

DERECHO Y PODER



REVISTA JURÍDICA DE LA FACULTAD DE DERECHO Y CIENCIAS
POLÍTICAS DE LA UNIVERSIDAD PRIVADA ANTONOR ORREGO

-
- A glowing, stylized image of the scales of justice, centered on the lower half of the cover. The scales are illuminated with a bright blue light, creating a strong contrast with the dark blue background. The background is filled with out-of-focus light points (bokeh) and faint, glowing lines, giving it a modern, digital feel.
- DERECHO PENAL
 - DELITOS INFORMÁTICOS
 - DERECHO LABORAL
 - DERECHO CONSTITUCIONAL
 - DERECHO CIVIL



DERECHO Y PODER

REVISTA JURÍDICA DE LA FACULTAD DE DERECHO Y CIENCIAS
POLÍTICAS DE LA UNIVERSIDAD PRIVADA ANTONOR ORREGO

AUTORIDADES UNIVERSITARIAS

RECTORA
DRA. FELÍCITA YOLANDA PERALTA CHÁVEZ

VICERRECTOR ACADÉMICO
DR. LUIS ANTONIO CERNA BAZÁN

VICERRECTOR DE INVESTIGACIÓN
DR. JULIO LUIS CHANG LAM

DECANO DE LA FACULTAD DE
DERECHO Y CIENCIAS POLÍTICAS
DR. RAÚL YVÁN LOZANO PERALTA

DERECHO Y PODER

REVISTA JURÍDICA DE LA FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS DE LA UNIVERSIDAD PRIVADA ANTENOR ORREGO



DIRECTOR

Dr. Segundo Edwin Cieza Mostacero
Universidad Privada Antenor Orrego - Perú
sciezam1@upao.edu.pe

EDITOR

Dr. Henry Armando Carbajal Sanchez
Universidad Privada Antenor Orrego - Perú
hcarbajals@upao.edu.pe

COMITÉ EDITORIAL

Dra. Claudia Elena Mori Ugarte
Universidad Privada Antenor Orrego - Perú
cmoriu1@upao.edu.pe

Dr. Carlos Guillermo Hakansson Nieto
Universidad Privada de Piura - Perú
carlos.hakansson@udep.edu.pe

Dr. Héctor Elvis Martínez Flores
Universidad Nacional Mayor de San Marcos - Perú
hmartinez@unmsm.edu.pe

Dr. Francisco Rogger Carruitero Lecca
Universidad Nacional Mayor de San Marcos - Perú
fcarruiterol@unmsm.edu.pe

Dr. José Felix Palomino Manchego
Universidad Nacional Mayor de San Marcos - Perú
jpalominom@unmsm.edu.pe

Ms. Pedro Paulino Grández Castro
Pontificia Universidad Católica del Perú
pgrandez@pucp.pe

Dr. Omar Alberto Sar Suarez
Universidad San Martín de Porres - Perú
osars@usmp.pe

Dr. Carlos Fernando Mesía Ramírez
Universidad San Martín de Porres - Perú
cmesiar@usmp.pe

Dr. Julio Francisco Villarreal
Universidad de Buenos Aires – Argentina
juliovillarreal@derecho.uba.ar

**Derecho y Poder, revista académica
interdisciplinaria de información
e investigación jurídica.**

ISSN N° 3028-9254

Depósito legal en la Biblioteca

Nacional del Perú N° 2023-12832

Vol. 3, Enero - Diciembre 2025, Trujillo Perú

Publicación anual

Título abreviado: DeryPod.

Dirección

UNIVERSIDAD PRIVADA ANTENOR ORREGO

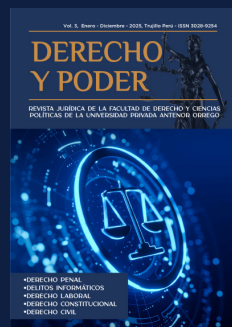
Av. América Sur N° 3145

Urb. Monserrate, Trujillo, Perú

Teléfono: 51-44-604444, anexo 2087

www.upao.edu.pe

Los artículos de esta revista expresan el
pensamiento personal de sus autores,
no de la institución.



