, identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona también constituyen datos de carácter personal" así mismo nos establece una lista ejemplificativa donde se establecen ejemplos de datos personales los cuales no está de más recalcar, y es que, entre los datos que son caracterizados como datos personales encontramos a los nombres completos, dirección domiciliaria, dirección electrónica, el número de identificación ciudadana, los datos de localización, direcciones IP y demás.

La protección de datos en Ecuador se regula mediante la ley Orgánica de Protección de Datos Personales, esta tiene como objetivo salvaguardar el derecho fundamental a la protección de datos personales, otorgando a los individuos el control sobre su información y estableciendo un marco normativo que garantice el cumplimiento, por lo tanto, dentro de sus textos, regula los principios, derechos y obligaciones aplicables, así como los mecanismos de tutela necesarios para su protección.

La promulgación de la ley de protección de datos en Ecuador en el año 2021, nace de una necesidad por la creciente expansión de las diferentes herramientas digitales de uso tanto privado como público para el manejo de datos personales, Alonso (2021), menciona que se debe "destacar la clara influencia de la ya existente normativa europea, así como un inequívoco espíritu garantista respecto a los titulares" esta normativa se caracteriza por tener hoy en día un alcance territorial, es decir también serán regidos por esta normativa los datos personales de personas que residen en el país cumpliendo ciertos parámetros.

Cabe recalcar que la normativa está cargada y respaldada con principios fundamentales de carácter constitucional que siempre están activos, en este caso uno de los principales es el principio

de responsabilidad proactiva y demostrada, Alonso (2021), comparte que este principio será el eje central de la normativa, el cual no sólo tiene que ser una actitud diligente al momento de cumplir con lo establecido por parte de las organizaciones, debe de estar también siempre a disposición de la implementación de mecanismos efectivos para proteger los datos personales encomendados.

En muchas ocasiones la privacidad suele confundirse con la intimidad, pese a esto, Villalba (2017), concibe a la intimidad como un derecho que "protege la esfera más privada del individuo" (p. 27), y señala que sus elementos pueden o no ser compartidos mediante la autorización del titular. Por su parte, Bidart y Carnota (1998), establecen que "la intimidad es la esfera personal que está exenta del conocimiento generalizado de terceros" mientras que la privacidad "es la posibilidad irrestricta de realizar acciones privadas (que no dañen a otros) que se cumplan a la vista de los demás y que sean conocidas por éstos" (p. 32).

En el presente artículo científico se busca determinar la frontera entre privacidad y evasión de responsabilidad relacionado con el anonimato en internet y desafíos jurídicos, ante lo cual se busca encontrar el límite normativo, así como llegar a identificar los mecanismos legales disponibles para sancionar actos ilícitos (cibercrímenes), también frenar el abuso de los comentarios agresivos en contra del honor y el buen nombre (artículo 66 numeral 18 de la Constitución de la República del Ecuador). Tofo esto en el contexto del análisis a los límites jurídicos del anonimato. En base a todo lo citado, se plantea la siguiente interrogante: ¿Cuáles son los desafíos jurídicos que limitan la evasión de responsabilidad ante el anonimato en internet?

Materiales y métodos

Para Cueva et al. (2023), la investigación científica es un proceso riguroso y estructurado cuya finalidad radica en la creación de nuevos conocimientos verificables y confiables. Para ello es necesario, en el presente documento la presente investigación de tipo cualitativa, por cuanto se procedió al análisis de las variables que conforman el problema. A través del método bibliográfico se pudo revisar documentos de autores que desarrollaron trabajos similares al aquí expuesto, mismos que constan en repositorios virtuales nacionales e internacionales.

Los criterios de inclusión estuvieron dados por artículos científicos, así como en otros formatos digitales. Los criterios de exclusión estuvieron enfocados en no incluir textos que limiten el análisis relacionado con anonimato en internet. Las bases de datos consultadas pertenecen a diversas revistas, como es el caso de Foros, Social & Legal Studios, en el Instituto Español de Estudios Estratégicos, Revista Chilena de Derecho y Tecnología, entre otros.

Se integró la información luego de haber seleccionado una serie de documentos electrónicos, 50 en total, quedando en 30 las referencias bibliográficas incorporadas en el presente estudio.

