FRÓNESIS
Revista de Filosofía Jurídica, Social y Política
Instituto de Filosofía del Derecho Dr. J.M. Delgado Ocando
Universidad del Zulia. ISSN 1315-6268 – Dep. Legal PP. 199402ZU33
Vol. 31, Nº 1, 2023: 115-140

Desafíos éticos de los nuevos emprendimientos tecnológicos y digitales: Un enfoque desde los derechos de los usuarios en el ciberespacio

Patricio Ernesto García Vallejo
Universidad San Gregorio de Portoviejo
patriciogvm31@hotmail.com
https://orcid.org/0009-0006-6958-3808

José Antonio García Vallejo
Abogado en libre ejercicio
joseantoniogarciav@hotmail.com
https://orcid.org/0060-0002-3530-3568

Resumen

En el artículo se examinan aspectos relacionados con los nuevos emprendimientos tecnológicos, los peritajes digitales, los contratos en línea, las firmas digitales y las asesorías virtuales a partir de los derechos de los usuarios en el ciberespacio. La relevancia del estudio radica en el abordaje de las inquietudes que se ciernen sobre la protección de la honra y la intimidad, frente al acoso cibernético, las suplantaciones de identidad y la falsificación, entre otros. El estudio tiene un enfoque cualitativo de carácter doctrinal-bibliográfico para lo cual se llevó a cabo un análisis comparativo para entender algunos aspectos relacionados con su abordaje normativo, interpretando los aportes a través de lo que han señalado distintos especialistas en la materia. Los resultados enfatizan la importancia de examinar críticamente las innovaciones digitales, destacando que, aunque mejoran la vida ofreciendo soluciones eficientes de algunos de los problemas cotidianos, también implican serios riesgos en el ámbito de la protección de los derechos humanos. La tesis central del estudio nos permitió concluir que estos avances demandan una regulación precisa para salvaguardar los

derechos fundamentales en la era digital, en consecuencia, sugerimos crear un marco normativo y ético, y promover educación digital para un uso responsable de la tecnología.

Palabras clave: Derechos del usuario, emprendimientos tecnológicos, firma digital, contratos en línea, peritajes digitales

Ethical challenges of new technological and digital ventures: a user rights perspective in cyberspace

Abstract

In the article, aspects related to new technological ventures, digital forensics, online contracts, digital signatures, and virtual consultations are examined from the standpoint of users' rights in cyberspace. The study's relevance stems from addressing concerns over the protection of honor and privacy against cyberbullying, identity theft, and forgery, among others. The study adopts a qualitative, doctrinal-bibliographic approach, involving a comparative analysis to understand certain aspects of its regulatory approach, interpreting contributions as highlighted by various specialists in the field. The findings stress the importance of critically examining digital innovations, noting that while they enhance life by providing efficient solutions to some everyday problems, they also entail serious risks in the realm of human rights protection. The core thesis of the study led us to conclude that these advancements necessitate precise regulation to safeguard fundamental rights in the digital age. Consequently, we propose the creation of a normative and ethical framework, and the promotion of digital education for responsible technology use.

Keywords: User rights, technological ventures, digital signature, online contracts, digital forensics

Introducción

La omnipresencia de la tecnología en nuestras vidas ha desencadenado transformaciones significativas en la manera en que nos relacionamos,

trabajamos, aprendemos y nos entretenemos. Estos avances, si bien han proporcionado innumerables beneficios a la sociedad, también han generado desafíos éticos y riesgos para los derechos fundamentales de los usuarios de Internet.

Este artículo explora los nuevos emprendimientos tecnológicos, tales como peritajes digitales, contratos en línea, firmas digitales, asesorías virtuales y otras innovaciones, pueden convertirse en vectores de vulneración de derechos, abordando cuestiones críticas como la protección de la honra y la intimidad frente a las conductas ilícitas del acoso cibernético, las suplantaciones de identidad y la falsificación, reconociendo que sin bien es cierto que los avances tecnológicos han traído consigo numerosos beneficios para la sociedad, como el acceso a la información, la educación, la salud, el entretenimiento y el comercio, no es menos cierto que también han generado riesgos para la protección de los derechos humanos.

En este contexto, la contribución de Guaña & Chipuxi (2023) en el análisis del impacto de la inteligencia artificial en la ética y la privacidad de los datos desde una perspectiva contemporánea y objetiva, arroja una luz invaluable sobre la materia intrínseca de este artículo. Por otro lado, la obra de Castillo Jiménez (2021) sobre "Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información" constituye una referencia fundamental para comprender a fondo el alcance de este tema. Peña (2021) resulta esencial para comprender el Big Data y la inteligencia artificial desde una perspectiva ética jurídica, mientras que Lucena (2019) ofrece una visión clara sobre el impacto de las nuevas tecnologías en los Derechos Humanos desde un enfoque ético.

Por su parte, Ramos & Sánchez (2023) aportan teorías cruciales sobre la protección de datos personales frente a la interceptación ilegal de datos. Además, Obando (2000) enriquece la investigación con su conocimiento sobre contratos electrónicos y digitales, aspectos centrales para el desarrollo del presente artículo. Finalmente, Zapata, Fernández & Neira (2008) destacan por su valioso aporte en el estudio del emprendimiento tecnológico,

especialmente en su impacto en Suramérica, lo que se vincula directamente con la esencia investigativa de este artículo.

La tesis de partida es que estos emprendimientos tecnológicos requieren una regulación adecuada y una educación digital para garantizar el respeto y la protección de los derechos de las personas en el ciberespacio, tomando en consideración algunos ejemplos puntuales sobre nuevos emprendimientos tecnológicos, entre estos los peritajes digitales, los contratos en línea, las firmas digitales, las asesorías virtuales y el uso de la inteligencia artificial, destacando en criterio de los autores consultados las causas y las consecuencias de las potenciales vulneraciones de los derechos humanos, lo que nos permitió proponer algunas medidas para prevenir o mitigar estos riesgos.