Preprensa

Fondo Editorial UPAO

Diagramación: Jorge Arévalo

ÍNDICE

SEXTING: USO DE INTERNET, VIOLACIÓN DE LA PRIVACIDAD, RIESGOS Y EL ROL DEL CONTROL PARENTAL <i>Geraldine E. Cáceres-Córdova</i>	7
EL TELETRABAJO EN LATINOAMÉRICA <i>Marco A. Chávez- Argomedeo</i>	35
EL HACKEO Y LA CIBERSEGURIDAD EN LA LEGISLACIÓN PERUANA: ANÁLISIS NORMATIVO Y DESAFÍOS FRENTE A LAS AMENAZAS DIGITALES <i>Leandro N. Delgado-Palacios</i>	55
IMPACTOS DE LOS MEDIOS DIGITALES Y EL MARCO LEGAL DE LOS DERECHOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD <i>Brenda Falcón-Alcántara</i>	81
IMPACTO DE LA TECNOLOGÍA EN LA ADMINISTRACIÓN DE JUSTICIA <i>Sofía L. Dionicio-Moreno, Brisa P. Montoya- Ramos, Yanella L. Navarro-Chira, Kiara M. Rivera-Vasquez, Aileen C. Saldaña- Ramírez, Y Kiara C. Tapia-Alzamora</i>	107
EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO: DESAFÍOS E IMPLICACIONES ÉTICAS <i>Víctor J. Flores-Ríos</i>	133

**TELETRABAJO POST PANDEMIA Y
SUS IMPLICANCIAS EN EL SECTOR
LABORAL INTERNACIONAL**

159

Hubert J. Fernández-Arroyo

**EL DESTINO DE LOS BIENES
DIGITALES POST MORTEM**

179

Angie F. Fernández-Silva

**VACÍOS JURÍDICOS EN LAS NORMATIVAS
LATINOAMERICANAS QUE REGULAN
EL TELETRABAJO: SALUD MENTAL
Y POSIBLES RIESGOS LABORALES**

203

Ana Lucía Gil-Morey

**TELETRABAJO Y SALUD
LABORAL: RIESGOS FÍSICOS,
PSICOSOCIALES E IMPACTO EN
EL DESEMPEÑO Y BIENESTAR**

221

Claudia F. Lozano-Arteaga

**SOMBRAS DIGITALES: EL
CIBERCRIMEN Y SU AFECTACIÓN EN LA
CIBERSEGURIDAD INTERNACIONAL**

247

Luhana V. Rodríguez-Ramos

**EL DERECHO A LA PRIVACIDAD
Y PROTECCIÓN DE DATOS EN LA
SOCIEDAD DE INFORMACIÓN DIGITAL**

267

Ibeth Nayeli Vargas Reyna

EDITORIAL

La tercera edición de *Derecho y Poder*, revista jurídica, se presenta como un espacio esencial para la reflexión sobre los nuevos desafíos que enfrenta el Derecho Público y Derecho Privado. En un escenario donde la tecnología redefine no solo la dinámica social sino también las estructuras institucionales, resulta urgente examinar como estos cambios afectan al funcionamiento del estado y, en particular, la administración de Justicia. Desde, la incorporación de herramientas de Inteligencia artificial en los Sistemas Judiciales, hasta la expansión de Teletrabajo y sus efectos en la Salud Mental, esta edición busca promover un debate informado, crítico y humanista sobre la necesidad de adaptar el derecho público a las nuevas realidades tecnológicas.

En este número se han reunido investigaciones que, por su finalidad, son básicas. Y en su gran mayoría, debido a su enfoque y profundidad, son de carácter descriptivo, pues examinan la integración de tecnologías disruptivas en los procesos judiciales, el impacto de la digitalización en el servicio público y los crecientes riesgos asociados a la ciberseguridad, así como las amenazas digitales que enfrentan tanto las instituciones como la ciudadanía. Además, la revista reflexiona sobre cómo estos cambios exigen una revisión de los estándares de transparencia estatal, la protección de datos personales y las salvaguardias que protegen los derechos fundamentales en contextos altamente tecnológicos.