Resultados

Petrović & Pavlović (2022), manifiestan que, con la llegada de las tecnologías digitales y la relativización del espacio físico, la privacidad se ha vuelto fluida, por lo tanto, la posibilidad de su violación es cada vez más sutil. Son precisamente las tecnologías digitales las responsables de una especie de dispersión de la diferencia entre anonimato y privacidad. Son porosas debido a la intensificación del uso de las tecnologías de vigilancia; para estos autores, el anonimato como tal no es sustancialmente ni bueno ni malo, sino que depende de las circunstancias y el contexto social en el que se manifiesta, por lo tanto, dentro del contexto de una sociedad represiva, el anonimato surge como un mecanismo cuyo propósito reside en la formulación de ideas encaminadas a la democratización de la sociedad, ideas que sólo pueden expresarse de forma anónima por miedo a la sanciones.

Gadotti et al. (2024), por su parte, establecen que la anonimización es un método clave para equilibrar la necesidad de compartir datos con la protección de la privacidad individual, a su vez manifiestan, que cuando un conjunto de datos se anonimiza correctamente, se convierte en información anónima, lo que significa que ninguna persona puede ser identificada a partir de ella, teniendo como objetivo principal que la información anonimizada no pueda ser asociada con un individuo en específico, lo que a su vez previene cualquier daño a su privacidad. Majeed y Lee (2021), incluso manifiestan que "la anonimización es una solución práctica para preservar la privacidad del usuario en la publicación de datos" (p. 8512).

Mientras que para Alnajrani et al. (2020), la privacidad es "un control legítimo sobre los datos personales ya que nadie puede obtener información profesional sin el consentimiento del titular a menos que existan leyes que permitan el acceso a dicha información". Hanover (2021), manifiesta que, si bien el derecho a la privacidad puede parecer abstracto, es el fundamento sobre el cual se construye otros derechos fundamentales. Y agrega manifestando que, del mismo modo, el anonimato al proporcionar un espacio seguro para la expresión, y desarrollo personal es una condición previa para la autonomía.

Ambos conceptos, aunque a veces invisibles son esenciales para una sociedad libre y justa; y es que la privacidad se consagra como un derecho fundamental, mecanismo de la libertad de expresión en redes sociales, un símbolo de protestas digitales ante gobiernos autoritarios o ante el abuso de poder de particulares que permiten al autor expresar un pensamiento sin temor a represalias, y que permite la protección de datos de los usuarios de tal forma que éstos no puedan ser manejados sin el consentimiento del tutor del derecho.

El anonimato y la privacidad se encuentran intrínsecamente ligados, tanto así que en palabras de Moreno (2024), el anonimato es fundamental al salvaguardar grupos vulnerables como activistas, denunciantes o periodistas, por cuanto, pueden compartir información fundamental, exponer abusos sin temor a represalias. Además, facilita que las personas puedan expresar opiniones consideradas como impopulares o polémicas sin enfrentar consecuencias negativas.

Por lo tanto, resulta esencial en contextos autoritarios o en sociedades restrictivas, además, agrega que, dentro de la era digital, el anonimato se convierte en un componente esencial de la privacidad, de la libertad de expresión. Si bien sus beneficios en la protección individual y la promoción de la libre expresión son innegables, los autores manifiestan que también conlleva desafíos, subrayando la necesidad de encontrar el equilibrio entre privacidad y seguridad. Por lo que proteger el anonimato de manera efectiva requiere considerar estos factores y ajustar las políticas y las tecnologías para garantizar este derecho fundamental en un mundo cada vez más globalizado.

Petrović & Pavlović (2022), señalan que en sociedades abiertas y democráticas, donde las opiniones generalmente se pueden expresar libremente, el anonimato puede resultar en ocasiones contraproducente; esto se debe a que puede ser utilizado como una herramienta para promover ideas populistas, discursos demagógicos, o campañas de desinformación que pueden dañar la honra de las personas, esto se produce porque quien ejerce estas acciones no toma medidas de responsabilidad, aprovechando la tecnología con fines destructivos, sin embargo, los autores agregan que esta realidad no invalida el papel modernizador del anonimato; pues del mismo modo, el anonimato aunque puede ser una herramienta utilizada para dañar a otros, dicho uso no deriva de sus características inherentes, sino que responde a distorsiones sociales modeladas por algunos procesos más amplios.