Metodología

Este estudio adoptó un enfoque metodológico cualitativo con el uso de los métodos analítico y comparativo. El enfoque cualitativo, basado en los principios y técnicas propuestas por autores como Fix-Zamudio (2007) y Juan Carlos Ferré Olivé (año de publicación), quienes ofrecen una comprensión profunda de la metodología de la investigación jurídica en la región, misma que sirvió para comprender en profundidad el fenómeno investigado mediante el análisis de documentos.

Paralelamente, empleamos el método comparativo, inspirado en Fix-Zamudio (2007), para analizar las diferencias y similitudes entre distintas legislaciones sobre el tema, considerando su alcance, enfoque, aplicación y efectividad. Además, realizamos una revisión analítica exhaustiva de la bibliografía relevante, siguiendo las pautas de Pérez (2010), para contextualizar nuestro estudio e identificar lagunas en las normas existentes. Integrando estos enfoques, se analizó y sintetizó los datos para interpretar los resultados y generar conclusiones significativas que contribuyan al entendimiento del tema y orienten futuras investigaciones.

Resultados

La influencia de la tecnología se ha extendido por todos los ámbitos de nuestra existencia, desde la forma de comunicarnos hasta las actividades laborales, educativas, comerciales y recreativas. Esta amplia presencia tecnológica ha generado transformaciones importantes en nuestras interacciones y conductas. Como respuesta a estos cambios, las normativas y leyes también deben adaptarse y progresar para estar en sintonía con los avances tecnológicos.

Como expresa Gómez (2019) desde una perspectiva jurídica, hay varios temas importantes que surgen en este contexto: la privacidad y protección de datos; el comercio electrónico y los nuevos emprendimientos digitales, entre otros. Esto lleva al autor a señalar que estas prácticas deben ser reguladas. Ciertamente, la validez y aplicabilidad de los contratos electrónicos, así como la incidencia de delitos cibernéticos, como la apropiación indebida de datos, la violación de la privacidad y los derechos de autor, son aspectos vitales en el contexto de su regulación actual, en virtud de que los emprendimientos basados en tecnología y avances cibernéticos pueden eventualmente poner en riesgo los derechos fundamentales.

En este sentido, identifica Rodríguez (2022), algunas de las prácticas relacionadas con la era digital, señalando que:

> *Los peritajes digitales son servicios que ofrecen análisis forenses de evidencias digitales para resolver conflictos legales. Las firmas digitales son mecanismos que permiten autenticar la identidad de un firmante y garantizar la integridad de un documento electrónico. Las asesorías virtuales son servicios que ofrecen orientación o asistencia profesional a través de plataformas digitales. La falsificación con IA es una técnica que utiliza inteligencia artificial para reemplazar la semejanza de una persona con otra en videos y otros medios digitales (p. 12).*

Estos aspectos constituyen la base del examen acerca de los nuevos emprendimientos y su relación con la debida protección de los derechos de los usuarios, que entraremos a detallar a continuación.

1. Los peritajes digitales desde la óptica de la protección de datos.

Respecto de los peritajes digitales, debemos entender que son el conjunto de técnicas y procesos utilizados para analizar, recolectar y presentar evidencia digital en entornos judiciales o de investigación. En el contexto contemporáneo, donde la información se encuentra predominantemente digitalizada, estos peritajes se han vuelto indispensables para el esclarecimiento de crímenes cibernéticos, disputas comerciales y otros casos relacionados con la tecnología. Sin embargo, este desarrollo no está exento de dilemas éticos y legales.

Uno de los dilemas, como expresa Sampaoli (2018) es la intrusividad inherente a los peritajes digitales, misma que se manifiesta en la forma en que los expertos en este campo acceden, examinan y utilizan datos personales. Como expresa el autor, a medida que las tecnologías avanzan, la capacidad de extracción de información aumenta, llevando consigo un riesgo significativo para la privacidad de los individuos. Respecto de esta idea debemos reconocer que la recolección de datos puede superar límites éticos si no se lleva a cabo con el máximo respeto a los derechos fundamentales de las personas.

En consecuencia, los peritajes digitales han emergido como herramientas fundamentales en la resolución de disputas y crímenes en el vasto terreno del mundo digital, aun así se deben reconocer las complejidades asociadas con estos peritajes, especialmente en relación con la privacidad y la integridad personal.

Subrayamos entonces con Alamillo (2022) que la recolección y análisis de datos en este contexto no solo plantean cuestiones éticas y legales, sino que también introducen el riesgo de decisiones injustas basadas en pruebas tecnológicas, por esta razón, la protección de la honra y la preservación de la

dignidad son elementos que deben ser salvaguardados en el vertiginoso avance de estas tecnologías digitales.

Así las cosas, el riesgo de malinterpretaciones y decisiones injustas también se cierne sobre los peritajes digitales. La complejidad de la evidencia digital y la interpretación de datos pueden dar lugar a errores que, en última instancia, podrían impactar de manera adversa en la vida de las personas. Este riesgo se ve agravado por la rapidez con la que evolucionan las tecnologías, superando la capacidad de las leyes y regulaciones para mantenerse al día.

Dentro de este marco de ideas, la protección de la honra y la preservación de la dignidad son aspectos críticos que a menudo se pasan por alto en el proceso de peritajes digitales. La exposición no autorizada de información sensible, la divulgación de detalles privados y la interpretación equivocada de datos pueden tener consecuencias devastadoras para la reputación y el bienestar psicológico de los individuos involucrados. La dignidad en el contexto digital se convierte en un valor de extrema vulnerabilidad, susceptible a la intrusión de tecnologías que, aunque su fin sea la búsqueda de la verdad, también pueden socavar la integridad personal y distorsionar la realidad.