En este sentido, la revista promueve una perspectiva crítica que, si bien reconoce el notable progreso alcanzado en la innovación pública, también reconoce la necesidad de fortalecer los marcos regulatorios y las capacidades institucionales para abordar los nuevos riesgos. Enfatiza a su vez, que la modernización digital debiera ir acompañada de políticas responsables, capacitación adecuada y una comprensión integral de los efectos psicosociales; que prácticas como el teletrabajo pueden generar para los funcionarios públicos y las profesionales del derecho punto.

Así mismo, los artículos de esta edición abordan perspectivas tanto teóricas como propuestas prácticas dirigidas a promover un equilibrio entre la eficiencia tecnológica y la protección de los derechos. Análisis que va más allá de la mera enumeración de problemas, sino que también presenta alternativas regulatorias, mejores prácticas comparativas y experiencias aplicadas que demuestran el compromiso de *Derecho y Poder* con la búsqueda de soluciones que respondan a los desafíos de la era digital.

Cabe destacar que *Derecho y Poder*, a partir de la tercera edición, consolida su calendario de publicación anual, manteniendo un riguroso proceso de selección tanto como evaluación de artículos, que garantiza la calidad académica y su alineación con los estándares internacionales; contenido que fortalecerá su impacto y le permitirá contribuir de manera sostenible al debate jurídico contemporáneo.

Finalmente, se extiende una cordial invitación a los estudiantes y docentes del Programa de Estudio de Derecho de la Universidad Privada Antenor Orrego, así como a sus homólogos en Perú, América Latina y el mundo, a sumarse a este espacio de divulgación científica. Además, es importante resaltar que esta iniciativa es el resultado del compromiso académico y valioso aporte de diversos investigadores cuyos esfuerzos y dedicación han sido fundamentales para la culminación de esta edición.

Dr. Segundo Edwin Cieza Mostacero
Director

SEXTING: USO DE INTERNET, VIOLACIÓN DE LA PRIVACIDAD, RIESGOS Y EL ROL DEL CONTROL PARENTAL

Geraldine E. Cáceres-Córdova¹

RESUMEN:

El presente estudio analizó el fenómeno del sexting como una práctica digital en expansión que, aunque puede ser consensuada, plantea riesgos significativos relacionados con la violación de la privacidad, delitos informáticos y afectaciones psicológicas; se abordaron las implicaciones legales y sociales de esta práctica, destacando la vulnerabilidad de adolescentes y jóvenes ante la difusión no autorizada de contenido íntimo; además, se identifican factores de riesgo como el desconocimiento de las consecuencias, la falta de supervisión parental y la presión social; la investigación subrayó la importancia de la educación digital y las estrategias de control parental para mitigar los riesgos y promover el uso seguro de las tecnologías; se concluyó que existe la necesidad de un enfoque integral que combine la alfabetización digital, la prevención y la protección para reducir los impactos negativos del sexting en la sociedad.

Palabras Clave: Sexting, privacidad digital, delitos informáticos, control parental, educación digital, ciberseguridad, adolescentes, riesgos en línea, pornografía no consentida, extorsión sexual.

¹ Gcacerescl@upao.edu.pe

Programa de estudio de Derecho, Universidad Privada Antenor Orrego

ABSTRACT

The present study analyzed the phenomenon of sexting as an expanding digital practice that, although it may be consensual, poses significant risks related to the violation of privacy, computer crimes and psychological effects; The legal and social implications of this practice are addressed, highlighting the vulnerability of adolescents and young people to the unauthorized dissemination of intimate content; In addition, risk factors are identified such as ignorance of the consequences, lack of parental supervision and social pressure; The research highlights the importance of digital education and parental control strategies to mitigate risks and promote the safe use of technologies; It was concluded that there is a need for a comprehensive approach that combines digital literacy, prevention and protection to reduce the negative impacts of sexting on society.

INTRODUCCIÓN

A pesar de que en muchos casos el sexting ocurre de forma consensuada, su práctica ha dado lugar a diversos problemas sociales y legales, especialmente cuando se transforma en un vínculo para la violación de la privacidad de las personas, originando delitos informáticos; en este sentido, puede derivar graves vulneraciones a los derechos fundamentales, como el derecho a la intimidad y la protección de los datos personales.