Ossa Monge (2024), sostiene que el ocultamiento de la identidad de quienes cometen delitos o conductas perjudiciales puede anular su sentido de responsabilidad, convirtiéndose en un componente esencial de su accionar; por lo que, la exposición de su identidad funciona como un poderoso disuasivo impulsado por el temor a las repercusiones sociales o legales, sin embargo, curiosamente, el mundo en línea presenta un escenario diferente, donde el anonimato es universalmente aceptado, buscado, y hasta resguardado.

Autores como Petrović y Pavlović (2022), han catalogado al anonimato en línea como una libertad negativa, en tanto permite a individuos resguardarse de sanciones amparándose en derechos fundamentales como la libertad de expresión. El autor en su ensayo sobre "Anonymity and the challenges of regulating online harmful conducts" cita el Libro Blanco sobre Daños en Línea, el cual identifica diversas prácticas dañinas perpetradas en entornos digitales como el acoso cibernético, troleo, contenido y actividad extremista, intimidación, desinformación, contenido violento, denuncia, doxing, etcétera (2024, p. 4).

Por su parte, García et al. (2024), señalan que, con la expansión del internet, especialmente a través de las redes sociales, los discursos de odio se han convertido en un problema de alcance global generando conflictos y actos de violencia en el entorno digital; a su vez, destacan que las plataformas digitales han transformado la forma en que la ciudadanía participa en la vida pública en la era digital.

En esta línea, un informe del UK Departament for Digital, Culture, Media and Sport (Spytska, 2024), identifica tres principales formas de abuso vinculadas al uso del anonimato en línea; la

primera consiste en desacreditar a personas mediante difusión de información falsa a través de redes anónimas; la segunda se refiere al uso del anonimato para perpetrar actos de ciberacoso y emitir amenazas en línea; y la tercera implica la vulneración de la privacidad y la intimidad de las personas, aprovechando el anonimato que ofrece el internet.

Las mujeres constituyen la mayoría de las víctimas de acoso, abuso y hostigamiento sexualizado en entornos digitales, tanto en contextos de anonimato como en situaciones de violencia en las que los agresores son personas conocidas, y aunque el anonimato facilita este tipo de agresiones, no es su único detonante. El abuso en línea tiene consecuencias profundas, ya que afecta la seguridad física, la salud mental, las oportunidades laborales y educativas, así como las relaciones personales de las mujeres, en este contexto, internet actúa como un amplificador del acoso al disminuir los costos sociales para quienes lo ejercen gracias al anonimato y a la validación de ciertos entornos digitales, y al ofrecer nuevas formas de ampliar su alcance y repercusión (Chemaly, 2019; Franks, 2019, citados por Ossa, 2024).

Discusión

Una vez revisada las investigaciones sobre el tema del anonimato, la privacidad y demás puntos, según diversos autores y fuentes de información se debe dejar claro que, en Ecuador, como tal no existe un derecho al anonimato y en muchas otras legislaciones primarias de diferentes naciones tampoco lo hay. Sin embargo, dentro de la Constitución sí se encuentra consagrado el derecho a la privacidad alineado a la protección de datos que garantiza el derecho de las personas a tener autonomía acerca de la información que permite identificarla, lo que se conoce como autodeterminación informativa, contemplada como un derecho en la Constitución, dentro de su artículo 66 numeral 19, que establece que los ciudadanos poseen un derecho inalienable a la tutela de sus datos personales, lo cual abarca el acceso, la gestión y la seguridad de dicha información; así como la recopilación, almacenamiento, procesamiento y difusión de datos personales que se encuentran condicionados a la autorización expresa del titular o de un fundamento legal.

La protección de datos personales garantiza a los individuos el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición (conocidos como derechos ARCO); en particular, los derechos de cancelación y oposición facultan a una persona para negarse a proporcionar sus datos personales. En este sentido, muchas plataformas en línea permiten la creación de cuentas únicamente con un correo electrónico, lo que facilita que los usuarios utilicen direcciones temporales o desechables para registrar cuentas con datos falsos pertenecientes a terceros o incluso inexistentes; esta práctica posibilita el uso de perfiles ficticios, a través de los cuales se pueden perpetrar diversos delitos que van desde el cyberbullying hasta delitos estafas u otras conductas ilícitas.