Conforme con lo expuesto, en el núcleo de los peritajes digitales y su impacto en la integridad personal están las consideraciones éticas y legales. Por esta razón, la ética en la recopilación y el uso de datos debe ser una preocupación primordial para garantizar que los derechos individuales sean respetados. Además, la legalidad de las técnicas utilizadas y la protección contra el uso indebido de información son aspectos esenciales que requieren la atención constante de legisladores y profesionales del Derecho.

Ahora bien, todos conocemos que la legislación y regulación en torno a los peritajes digitales están en constante evolución para hacer frente a los desafíos emergentes que plantea su uso. En el contexto de Ecuador y otras jurisdicciones, como indican Bolaños & Gómez (2015) se hace necesario revisar y actualizar las leyes para abordar los riesgos y proteger los derechos

de los individuos. La adaptación de la legislación es esencial para garantizar que las prácticas de peritajes digitales estén alineadas con los principios fundamentales de justicia, equidad y respeto a los derechos humanos.

Particularmente, en Ecuador, los peritajes digitales están regidos principalmente por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2023). Esta legislación reconoce la equivalencia funcional entre documentos electrónicos y sus contrapartes físicas. Sin embargo, la aplicación de estas disposiciones en el ámbito de los peritajes digitales plantea desafíos específicos, especialmente en lo que respecta a la privacidad y la integridad personal.

A pesar de los esfuerzos regulatorios existentes, aún queda un camino por recorrer, ya que es necesario abordar de manera integral cómo se obtienen, almacenan y utilizan los datos digitales en los peritajes. Como señalamos, la naturaleza intrusiva de estas prácticas y el riesgo de malinterpretaciones deben ser cuidadosamente considerados en leyes y regulaciones específicas para garantizar una protección adecuada de los derechos individuales.

Bajo este orden de ideas, Galindo (2009) expresa que el principio de protección de la integridad personal es central en los peritajes digitales, y su consideración ética y legal es esencial, ya que la exposición de información sensible y la interpretación de datos plantean riesgos significativos para la privacidad y la reputación de los individuos involucrados. En este contexto, la legislación ecuatoriana debe establecer salvaguardias específicas que equilibren la necesidad de realizar peritajes con la protección de los derechos fundamentales de las personas.

Además, es importante abordar la interpretación de datos en los peritajes digitales de manera rigurosa y transparente. Esto implica desarrollar protocolos claros y criterios consistentes para la evaluación de la evidencia digital, asegurando así la fiabilidad y la objetividad en los procesos periciales. La capacitación continua de los peritos en el análisis de datos digitales y la colaboración interdisciplinaria entre expertos en tecnología y

juristas son aspectos fundamentales para garantizar una interpretación precisa y justa de la evidencia digital en el ámbito judicial, ya que como explica Quiroz & Quiroz (2021) la velocidad del avance tecnológico puede superar la capacidad de las leyes para mantenerse actualizadas, lo que subraya la necesidad de una legislación flexible y adaptable que pueda abordar las complejidades emergentes en este campo.

Frente a esto debemos reconocer los aportes del ámbito del derecho internacional, donde los peritajes digitales están influenciados por diversas normativas y convenciones, entre estas la Convención de Budapest sobre Ciberdelincuencia, de la cual Ecuador es parte, la cual proporciona un marco para la cooperación internacional en la lucha contra la delincuencia cibernética. Sin embargo, no basta conocer su contenido, sino entender que la aplicación de estos principios a peritajes digitales específicos requiere una consideración y conocimiento minucioso.

En este orden de análisis, la transfronterización de datos y la colaboración internacional en pericias digitales también es un aspecto que plantea importantes desafíos legales, al involucrar temas como el respeto a la soberanía de las naciones y la protección de los derechos individuales, los cuales se deben convertir en elementos fundamentales en cualquier cooperación internacional en este ámbito (Torres, 2017).

En conclusión, los peritajes digitales, a pesar de su papel crucial en la resolución de disputas y crímenes en el mundo digital, no están exentos de desafíos éticos y legales. La intrusividad, los riesgos de malinterpretación y la vulnerabilidad de la honra y la dignidad son cuestiones que demandan una atención cuidadosa. Frente a esto, señala Centorame (2021) que la evolución constante de la legislación y la implementación de salvaguardias éticas y técnicas son imperativos para equilibrar la necesidad de justicia con la protección de los derechos individuales en la era digital.

2. Los contratos en línea: una mirada desde la validez y aplicabilidad.

La proliferación de contratos en línea ha marcado un cambio significativo en la dinámica de las transacciones comerciales, tanto de bienes

como de servicios. La aceptación virtual de términos y condiciones se ha vuelto ubicua en la era digital, generando interrogantes sobre la validez jurídica de estos contratos, tanto en el ámbito nacional como en el internacional. En este acápite, nos adentraremos en la definición de contratos en línea, explorando algunos aspectos acerca de su validez en el marco del derecho ecuatoriano, lo cual nos permitirá identificar algunos riesgos inherentes de esta práctica, que van desde la desinformación hasta la estafa.

Precisa Obando (2000) que los contratos en línea, también conocidos como contratos electrónicos, son acuerdos legales celebrados a través de medios electrónicos. Estos contratos abarcan una amplia gama de transacciones, desde compras en línea hasta acuerdos de servicios, donde las partes involucradas aceptan los términos y condiciones mediante interacciones digitales.

Entre otros aspectos, la ausencia de una firma física convencional plantea preguntas sobre la autenticidad y la validez legal de estos contratos. Por otra parte, uno de los riesgos más significativos de la aceptación rápida de contratos en línea es la falta de comprensión de los términos por parte de los usuarios. Las cláusulas poco claras pueden exponer a las partes a responsabilidades no anticipadas. La desinformación también juega un papel crucial, ya que los usuarios pueden aceptar condiciones que afectan sus derechos sin estar plenamente conscientes de las implicaciones legales. Todos estos aspectos crean un terreno fértil para abusos, estafas y malentendidos.