El sexting ha proliferado entre adolescentes y adultos jóvenes, convirtiéndose en una forma de expresión sexual en el entorno digital, no obstante, este acontecimiento ha sido aprovechado por ciberdelincuentes para cometer delitos que atentan contra la privacidad de las personas, por otro lado Microsoft con ICD el cual mide la exposición de riesgos registrando contacto no deseado, engaños, fraude, estafas y sexting no deseado (CONAPOC, 2020).

Una vez que este tipo de contenido es compartido, ya sea de manera voluntaria o no, su control es prácticamente inexistente, lo que puede derivar en delitos como la pornografía no consentida, conocida comúnmente como porno venganza o extorsión sexual lo cual origina muchos problemas legales que normalmente terminan en casos de denuncias u otros tipos penales que generan daños en la población normalmente entre jóvenes.

Uno de los principales delitos derivados del Sexting es la violación del derecho a la privacidad, un derecho fundamental protegido por múltiples normativas nacionales e internacionales, en Perú, el código penal incluye disposiciones específicas que sancionan la violación de la

intimidad, especialmente cuando se difunde su formación privada sin el consentimiento de la persona afectada.

Sin embargo, la legislación peruana, en el artículo 6 de tráfico ilegal de datos sobre utilizar indebidamente los datos de una persona, crea una medida para sancionar estos actos, no obstante debido a que muchas personas, en especial adolescentes, desconocen los riesgos y las consecuencias legales que implican el sexting, frente a esta problemática, la solución requiere un enfoque integral que combine educación, prevención y protección; en el ámbito preventivo, es crucial la alfabetización digital (Ley de delitos informáticos, 2013).

La ley Nro. 30096, Ley de delitos informáticos, contempla sanciones para quienes accedan de manera indebida a sistemas informáticos o difundan información privada, incluidas imágenes íntimas obtenidas mediante sexting como en eso de la República del Perú 2013, este tipo de conductas puede conllevar pena de hasta cinco años de prisión si se demuestra la violación del derecho a la intimidad o el uso individual de datos personales.

Este desconocimiento coloca al Perú en una situación de vulnerabilidad, especialmente frente a situaciones de acoso, extorsión o exposición pública, prácticas que afectan gravemente su bienestar emocional y su integridad, el impacto social de la distribución no consentida de imágenes sexuales es devastador.

En términos preventivos se debe promover educación digital y alfabetización en Ciberseguridad con especial énfasis en los jóvenes, debido a que estos se involucran en estos actos ya sea razones por problemas de identidad sexual, tener una autoestima deficiente y que se perciben socialmente discriminados, a lo cual al intentar sobresalir e impresionar a otro con una prueba de amor llegan en internet a suplir sus pensamientos sobre el sexo (Tavares et al., 2019).

Para abordar estas problemáticas, este trabajo se propuso examinar la influencia del uso de internet en la práctica del sexting, analizar la violación del derecho a la privacidad y su relación con delitos informáticos, identificar los factores de riesgo y las consecuencias del sexting, y analizar estrategias de control parental efectivas. Estos objetivos permitirán una comprensión integral del fenómeno y contribuirán al desarrollo de medidas más efectivas para prevenir y mitigar los impactos negativos asociados al sexting en nuestra sociedad.

METODOLOGÍA

Esta investigación tuvo un enfoque cualitativo con el fin de lograr un acercamiento al tema del sexting como problema base por el acceso a la información sin la supervisión necesaria y como consecuencia innumerable delitos informático; además el tipo de investigación fue básica debido a que se caracteriza en incrementar los conocimientos científicos pero sin usar aspectos prácticos (Gabriel-Ortega, 2017) y el diseño de investigación fue no experimental- descriptivo (Ponce et al., 2018). La técnica se limitó a la revisión bibliográfica de diferentes artículos científicos y, marcando los puntos más relevantes como los factores de riesgo del sexting y las consecuencias de cada uno de ellos, que para su análisis se necesito de un enfoque deductivo con un tipo de argumentación ordenando al orden de ideas de forma prevalente.