Revisando el trabajo de Ossa (2024), este tipo de acciones son perjudiciales, porque suelen darse en espacios virtuales: redes sociales, foros o plataformas que permiten la interacción entre los usuarios, así como la publicación de contenidos. Y aunque muchas de estas conductas no

son tipificadas como delitos en determinadas jurisdicciones, podrían generar efectos nocivos, incluyendo daños psicológicos a las víctimas, subrayando el autor, que el anonimato incita a la comisión de infracciones debido a la percepción de impunidad, ya que, precisamente por el anonimato resulta difícil identificar al autor en el entorno digital.

De igual manera, Petrović y Pavlović (2022), sostienen que el anonimato posee un nivel de protección debido a que representa un soporte fundamental de derechos como la libertad de expresión, la privacidad. Aportes que guardan relación con lo indicado en esta investigación, debido que la libertad de expresión en un sentido más amplio; tiene en el anonimato un aliado clave en la lucha por los Derechos Humanos, Derechos Civiles, Culturales, Económicos y Sociales, sumado a los derechos de las mujeres. En la actualidad, se ha convertido en una herramienta esencial para proteger a quienes manifiestan disidencia política.

Tanto la privacidad como el anonimato son fundamentales e inherentes entre sí en el entorno digital moderno, sin embargo, el problema radica en el uso que se les da y de cómo actúa el anonimato como un evasor de responsabilidad en entornos digitales. Por tal razón, resulta imperioso la necesidad de establecer mecanismos regulatorios en torno a la utilización del anonimato en el entorno digital, porque el uso de perfiles anónimos o seudónimos ha permitido la proliferación de comportamientos como el acoso, discursos de odio y estafas.

Autores como García et al. (2024), advierten que espacios virtuales que inicialmente fueron creados para fomentar conexiones entre amigos y desconocidos, lamentablemente se han convertido en plataformas para la difusión de odio y discriminación hacia diversos colectivos, causando estas manifestaciones de ciberodio consecuencias perjudiciales en la calidad de vida y estado emocional de las víctimas. Esto concuerda con la investigación de Petrović y Pavlović (2022), que en el caso ecuatoriano, durante las recientes contiendas electorales se evidenció el uso de los llamados “Troll Centers” como mecanismos de difusión de noticias falsas y mensajes de odio motivados por diferencias ideológicas, con el objetivo de manipular la opinión pública.

Por lo tanto, el problema del anonimato radica en que en un mundo globalizado y digitalizado, el cometimiento de delitos informáticos a través de este se vuelve cada vez más común, García et al. (2024), manifiestan que este permite el cometimiento de actividades ilícitas o dañinas como el ciberacoso, la propagación de información falsa, el fraude, entre otros ciberdelitos; y precisamente, la ausencia de un rastro (trazabilidad) claro de las identidades digitales propicia conductas negativas en la web, representando un obstáculo considerable para las autoridades al intentar rastrear y sancionar a los individuos que se amparan en el anonimato para delinquir.

De acuerdo con Spytska (2024), una estrategia eficaz consiste en restringir la jurisdicción en países que tengan una conexión real y significativa con el hecho investigado, Alemania, por ejemplo, ha implementado un sistema eficiente para combatir las infracciones de derechos de autor en redes.

Aspectos específicos de regulación en China, Francia y Ecuador

China y su privacidad inexistente.

En China prevalecen "las restricciones existentes a la libertad de expresión y al acceso libre a la información han sido temas controvertidos desde mucho antes de internet" (Ramírez, 2017, p. 3). En el sistema de gobierno socialista "el control que ejerce el gobernante Partido Comunista sobre la internet fue fortalecido y es crucial para que el Estado gobierne el ciberespacio", la restricción a la libertad de expresión es un tema que ha llegado incluso a ser normalizado por sus ciudadanos esto con el fin de evitar el surgimiento de problemas con el gobierno.

Según Amnistía internacional "los primeros tiempos de Internet en China se caracterizaron por animados debates en línea. Pero el potencial de la red para difundir nuevas ideas ha hecho que las autoridades tomen medidas para controlar su uso" (2002). El poder que tiene el gobierno o las diferentes instituciones para hacer y deshacer con sus ciudadanos en un país tan imperialista es asombroso, desde vigilancia pública, hasta reconocimiento facial general, el control no tiene límite alguno cuando se trata de proteger los intereses nacionales.