Desde el punto de vista legal, los desafíos inherentes a los contratos en línea incluyen la autenticidad de la aceptación y la garantía de que las partes tengan la capacidad legal para aceptar los términos propuestos. La protección del consumidor también es un área crítica, ya que los contratos en línea a menudo contienen cláusulas que limitan la responsabilidad de los proveedores de servicios de manera desproporcionada.

Así las cosas, la validez de los contratos en línea en Ecuador y el ámbito internacional plantea complejidades legales y éticas. A medida que la

sociedad digital avanza, es imperativo abordar estos desafíos para garantizar la equidad y la protección de los derechos de los consumidores. Se requiere entonces una mayor claridad normativa, así como iniciativas educativas para empoderar a los usuarios y fomentar una aceptación informada de los contratos en línea, ya que como exponen Rosales & Molestina (2000) la intersección entre la tecnología y el Derecho demanda una atención continua para garantizar la integridad y la equidad en las transacciones digitales.

Si bien es cierto que la celebración de contratos en línea ha simplificado la transacción de bienes y servicios, es menester preguntarnos: ¿en qué medida están protegidos los derechos de los consumidores? Esta pregunta ha sido analizada y respondida por Rodríguez (2012), autor que advierte sobre la opacidad en los términos y condiciones, la falta de comprensión del usuario promedio y la posible manipulación en la redacción de contratos como elementos que ocupan la atención de los especialistas en estas áreas. Por tanto, la recomendación del autor es persistir en explorar como estos contratos pueden convertirse en herramientas de explotación, profundizando en la necesidad de que los Estados implementen políticas y leyes que aseguren transparencia y equidad en las transacciones digitales.

Frente a esto colegimos que la adopción de firmas digitales ha simplificado los procesos de autenticación, pero también ha planteado problemas en términos de seguridad. Fernández (2016) aporta en esta discusión su conocimiento despejando la siguiente pregunta ¿Hasta qué punto podemos confiar en la autenticidad de una firma digital? Ciertamente, la amenaza de suplantación de identidad y falsificación digital es real, y por esta razón es imperativo contar con regulaciones más estrictas para garantizar la integridad de las firmas digitales y la protección de la identidad personal.

3. Puntuales aspectos sobre los riesgos relacionados con el uso de la Inteligencia Artificial y el derecho de los usuarios a la protección de su intimidad.

Como expresan Rebaza, Demichelli & Silva (2017), la confidencialidad de la información compartida en entornos virtuales de asesoramiento puede

estar en peligro, y por tanto siempre se debe abogar por medidas que preserven la confianza del usuario y protejan la privacidad en este contexto emergente. A título ilustrativo, reconocemos el auge de las asesorías virtuales como una nueva modalidad de emprendimiento, lo cual por un lado, ha facilitado el acceso a servicios profesionales, pero por el otro ha representado serios riesgos en términos de privacidad de las personas.

Otro fenómeno contemporáneo es el del acoso cibernético, que parte de la exposición mediática de las personas en las redes sociales y que ha alcanzado proporciones alarmantes. Partamos de que las redes sociales son un negocio que, si se quiere, puede homologarse con el emprendimiento. En este sentido expresa López (2012) que la venta de datos personales ha estado en la mira de los especialistas desde hace tiempo ya que representa un grave peligro para los usuarios.

Particularmente, la libertad de expresión y la interconexión global han traído consigo nuevas formas de vulnerabilidad, como la difamación en línea y la exposición no consensuada de información personal. Así, la profusión de datos en las redes sociales puede ser utilizadas como herramientas de hostigamiento mediático, por esto la urgencia de que los Estados adopten estrategias que mitiguen estos riesgos.

Solo a título ilustrativo, tenemos casos de falsificación con IA, que es una técnica que utiliza inteligencia artificial (vista como emprendimiento de grandes empresas que la comercializan o difunden) para reemplazar la semejanza de una persona con otra en videos y otros medios digitales. Así, Flores (2019) manifiesta que la utilización de IA puede aportar beneficios como la creatividad, el entretenimiento, la educación mejorada, la ganancia de tiempos y esfuerzos importantes en la investigación y desarrollo del conocimiento; pero tiene un lado oscuro sobre el que hay que legislar a tiempo.

En este orden de ideas, los usuarios tienen derechos específicos, como el derecho a la privacidad y el derecho a un trato justo. La violación de estos derechos podría dar lugar a acciones legales por parte de los consumidores.

Ante esto, la mayoría de las legislaciones de Europa y de forma incipiente las de América Latina, exigen un consentimiento informado para recopilar y utilizar datos personales.

Ilustra Riofrio (2014) en este particular que, el incumplimiento del consentimiento informado trae importantes consecuencias legales, en virtud de que los individuos afectados podrían emprender acciones civiles contra las entidades responsables por daños y perjuicios derivados del mal uso de sus datos o de la exposición a publicidad no deseada. Los perjudicados tendrían también la opción de buscar compensación económica por pérdida de privacidad, daño reputacional u otros daños tangibles e intangibles.

En algunas legislaciones, las plataformas digitales podrían ser consideradas responsables por facilitar o permitir prácticas ilícitas en sus servicios. La legislación puede imponer la obligación de implementar medidas para prevenir el mal uso de datos y la publicidad no deseada.

Todo lo expuesto nos lleva a considerar la necesidad de que los Estados fortalezcan sus leyes para garantizar que las plataformas cumplan con estándares éticos y legales, y en caso de incumplimiento estarían compelidos a imponer las correspondientes sanciones. En efecto, Diaz (2017) expresa que, las autoridades de regulación, tanto a nivel nacional como internacional, pueden llevar a cabo investigaciones para garantizar el cumplimiento de las leyes de protección de datos y de prácticas comerciales justas. Las entidades que violan las leyes pueden estar sujetas a acciones de cumplimiento que podrían incluir la corrección de prácticas, la implementación de medidas de seguridad adicionales y la supervisión continua.