El diseño metodológico fue no experimental y descriptivo, lo que significa que no se manipularon variables ni se realizaron intervenciones en el objeto de estudio. En su lugar, se buscó describir las características del sexting, los riesgos asociados, y la influencia del control parental, siguiendo un enfoque basado en la observación de información secundaria y la identificación de patrones relevantes.

El desarrollo del análisis siguió un esquema temático definido, se examinó cómo los hábitos de uso de internet influyen en la práctica del sexting y su origen como fenómeno social, se investigó cómo esta actividad puede vulnerar el derecho a la privacidad y su conexión con delitos informáticos, como la difusión no consentida de imágenes íntimas, finalmente se identificaron los factores de riesgo y las consecuencias que esta práctica tiene entre adolescentes y jóvenes adultos.

Este enfoque metodológico permitió abordar el fenómeno desde distintas perspectivas, proporcionando una visión integral que combina los aspectos sociales, legales y familiares relacionados con el sexting y su impacto en la privacidad. Por último, se exploró la influencia del control parental en la prevención y manejo del sexting, identificando estrategias que pueden mitigar los riesgos asociados a este comportamiento.

RESULTADOS

Influencia del uso de internet en la práctica del sexting

Según Rodríguez-Otero & Cerros-Rodríguez (2021) destacan al sexting, como la recepción y envío de contenido erótico-sexual mediante dispositivos digitales, por ejemplo se ha convertido en una práctica común entre los estudiantes universitarios en Nuevo León y Jalisco; los datos muestran que un 79.5% de los participantes realiza sexting pasivo y un 53.6% participa en sexting activo, este fenómeno es facilitado por el acceso extendido al internet y a redes sociales, que permite que la interacción íntima cobre nuevas formas, caracterizadas por la rapidez y el anonimato.

El uso generalizado de internet y redes sociales ha transformado las prácticas de interacción entre adolescentes, quienes encuentran en estas plataformas un medio propicio para compartir aspectos de su intimidad, el fenómeno de extimidad que se refiere a las conductas de exhibición de lo más íntimo genera que mediante estas redes sociales los adolescentes puedan desembocar en prácticas como el sexting debido a la necesidad de exhibirse y hablar de sí mismo para que el mundo vea (Narvaja & De Piero, 2016)

El sexting se ha convertido en una práctica común entre los adolescentes, potenciado por el acceso a dispositivos móviles y redes sociales. En el estudio realizado en adolescentes de Argentina por Resett (2019), se identificó que el 21.5% había enviado algún tipo de contenido sexual al menos en una ocasión. Esta prevalencia fue mayor en el envío de mensajes de texto con contenido sexual (18%) y en el envío de fotos (17.6%), mientras que el envío de videos fue menos frecuente (6.9%). Esta conducta ha sido vinculada con la popularización de las tecnologías de información y comunicación, lo cual facilita un contexto en el que los jóvenes pueden interactuar de forma inmediata y sin restricciones aparentes.

El uso extendido de dispositivos móviles ha facilitado la práctica del sexting, especialmente entre jóvenes universitarios que buscan nuevas formas de expresar su intimidad. Estudios recientes señalan que el sexting, o el envío de contenido sexual a través de medios digitales, se encuentra presente en ambos sexos, aunque los hombres participan en mayor medida. En el análisis de la Universidad de Granada, casi el 41.57% de los hombres y el 34.47% de las mujeres reportaron haberse involucrado en esta práctica en algún momento (Chacón-López et al., 2019).

Por otro lado, según Rodríguez-Otero & Cerros-Rodríguez (2021) las situaciones de vulnerabilidad derivadas de la práctica del sexting, específicamente en cuanto a la coacción, el chantaje y las burlas, siendo que un 27.9% de los encuestados menciona haber enfrentado algún tipo de coacción, un 10.8% chantaje y un 4% burlas; estas cifras reflejan cómo el sexting puede ser usado como una herramienta de control o violencia en las relaciones personales, un fenómeno exacerbado por la facilidad de compartir contenido a través de las redes.