Las autoridades bloquean de manera habitual los sitios de noticias, especialmente los extranjeros, incluidos aquellos que dan cabida a las opiniones de disidentes o grupos prohibidos. El bloqueo parece intermitente, pero es mayor en momentos en que se incrementan las medidas de seguridad, como el aniversario de la represión de las protestas de 1989 en favor de la democracia, la reunión anual de la Asamblea Nacional del Partido o las visitas de jefes de Estado o gobierno (Amnistía Internacional, 2002, p. 8). La libertad de expresión se encuentra vetada por la prohibición de tratar ciertos temas. Se impone a través del artículo 21 un sistema de monitorización por el que los registros de actividad de red deben guardarse durante un periodo de 6 meses (Ramírez, 2017, p. 6).

El gobierno puede acceder a los datos recopilados por Baidu, Alibaba, Tencent, Xiaomi y otros operadores (Ollier, 2024), actividades que puede ir desde filtrar información, crear páginas web, hasta comprar una computadora. Lin Hai, técnico informático de Shanghai, fue detenido en marzo de 1998 y se le considera la primera persona condenada por utilizar Internet China. Fue acusado de subversión y de facilitar 30.000 direcciones de correo electrónico a VIP Reference, revista electrónica favorable a la democrática publicada desde Estados Unidos. Fue condenado a dos años de cárcel en junio de 1999 (Amnistía Internacional, 2002, p. 3).

Aylo vs Europa

En Europa, el gobierno francés también acometió en el tema del control de la privacidad de sus ciudadanos, si bien es cierto, las medidas que Francia están enfocadas en proteger la seguridad virtual de sus ciudadanos o dotarle un mejor respaldo en caso de necesitarlo, sobre todo a sus

compatriotas más jóvenes. Esto ha causado revuelo en aquellos que consumen contenido para adultos desde las principales paginas porno de la multinacional Aylo, situación que ha llegado hasta los altos directivos de esta compañía y es que en Francia ahora rigen nuevas medidas en contra de estas productoras.

> Estos sitios X deben exigir a los usuarios que envíen una foto o un documento de identidad, por ejemplo, y ofrecer al menos un método que respete el principio del doble anonimato, que permite a los usuarios demostrar su mayoría de edad sin revelar su identidad, o enfrentarse a sanciones que podrían llegar hasta el bloqueo del sitio. (France 24, 2025)

Aylo es la matriz empresarial y dueña de tres de los sitios y productoras pornográficas más grandes del mundo. Mismas que ha manifestado su total descontento hacia las medidas tomadas ya que las considera excesivas. Aylo enfatizó que, las medidas puestas en marcha por el Gobierno francés son irrazonables, desproporcionadas e ineficaces (2025). Para esta empresa, la única solución que hacer de Internet un entorno más seguro, es preservar la intimidad del usuario e impidiendo que los niños accedan a contenidos para adultos, así como realizar la verificación de la edad en la fuente. Es decir, en el propio dispositivo, sea un móvil, un ordenador o cualquier otro (Martín, 2025).

Este no es un tema nuevo, de hecho, en España se ha estado trabajando en un sistema denominado Cartera Digital Beta, una herramienta de verificación de edad para acceso a contenido adulto, más allá de restringir el acceso sin restricción a contenido sexual por parte de menores de edad esta sueva herramienta "obliga a los fabricantes de móviles a implementar sistemas de control parental realmente efectivos, crea órdenes de alejamiento digital y tipifica que los deepfakes serán a partir de ahora delitos en contra de la integridad moral (Martín, 2025).

Ecuador y delitos en la web

De acuerdo con la Procuraduría General del Estado (2021, citado por Hernández et al., 2024) uno de los principales desafíos que presenta el sistema frente a los delitos informáticos se encuentra en la duración de la instrucción fiscal que dentro del proceso penal tiene una duración de hasta dos años, durante este tiempo, la Fiscalía, responsable de ejercer la acción penal pública, dirige tanto la fase de la investigación preprocesal como la procesal. Con el apoyo de la Policía de Investigación Judicial sumado a la posibilidad de acudir a profesionales especializados, como es el caso de los peritos.