Como observamos, en un entorno digital cada vez más complejo, las consecuencias legales del mal uso de la información del usuario y la publicidad no deseada son significativas. Esta premisa lleva a Muela-Molina (2011) a señalar que los marcos legales, tanto a nivel nacional como internacional, están evolucionando para abordar estos problemas y proteger los derechos fundamentales de los usuarios, por lo que es necesario que los creadores y las plataformas digitales operen con transparencia y ética,

cumpliendo con las leyes y regulaciones vigentes, adoptando prácticas que respeten la privacidad y la autonomía de los usuarios.

4. La protección de los derechos de los usuarios frente a la responsabilidad ética de los creadores.

En criterio de Mieles (2020) los creadores de nuevas tecnologías y desarrollos digitales se encuentran en una posición paradójica: mientras son los arquitectos de innovaciones que transforman la sociedad, también se han convertido en detractores de sus propias creaciones debido al uso que se les da. Esto lleva al autor a explorar la compleja dinámica de esta paradoja, enfocándose en el mal uso de la información de los usuarios y la proliferación de publicidad no deseada basada en sus preferencias de navegación y a través de un análisis crítico logra identificar los desafíos éticos y sociales que emergen de este fenómeno.

Reiteramos que uno de los desafíos más acuciantes es el mal uso de la información del usuario, que a menudo es recopilada y utilizada para diversos fines sin el conocimiento o con un consentimiento no informado. A partir de estos resultados, es importante reconocer que, la información personal, desde preferencias de compra hasta datos de ubicación, se convierte en una herramienta valiosa, pero también en un riesgo para la privacidad y la seguridad. Por esta razón, la Oficina de Comunicación y Mercadeo del Tecnológico de Costa Rica, en el año 2016, ha señalado que la creación de perfiles detallados puede llevar a la manipulación de opiniones, la discriminación y, en última instancia, a la erosión de la confianza en las plataformas digitales.

En relación con esto, la publicidad digital, está asociada con aquellos anuncios personalizados, pero en la práctica, este intento de personalización puede convertirse en un invasivo recordatorio del mal uso de la información del usuario. A esto se une la advertencia que realiza De Salas (2010) cuando señala que la publicidad indeseada, basada en patrones de navegación y preferencias, no solo interrumpe la experiencia en línea, sino que también plantea cuestiones éticas sobre la privacidad y la autonomía del usuario.

Entonces, la creación de sistemas éticos implica la incorporación de principios como la transparencia, el consentimiento informado y la seguridad robusta que los creadores deben considerar, no solo en la creación inicial, sino también en la implementación y el monitoreo continuo de sus tecnologías. Ante esto, el Derecho debe normar, incluso desde la coercitividad de la ley, para evitar que estos hechos ocurran.

La regulación entonces emerge como un componente vital en la mitigación de los riesgos asociados con el mal uso de la información del usuario y la publicidad no deseada. En el contexto de Ecuador, y otras jurisdicciones la legislación debería evolucionar para abordar los vacíos legales que permiten la explotación de datos y establecer límites claros sobre cómo se pueden utilizar los datos personales. El papel de las autoridades regulatorias es relevante para garantizar que las prácticas sean éticas, transparentes y alineadas con los derechos del usuario.

Nótese que el mal uso de la información del usuario y la publicidad no deseada no solo tienen implicaciones éticas, sino que también generan un impacto significativo en el plano social y psicológico. Además, la manipulación de la información puede afectar la toma de decisiones individuales y la percepción de la realidad, planteando preguntas sobre la autonomía y la libertad de elección en el entorno digital.

Ante este panorama, los creadores deben adoptar enfoques éticos desde las etapas iniciales de desarrollo, precisando que las leyes han de estar ahí para corregir cualquier problema asociado con la vulnerabilidad de los usuarios. Ya que tal y como lo expresa Jonás (2014) la inclusión de evaluaciones éticas en el diseño de tecnologías, la promoción de la diversidad en los equipos de desarrollo y la implementación de prácticas de desarrollo centradas en el usuario son elementos clave en la construcción de sistemas digitales que respeten la integridad del usuario.

Parafraseando a Katz & Rice (2006) el mal uso de la información del usuario y la publicidad no deseada plantean desafíos éticos que requieren un abordaje multidisciplinario para su tratamiento. Esto nos lleva a subrayar las

consecuencias legales derivadas del mal uso de la información del usuario y la publicidad no deseada en el entorno digital son un tema de creciente importancia y complejidad.

Las repercusiones legales que podrían surgir en este contexto tanto en Ecuador como en la Unión Europea las podemos resumir en estos dos párrafos. En el ámbito de la legislación ecuatoriana, las violaciones de privacidad y protección de datos se abordan a través de la Ley Orgánica de Protección de Datos Personales (2021), en esta norma se dispone tajantemente que utilizar la información del usuario sin su consentimiento o de manera contraria a los principios establecidos en esta ley podría resultar en sanciones legales.

Si el mal uso de la información del usuario involucra transacciones transfronterizas, las leyes de protección de datos internacionales, como el Reglamento General de Protección de Datos (2016) de la Unión Europea, pueden tener relevancia por lo que la violación de estas regulaciones podría resultar en multas significativas.

Por último, los creadores, reguladores, y la sociedad en su conjunto deben colaborar para desarrollar soluciones sociales y jurídicas que equilibren la innovación con la protección de los derechos individuales, construyendo así un futuro digital más ético y sostenible.

Discusión

Los resultados nos permiten realizar la siguiente discusión. Mientras celebramos los avances tecnológicos que han transformado nuestras vidas, es imperativo reconocer y abordar los desafíos éticos que acompañan a estos cambios reconociendo que los derechos fundamentales de los usuarios deben ser resguardados en el ciberespacio, acción que requiere un enfoque integral que involucre tanto a legisladores como a educadores. Frente a esto, la creación de un entorno digital seguro y ético es una tarea colectiva que define el camino hacia un futuro tecnológico más equitativo y sostenible.