La creciente penetración de internet y el comportamiento de producir y enviar o llegar a recibir contenidos sexuales hace que mediante los teléfonos móviles interactúen en entornos digitales de forma intensiva, lo cual ha contribuido a la normalización del sexting. Este término hace referencia al envío o recepción de contenido sexual a través de plataformas digitales, lo cual ha encontrado un terreno fértil en la dinámica social de los adolescentes, quienes buscan expresar y explorar su identidad sexual en un contexto de comunicación inmediata y sin barreras físicas (Tavares et al., 2019).

El sexting tiende a ser más común en los varones, especialmente en el envío de mensajes de texto con contenido sexual, en el cual la prevalencia masculina alcanzó el 23.7%, en comparación con el 10% en mujeres. Esta diferencia entre géneros se relaciona con patrones culturales donde los hombres suelen asumir un rol más activo en la expresión de su sexualidad mediante medios digitales (Resett, 2019), no obstante, la investigación no halló una variación significativa en el envío de fotos y videos entre ambos géneros, lo cual sugiere que, aunque existen diferencias, el sexting no es exclusivo de uno u otro sexo.

Asimismo, la facilidad de compartir contenido íntimo sin supervisión, combinada con la percepción de privacidad que algunos medios digitales otorgan y facilitan que los adolescentes perciban el sexting como una extensión de sus relaciones interpersonales. Sin embargo, este material, creado bajo un supuesto de confianza, queda vulnerable a la difusión no autorizada, amplificando los riesgos de exposición pública y afectando la percepción que los jóvenes tienen sobre su propia intimidad (Narvaja & De Piero, 2016b); de este modo, internet actúa como un catalizador que no solo potencia la comunicación, sino que también redefine la interacción juvenil.

Además, el estudio de Chacón-López et al. (2019) refleja que la participación en sexting aumenta conforme los jóvenes avanzan en edad, alcanzando un

pico a los 20 años y disminuyendo progresivamente a partir de los 21, lo cual podría estar relacionado con una mayor conciencia de los riesgos o una adaptación a nuevas formas de comunicación dentro de las relaciones afectivas; sin embargo, los datos no muestran una relación significativa entre esta práctica y la autoestima de los participantes, sugiriendo que factores sociales y culturales pueden influir más en la inclinación hacia esta conducta que las características individuales de autovaloración.

Diversos estudios, como el de Tavares et al. (2019), subrayan que el uso de redes sociales y aplicaciones de mensajería ha incrementado la exposición de los jóvenes a prácticas de sexting, reforzando además la idea de popularidad o aceptación social. En este sentido, la facilidad de acceso a internet fomenta la interacción constante y la creación de relaciones digitales en las que compartir imágenes o mensajes íntimos es percibido como una forma de conexión emocional o incluso de reafirmación personal.

El sexting ha emergido como una práctica común en la adolescencia, impulsado por el uso intensivo de redes sociales y la accesibilidad de dispositivos móviles. En un estudio cualitativo realizado en adolescentes españoles, se observó que alrededor de un quinto de los participantes admitió haber enviado algún tipo de contenido erótico a través de internet, aunque la percepción general es que el sexting es aún más frecuente entre sus pares (Alonso-Ruido et al., 2018).

La práctica del sexting entre adolescentes se ve influenciada también por una falta de supervisión parental. Algunos padres no monitorean las actividades virtuales de sus hijos de forma adecuada, lo cual permite que estos últimos busquen satisfacción o aprobación en un espacio donde las normas son más difusas. La literatura ha mostrado que el comportamiento de los padres en el ámbito digital puede influir en el uso de internet de los adolescentes, ya sea como modelo a seguir o como consecuencia de una permisividad en el uso de las tecnologías (Tavares et al., 2019).

Esta práctica se justifica principalmente como un acto de exploración de la sexualidad, aunque también es impulsada por el aburrimiento y el deseo de aceptación social. Las chicas parecen participar más en el envío de fotos, mientras que los chicos suelen optar por mensajes de texto, reflejando diferencias en las dinámicas de género dentro de este fenómeno. (Alonso-Ruido et al., 2018).