Se debe tomar en consideración, a pesar de tener esta colaboración, resulta insuficiente, ya que existe una notoria escasez de expertos informáticos, así como una carencia normativa que permita enfrentar eficazmente esta problemática. Según datos publicados en la revista científica de la Fiscalía General del Estado, la cual realiza periódicamente publicaciones en materia penal y temas relacionados a las nuevas modalidades de delincuencia, los datos recolectados por estos investigadores demuestran que con el paso de los años los delitos informáticos no están

disminuyendo, de hecho, algunos de estos están en aumento.

Entre 2017 y 2021, los tipos penales con mayor crecimiento corresponden a la violación de la intimidad, la estafa, el acceso no consentido a un sistema informático, telemático o de telecomunicaciones, y la apropiación fraudulenta por medios electrónicos; estos delitos lideran las estadísticas nacionales referente a los delitos informáticos dentro de ese período de 5 años (Fiscalía General del Estado & Chávez, 2021, p. 59).

En este orden de ideas, la Sentencia No. 2064-14-EP/21 la Corte Constitucional del Ecuador, abordó el tema de la intimidad enfocado como una esfera y espacio en sí mismo, bajo los siguientes términos:

El derecho a la intimidad en su contenido mínimo puede formularse como el derecho a participar en la vida colectiva, a aislarse de la comunidad de cierto modo y durante cierto tiempo, a establecer una relación cero, a disfrutar de un espacio para respirar, a ejercer un derecho de anonimato o también como se dice en doctrina, a tener derecho a un círculo de vida exclusiva, a no ser conocido en ciertos aspectos por los demás, un derecho en definitiva a la propia personalidad.

Conclusiones

En el contexto digital que se vive, internet permite la utilización de una plataforma global, en la cual pueden ser escuchadas las voces allende de las fronteras geográficas. Los foros de mensajería instantánea, plataformas y las redes sociales hacen posible que las personas compartan opiniones e información en tiempo real, o las coloquen emitiendo algún comentario sobre determinados temas. Ante lo cual, los derechos digitales están considerados una extensión de los derechos humanos. Tienen la finalidad de precautelar y servir de garantes a la seguridad de los ciudadanos, cuando estos navegan en la web.

El anonimato también conlleva el incremento de actividades nocivas para la convivencia, como es el caso de la difusión de noticias falsas, discursos de odio, ciberacoso, por nombrar unas cuantas. Si bien el anonimato es una herramienta fundamental para lograr el ejercicio de las libertades individuales, empero, se debe colocar límites a quienes navegan en las redes sociales, para que sus expresiones se enmarquen en el respeto y no crucen la frontera entre la privacidad y la evasión de responsabilidad.

Por esta razón, resulta fundamental que los marcos jurídicos se adapten a este entorno tecnológico, incorporando leyes o adecuar las ya existentes en consonancia con lo establecidos en cuerpos legales supranacionales, para implementar medidas efectivas tendientes a equilibrar la protección de los derechos fundamentales de quienes se pronuncian, así como establecer sanciones administrativas, civiles o penales para frenar el crecimiento de ciberdelitos cometidos bajo el amparo del anonimato.

Referencias

Alnajrani, M. (2020). Privacy and data protection in mobile cloud computing: A systematic mapping study. *PLOS ONE, 15*(6). https://doi.org/10.1371/journal.pone.0234312

Alonso, C. (2021). Claves de la Ley Orgánica de Protección de Datos Personales de Ecuador. GlobalSuite Solutions. https://n9.cl/3327h

Amnistía Internacional. (2002). Métodos de investigación cualitativa, tipos y ejemplos. ATLAS.ti. https://n9.cl/18r3v

Bidart, B., & Carnota, W. (1998). *Derecho constitucional comparado.* Sociedad Anónima Editora, Comercial, Industrial y Financiera.

Comisión Europea. (s/f). ¿Qué son los datos personales? https://n9.cl/evcdl

ueva Luza, T., Jara Córdova, O., Arias Gonzáles, J. L., Flores Limo, F. A., & Balmaceda Flores, C. A. (2023). *Métodos mixtos de investigación para principiantes.* Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://doi.org/10.35622/inudi.b.106

Dávila, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. *Revista de Educaciòn,* 12.

Eklund, L. (2022). Beyond a Dichotomous Understanding of Online Anonymity: Bridging the Macro and Micro Level. *Sociological Research Online, 27*(2), 486–503.