Surge de lo expuesto, que la relación entre emprendimiento digital, de la naturaleza que fuere, incluido el desarrollo de redes sociales y comunidades, así como los materiales de consumo monetarizado deben estar fundamentados en el respeto de los derechos básicos de los usuarios. En consecuencia, se ha de tomar en cuenta aspectos que la doctrina especializada ha planteado, como en el caso de los peritajes digitales, los cuales tienen un potencial para vulnerar el derecho a la intimidad de los usuarios, entendiendo que toda persona goza de la prerrogativa de mantener en reserva ciertos aspectos de su vida privada, como sus datos personales, sus comunicaciones, sus preferencias, sus hábitos, entre otros.

Precisamente, los servicios que ofrecen el análisis forenses de evidencias digitales para resolver conflictos legales se centran en la observación y colección de evidencias entre las que se incluyen correos electrónicos, mensajes de texto, fotos, videos, historiales de navegación, registros de llamadas, ubicaciones, entre otros. En efecto, los peritos digitales pueden acceder a estas evidencias mediante técnicas como la extracción de datos, la recuperación de datos borrados, el análisis de metadatos, el rastreo de dispositivos, subrayando que estas técnicas pueden vulnerar el derecho a la intimidad de los usuarios si se realizan sin su consentimiento o sin una orden judicial que lo autorice. Amén del riesgo de exposición o filtración de las evidencias que analizan, lo que puede generar riesgos adicionales para la seguridad y la reputación de los usuarios.

Conforme con lo señalado, denotamos que la rápida evolución de la tecnología y la consiguiente complejidad de los peritajes digitales, obligan al Estado ecuatoriano y a todos los países a evolucionar normativamente. Esto implica revisar y actualizar las leyes para abordar los riesgos emergentes y proteger eficazmente los derechos de las personas.

Es esencial también considerar cómo la legislación puede fomentar la formación ética y técnica de los profesionales involucrados en pericias informáticas. Esto puede incluir la incorporación de estándares éticos claros y programas de capacitación para garantizar que la integridad personal y la privacidad estén en el centro de estas prácticas. En el caso de Ecuador,

consideramos que se podrían incluir disposiciones claras sobre la obtención de consentimiento informado, restricciones en la recolección de datos sensibles y mecanismos para corregir errores en la interpretación de datos.

Aunque, reconozcamos el valor de las buenas prácticas, la legislación de cada país, y en particular, la de Ecuador, debe ser un reflejo de los valores fundamentales de justicia, equidad y respeto a los derechos humanos, asegurando al mismo tiempo la eficacia en la resolución de disputas y crímenes en la era digital. Subrayando con Sánchez (2014) que debe existir un perfecto equilibrio entre la necesidad de justicia y la preservación de los derechos individuales, elementos vitales para construir un marco legal coherente y ético para los peritajes digitales en Ecuador y a nivel internacional.

Respecto de los contratos en línea, que son acuerdos que se redactan, firman y ejecutan electrónicamente a través de Internet, ha quedado planteado que pueden aportar beneficios como la rapidez, la comodidad, la eficiencia, la reducción de costos y la seguridad jurídica, con lo cual pueden facilitar las transacciones comerciales, las relaciones laborales, las operaciones financieras y otros tipos de acuerdos entre las partes.

Sin embargo, también pueden generar riesgos como la falta de transparencia, la vulneración de la autonomía, la manipulación de la información y el incumplimiento de las obligaciones. A esto se suma, la afectación del derecho a la honra de los usuarios si se utilizan para difamar, injuriar o calumniar a una persona o a una entidad. Finalmente, pueden afectar el derecho al debido proceso de los usuarios si se establecen cláusulas abusivas, arbitrarias o ilegales que limiten sus derechos o garantías.

En franca relación con lo señalado, las firmas digitales, reconocidas en esta era como mecanismos que permiten autenticar la identidad de un firmante y garantizar la integridad de un documento electrónico también pueden aportar beneficios como la seguridad, la confiabilidad, la validez y la eficacia de los documentos electrónicos, también pueden facilitar la firma de

documentos legales, administrativos, académicos y personales sin necesidad de imprimirlos o enviarlos físicamente.

Empero, generan ciertos riesgos como el robo, la pérdida, el uso indebido o la falsificación de las firmas digitales. En este sentido, las firmas digitales pueden afectar el derecho a la identidad de los usuarios si se utilizan para suplantar o usurpar la identidad de una persona o de una entidad. También pueden afectar el derecho a la propiedad de los usuarios si se utilizan para apropiarse o transferir ilegalmente bienes o derechos.

Cabe explicar que el entorno de las asesorías virtuales, como servicios que ofrecen orientación o asistencia profesional a través de plataformas digitales, al igual que los otros aspectos tratados, pueden aportar beneficios como la accesibilidad, la flexibilidad, la personalización y la diversidad de las ofertas, facilitando el acceso a profesionales cualificados en diferentes áreas del conocimiento, como la educación, la salud, el derecho, la contabilidad, entre otros. Además, pueden adaptarse a las necesidades, los horarios y los ritmos de aprendizaje de los usuarios.

La problemática que afrontan estos emprendimientos es la falta de calidad, la deshumanización, la desconfianza y la vulnerabilidad de los datos. Las asesorías virtuales pueden afectar el derecho al acoso cibernético de los usuarios si se utilizan para hostigar, intimidar, amenazar o extorsionar a una persona o a una entidad. También pueden afectar el derecho a la protección de datos de los usuarios si se utilizan para recopilar, almacenar, procesar o divulgar información personal o sensible sin el consentimiento o la autorización de los titulares.

En el contexto jurídico de Ecuador, la aceptación de contratos en línea se rige por la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, que reconoce la equivalencia funcional entre documentos electrónicos y físicos. Sin embargo, surge la interrogante sobre la capacidad de las partes para comprender completamente los términos de esta regulación, en especial cuando se aceptan rápidamente y sin una revisión adecuada. Por tanto, la

jurisprudencia ecuatoriana debe abordar estos desafíos para garantizar que la aceptación en línea sea informada y voluntaria.