Por otro lado, existe una correlación entre la edad de los adolescentes y la frecuencia de las prácticas de sexting; los adolescentes mayores,

específicamente aquellos entre 15 y 17 años, reportaron una mayor frecuencia en el envío de mensajes sexuales en comparación con los adolescentes de menor edad (13-14 años), este aumento de participación podría estar asociado con la maduración sexual y un mayor interés en las relaciones románticas propias de la adolescencia media y tardía (Resett, 2019).

El desconocimiento de los riesgos y la falta de supervisión parental aumentan la vulnerabilidad de los adolescentes ante las posibles consecuencias negativas del sexting; aunque muchos adolescentes perciben esta conducta como parte de la normalidad digital, también reconocen que las chicas tienden a sufrir mayores repercusiones sociales, siendo frecuentemente juzgadas con dureza por sus pares, los participantes del estudio revelaron que existen presiones hacia las chicas para involucrarse en el sexting, principalmente por parte de sus parejas o amigos cercanos, lo cual genera un contexto de desigualdad en las relaciones digitales (Alonso-Ruido et al., 2018).

Los resultados obtenidos señalan la relevancia de los factores sociales y tecnológicos en la expansión del sexting, al evidenciar cómo el entorno digital ha modificado la interacción íntima, haciendo posible una rápida difusión de contenido personal, las diferencias en la inclinación hacia esta práctica, asociadas a variables como el género, estado sentimental y creencias, sugieren que el sexting no es uniforme, sino que depende de ciertos contextos culturales y personales.

Los datos sobre los efectos negativos del sexting, como la coacción y el chantaje, revelan la necesidad de establecer sistemas de apoyo y protección para los estudiantes que puedan encontrarse en situaciones vulnerables, la frecuencia de estos problemas destaca la importancia de implementar políticas de prevención que enfoquen la educación en torno al respeto a la privacidad y a las repercusiones legales y emocionales del sexting, además, el uso del sexting en relaciones de pareja como medio de control subraya la necesidad de incluir este tema en los programas de educación sobre relaciones sanas (Rodríguez-Otero & Cerros-Rodríguez, 2021).

Se sugiere en los resultados que el acceso y uso extendido de internet han creado un entorno propicio para el sexting en la adolescencia, configurando un nuevo reto tanto para los jóvenes como para sus familias. Es evidente que el papel de los padres es fundamental para establecer límites y educar en el uso responsable de las tecnologías; sin embargo, la falta de comunicación

efectiva y de un monitoreo equilibrado ha propiciado que los adolescentes se sientan incentivados a participar en estas prácticas (Tavares et al., 2019).

Los resultados sugieren que la práctica del sexting responde a un complejo entramado de búsqueda de identidad y visibilidad en el entorno digital. Los jóvenes ven en estas plataformas un medio para expresarse, aunque sin medir completamente las consecuencias de la exposición. La literatura coincide en que el fenómeno del sexting se enmarca en la cultura de la “extimidad”, donde la exhibición pública de lo íntimo se convierte en una herramienta de validación social, lo cual resalta la importancia de un control parental informado y una educación digital consciente para mitigar los riesgos asociados (Narvaja & Alonso, 2022).

En los resultados se confirma que el sexting se ha convertido en una práctica común entre los universitarios, sin diferencias notables en relación con la autoestima, pero con una tendencia hacia una mayor participación masculina. Esta diferencia puede reflejar una presión social sobre los hombres para involucrarse en este tipo de interacciones, como indican estudios recientes, la exposición constante a redes y dispositivos móviles crea una cultura de conectividad que facilita esta forma de comunicación íntima, lo cual destaca la necesidad de implementar estrategias educativas que promuevan el uso seguro y consciente de la tecnología, especialmente entre jóvenes adultos (Chacón-López et al., 2019).

Se destaca que el sexting en adolescentes puede responder tanto a factores de desarrollo como a influencias sociales y tecnológicas, sugiriendo que la maduración emocional y el contexto cultural juegan un rol importante en esta conducta. La mayor prevalencia en adolescentes de mayor edad y en varones señala la necesidad de implementar estrategias de prevención que consideren estas diferencias de género y etapas del desarrollo, el contexto digital facilita un entorno donde las conductas de sexting se vuelven parte de la vida social adolescente, evidenciando la importancia de orientar a los jóvenes sobre los riesgos y consecuencias de la difusión de contenido íntimo (Resett, 2019).