Chávez, F. (2021). Ciberdelitos: Una primera aproximación y proyección institucional. *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad,* 30.

France 24. (2025, 03 de junio 3). Youporn y Pornhub suspenden el acceso en Francia. https://n9.cl/x312e1

Gadotti, A. (2024). Anonymization: The imperfect science of using data while preserving privacy. *Science Advances, 10*(29). https://doi.org/10.1126/sciadv.adn7053

García-Prieto, V., Bonilla-del-Río, M., & Figuereo-Benítez, J. C. (2024). Discapacidad, discursos de odio y redes sociales: video-respuestas a los haters en TikTok. *Revista Latina De Comunicación Social,* (82), 1–21. https://doi.org/10.4185/rlcs-2024-2258

Hanover, S. (2021). Disconnecting the Dots: Anonymity in the Digital Age. University of Oregon. https://hdl.handle.net/1794/26371

Hernández , J. E. P., Criollo , C. A. P., Mera, J. S. P., & Segura, M. W. S. (2024). Organized Crime And Cybercrime In Ecuador, A New Reality Of Complex Criminality. *Migration Letters, 21*(10), 734–747. https://doi.org/10.59670/ml.v21iS11.10561

Kubli-García, F. (2019). Componentes del derecho a la privacidad. *Revista Del Posgrado En Derecho De La UNAM*, (7). https://doi.org/10.22201/fder.26831783e.2019.7.109

Majeed, A., & Lee, S. (2021). Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. *IEEE Access,* 9, 8512–8545.

Martín, N. (2025). ¿Qué pasó con el "pajaporte"?: La app antiporno del Gobierno que debía estar lista el verano pasado. El Independiente. https://n9.cl/d1hvn7

Marx, M. (2018). *Anonymity Online – Current Solutions and Challenges.* Springer.

Moreno, L. (2024). *El derecho al anonimato en la era digital y la libertad de expresión* [Proyecto de investigación, Universidad Regional Autónoma de los Andes].

Naciones Unidas. (2018, 29 de noviembre 29). Artículo 12: Derecho a la intimidad. https://news.un.org/es/story/2018/11/1446671

Ollier, A. (2024). Digital surveillance is omnipresent in China. Here's how citizens are coping. The Conversation. https://n9.cl/6i8qf

Ossa, M. (2024). Anonymity and the challenges of regulating online harmful conducts. *Revista Chilena de Derecho y Tecnologia,* 13. https://doi.org/10.5354/0719-2584.2024.70729

Petrović, D., & Pavlović, D. (2022). Anonymity in the age of the internet. *ANNALS, 70*(1), 161–190.

Ramírez, D. (2017). Ciberseguridad en China. bie3: Boletín IEEE. *Instituto Español de Estudios Estratégicos*, 5, 8–15.

Spytska, L. (2024). Practice-based methods of bringing to legal liability for anonymous defamation on the Internet and in the media. *Social and Legal Studios, 1*(7). https://doi.org/10.32518/sals1.2024.202

Vargas, Y. (2023). *Hábeas data y la protección del derecho a la intimidad desde la sentencia constitucional Nro. 2064-14-EP/21* [Proyecto de titulación, Pontifica Universidad Católica del Ecuador].

Véliz, C. (2019). Online Masquerade: Redesigning the Internet for Free Speech Through the Use of Pseudonyms. *Journal of Applied Philosophy, 36*(4), 643–658. https://doi.org/10.1111/japp.12342

Villalba, A. (2017). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *Foro: Revista de Derecho,* 27.

Autores

Kenlly Stefanía Molina Párraga. Estudiante del 9no semestre de la Carrera de Derecho, Facultad de Ciencias Sociales, Derecho y Bienestar

Steven Orley Mendoza Moreira. Estudiante del 9vo semestre de la Carrera de Derecho, Facultad de Ciencias Sociales, Derecho y Bienestar

Javier Andrés Espinoza Suárez. Abogado por la Universidad Laica Eloy Alfaro de Manabí. Máster en Propiedad Intelectual por la Universidad Carlos III de Madrid. Magister en Derecho Procesal por la Universidad de Especialidades Espíritu Santo de Guayaquil.

Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes externas a este artículo.

Nota

El artículo es original y no ha sido publicado previamente.