El Reglamento del Sistema Pericial Integral (2014) que rige el servicio pericial de la Función Judicial en Ecuador, incluidos los peritajes digitales, es fundamental para esta investigación. Asimismo, la Ley Orgánica de Protección de Datos Personales (2021) garantiza el ejercicio del derecho a la protección de datos personales, mientras que la Política Nacional de Ciberseguridad (2021) aborda aspectos relacionados con la seguridad de la información y las nuevas tecnologías en Ecuador.

A nivel internacional, la aceptación de contratos en línea plantea desafíos debido a la diversidad de sistemas legales. Sin embargo, la Convención de las Naciones Unidas sobre Contratos de Compraventa Internacional de Mercaderías (CISG) proporciona un marco para las transacciones comerciales internacionales, pero la falta de uniformidad en las leyes aplicables a los contratos en línea aún está por resolver, como señala Galán (2004).

Del mismo modo, las Normas de Comercio Electrónico de la Unión Europea (2021) y el Reglamento General de Protección de Datos (RGPD) garantizan la seguridad y el respeto de los derechos fundamentales en el uso de inteligencia artificial en la UE, según indican Ortega & Domenech (2018). Finalmente, la Ley de Ciberseguridad de la Unión Europea (2023) introduce un marco de certificación de ciberseguridad para productos, servicios y procesos de la Tecnología de la Información y las Comunicaciones (TIC) a escala de la UE.

En este contexto, la tesis subyacente en este análisis es que estos emprendimientos tecnológicos demandan una regulación adecuada y una educación digital extensa para garantizar el respeto y la protección de los derechos de las personas en el ciberespacio. A esto se le suma la creación de marcos legales que aborden específicamente estas cuestiones y la promoción de programas educativos que fortalezcan la conciencia digital son pasos

necesarios para mitigar los riesgos asociados con las innovaciones tecnológicas.

Conclusiones

Con base en lo expuesto concluimos que, si bien los peritajes digitales desempeñan un papel esencial en la resolución de disputas y delitos en el entorno digital, también plantean algunos cuestionamientos relacionados con la protección de la privacidad y la integridad personal, circunstancia que deben ser tomada en consideración por los operadores de justicia. Por consiguiente, es necesario tomar precauciones para evitar que, durante la recolección y análisis de datos, los peritos puedan ser intrusivos.

Además se debe precaver que algunas conclusiones contenidas en los informes periciales puede conllevar a interpretaciones erróneas por parte de las y los jueces y a decisiones injustas basadas en un mal manejo de las pruebas tecnológicas. La comprensión de este tema es fundamental ya que la protección de la reputación y la preservación de la dignidad, como señala Castillo (2020), son aspectos críticos que deben ser resguardados frente a la expansión de estas tecnologías.

Por otra parte, la Inteligencia Artificial puede facilitar la creación de contenidos audiovisuales originales, divertidos, didácticos o científicos pero al mismo tiempo puede generar riesgos como la desinformación, la manipulación, la difamación y el engaño. Incluso, la falsificación con Inteligencia Artificial afecta el derecho a la verdad de los usuarios si se utiliza para crear o difundir noticias falsas, propaganda política, testimonios o evidencias falsas. También puede afectar el derecho a la imagen de los usuarios si se utiliza para crear o difundir imágenes comprometedoras, ofensivas o ilegales.

En este artículo, se han dispuesto, de una manera genérica, un conjunto de aspectos relativos a los emprendimientos tecnológicos, los peritajes digitales; contratos en línea, firmas digitales y asesorías virtuales, que basados en el uso de las nuevas tecnologías pueden vulnerar derechos de los usuarios, tales como la honra y la intimidad. Frente a esto, hemos

argumentado que todos ellos requieren una regulación adecuada y una educación digital para garantizar el respeto y la protección de los derechos humanos en el ciberespacio.

Las recomendaciones del estudio apuntan a la protección de los derechos de los usuarios frente al uso de las nuevas tecnologías, entre las cuales consideramos que se debe promover una legislación nacional e internacional que armonice los derechos de los creadores y los usuarios, y que establezca mecanismos efectivos de protección y sanción; al mismo tiempo se debe fomentar una cultura de respeto y responsabilidad en el uso de estos medios, mediante la educación, la sensibilización y la difusión de sus riesgos.

La idea central del estudio es que tales innovaciones digitales reposen bajo una lupa crítica, ya que a pesar de que tienen el potencial de mejorar la calidad de vida de las personas, al ofrecer soluciones innovadoras, eficientes y accesibles para diversos problemas o necesidades, también tienen el riesgo de vulnerar los derechos humanos de los usuarios, al exponerlos a situaciones de violencia, discriminación, explotación o injusticia. Por lo tanto, el primer paso en este camino es el establecimiento de un marco normativo y ético que regule el uso y el desarrollo de estas tecnologías, y que se promueva una educación digital que forme a los usuarios en el ejercicio responsable y crítico de su ciudadanía digital. De esta manera, se podrá aprovechar el potencial de los nuevos emprendimientos tecnológicos, sin renunciar al respeto y la protección de los derechos humanos en el ciberespacio.

Referencias

Alamillo, J. R., & Clemente, C. D. M. (2022). Peritaje informático, análisis forense digital y respuesta a incidentes. Revista de Unidades de Información, (19).

Asamblea Nacional de la República del Ecuador (2002). Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Ley 67 Registro Oficial Suplemento 557 de 17-abr-2002. Estado: Vigente.

Asamblea Nacional de la República del Ecuador (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459 del 26 de mayo de 2021.

Bolaños, F., & Gómez, C. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. RECIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, (3).

Castillo Barquero, R. (2020). ¿Qué es un perito informático forense? https://repositorio.usam.ac.cr/xmlui/handle/11506/localhost/xmlui/handle/11506/2176.

Castillo, C. (2001). Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información. Universidad de Huelva. https://rabida.uhu.es/dspace/bitstream/handle/10272/1565/b1205654.pdf?sequence=1

Centorame, F. (2021). Investigaciones criminales intrusivas y búsqueda de pruebas a través de "software espías" en la experiencia procesal italiana. Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos, 161-177. Aranzadi Thomson Reuters.

Comisión Europea (2016). Reglamento General de Protección de Datos de la Unión Europea. 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016.

Comisión Europea (s.f). Normas de comercio electrónico en la UE. Configurar el futuro digital de Europa. https://digital-strategy.ec.europa.eu/es/policies/e-commerce-rules-eu.

Díaz, M. A. (2017). Reflexiones en torno a la responsabilidad de las plataformas electrónicas de economía colaborativa. Revista de Estudios Europeos. https://dialnet.unirioja.es/servlet/revista?codigo=2935

Fix-Zamudio, Héctor (2007). Metodología, docencia e investigación jurídicas (Décimo cuarta edición). Editorial Porrúa. Argentina.

Flores, J. M. (2019). Inteligencia artificial y periodismo: diluyendo el impacto de la desinformación y las noticias falsas a través de los bots. Doxa Comunicación, 29, pp. 197-212.

Función Judicial de la República del Ecuador (2014). Reglamento del Sistema Pericial Integral de la Función Judicial. Resolución No. 0402014 del 28 de abril de 2014. Pleno del Consejo de la Judicatura.

Galán, D. R. (2004). La convención de las naciones unidas sobre los contratos de compraventa internacional de mercaderías. Estudios Gerenciales, 20(91), 49-64.

Gómez, M. E. (2019). Emprendimiento de base tecnológica: Un reto por cumplir. Tec Empresarial, 13(2), 33-44.

Guaña, J., & Chipuxi, L. (2023). Impacto de la inteligencia artificial en la ética y la privacidad de los datos. RECIAMUC, 7(1), 923-930.

Jonás, H. (2014). El principio de responsabilidad: ensayo de una ética para la civilización tecnológica. Herder Editorial.

Katz, J. E., & Rice, R. E. (2006). Consecuencias sociales del uso de Internet. Editorial UOC.

López, E. M. (2012). Acoso cibernético o cyberbullying: Acoso con la tecnología electrónica. Pediatría de México, 14(3), 133-146.

Lucena, I. V. (2019). Las Nuevas Tecnologías y su impacto en los Derechos Humanos. Hacia un nuevo enfoque. https://ojs.uv.es/index.php/CEFD/article/view/13035.

Mieles, V. P. (2020). Desafíos éticos de los comunicadores en la era digital. Derechos a la comunicación: ética y competencias del comunicador, 46.

Ministro de Telecomunicaciones y de la Sociedad de la Información de la República de Ecuador (2021). Política de Ciberseguridad 2021. Acuerdo Ministerial 006-2021.

Muela-Molina, C. (2011). La publicidad en Internet: situación actual y tendencias en la comunicación con el consumidor. ER: Revista De Estudios De Comunicación = Komunikazio Ikasketen Aldizkaria, 13(24). https://doi.org/10.1387/zer.3616.

Obando, J (2000). Los contratos electrónicos y digitales. Revista electrónica de derecho informático, (39).

Oficina de Comunicación y Mercadeo (2016). El gran reto ante internet. Tecnológico de Costa Rica. https://www.tec.ac.cr/pensis/articulos/regular-gran-reto-internet.

Ortega, A., & Domenech, J. J. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. Revista de la Facultad de Derecho, (44), 31-73.

Peña, N. (2021). Big data e inteligencia artificial: una aproximación a los desafíos éticos y jurídicos de su implementación en las administraciones tributaria. IUS ET SCIENTIA, 7(1), 62-84.

Pérez Escobar, J. (2010). Metodología y Técnica de la Investigación Jurídica. Editorial Temis. Bogotá.

Porcelli, A. M. (2020). La inteligencia artificial y la robótica: sus dilemas sociales, éticos y jurídicos. Derecho global. Estudios sobre derecho y justicia, 6(16), 49-105.

Quiroz, J. J., & Quiroz, D. L. Z. (2021). Informática forense–el caos de la manipulación de la información digital. Suplemento CICA, multidisciplinario N: 011-2021.

Rebaza, L., Demichelli, F., & Silva, A. (2017). Asesoría legal prepagada. Universidad Peruana de Ciencias Aplicadas (UPC). Retrieved from http://hdl.handle.net/10757/622708.

Riofrío, J. C. (2014). La cuarta ola de derechos humanos: Los derechos digitales. Revista latinoamericana de derechos humanos, 25(1).

Rodríguez, G. (2012). Riesgos del consumidor electrónico en las prácticas publicitarias. Revista de derecho, (37), 254-282.

Rodríguez, T. C., Flores, P. I., Vásquez, A. P., & Toala, F. P. (2022). Peritaje digital y delito informático. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 4(5), 22-30.

Rosales, M. R., & Molestina, T. R. (2000). El comercio electrónico en Ecuador: régimen jurídico y comentarios. Iuris Dictio, 1(2).

Sampaoli, J. (2018). Peritaje informático: marco teórico-practico. Universidad Católica Argentina. Facultad de Química e Ingeniería "Fray Rogelio Bacon".

Sánchez, J. I. (2014). Seguridad y privacidad en comunicaciones inalámbricas personales. Tesis Doctoral. Universidad Nacional de Educación a Distancia. Escuela Técnica Superior de Ingenieros Informáticos. Departamento de Informática y Automática.

Torres, M. L. (2017). Entre el espionaje y la colaboración con la justicia:(geolocalización y retención de datos personales por mandato de autoridad). Tesis de Maestría. Universidad de Michoacán. Facultad de Derecho y Ciencias Sociales. Maestría en Derecho de la Información