Violación del derecho a la privacidad y su relación con delitos informáticos

El sexting, al involucrar la creación y envío de material íntimo, ha aumentado los riesgos de violación de la privacidad, especialmente en entornos donde la falta de control sobre el contenido digital es evidente,

según Agustina & Gómez-Duran (2016), uno de los principales problemas es que los usuarios, al compartir material de carácter sexual, suelen desconocer las posibles consecuencias de su difusión; esta conducta puede llevar a una pérdida del control sobre el contenido, exponiendo a los individuos a situaciones de ciber victimización, tales como chantaje, acoso o extorsión.

El entorno digital ha transformado la privacidad en un bien particularmente vulnerable, especialmente para los jóvenes, quienes suelen participar activamente en redes sociales y otras plataformas de interacción en línea según Montiel (2016) señaló que este contexto digital actúa como un espacio de socialización y, simultáneamente, como un espacio de oportunidad criminal. Los adolescentes, al compartir datos personales y contenido íntimo en línea, se exponen a riesgos de ciber victimización, como el ciberacoso y el grooming online, que ponen en peligro su integridad y privacidad.

El incremento en el uso de internet y redes sociales ha creado un contexto donde los derechos a la privacidad de los usuarios se ven frecuentemente vulnerados, dando pie a una serie de nuevos delitos informáticos según (Pifarré, 2013) expuso que este entorno digital permite una interacción sin precedentes que acerca a usuarios y contenidos de forma instantánea, facilitando que la información personal se comparta a una escala global. La autora destaca cómo el anonimato y la facilidad de acceso a los datos en redes sociales convierten a los usuarios en blanco fácil para actividades criminales.

En la III Jornada de Criminología organizada por la Universidad Oberta de Catalunya, se abordó el aumento de los ciberdelitos que afectan la privacidad, especialmente entre jóvenes, según Tamarit (2013), el uso constante de tecnologías digitales ha facilitado la aparición de nuevos riesgos en línea, como el ciberacoso y la divulgación de contenido íntimo sin consentimiento, ambas violaciones serias a la privacidad. Los jóvenes, al compartir datos personales en plataformas digitales, quedan particularmente expuestos, debido a que en muchos casos no son plenamente conscientes de los riesgos asociados.

Se evidencia que el uso de internet sin supervisión contribuyó significativamente al aumento de la práctica del sexting entre adolescentes y jóvenes adultos, en muchos casos, los participantes compartieron contenido íntimo en un contexto privado, pero este material fue posteriormente

distribuido sin su consentimiento, lo que ocasionó serias violaciones de la privacidad (Walker et al., 2019).

El acoso y la divulgación de datos sin consentimiento, que en el mundo físico requieren de proximidad y riesgo, en la red encuentran una plataforma segura para los delincuentes, quienes se aprovechan de la falta de control sobre el contenido compartido lo cual genera una problemática sobre también lo que desarrolla en el sexting (Pifarré, 2013).

Es importante una mayor sensibilización y educación en materia de privacidad digital Tamarit (2013) destacó que una de las formas más efectivas de prevención es educar a los jóvenes y sus familias sobre los riesgos de compartir información personal en línea y sobre la importancia de mantener el control sobre su privacidad, la cooperación entre instituciones educativas y organismos de seguridad es esencial para construir una cultura digital de responsabilidad y para crear conciencia sobre los efectos duraderos que una violación de la privacidad puede tener en la vida de una persona.

La exposición pública de estos contenidos derivó en problemas psicológicos, como ansiedad, depresión y acoso cibernético, además de riesgos legales relacionados con la distribución de pornografía infantil en situaciones que involucraron menores de edad son una gran problemática en la sociedad lo que también vulnera la violación al derecho a la privacidad (Döring, 2014).

La vulnerabilidad es mayor en contextos donde la supervisión es limitada y la conciencia sobre la privacidad digital es escasa. La tendencia de los jóvenes a no considerar los riesgos al compartir contenido íntimo agrava esta situación, lo cual subraya la necesidad de implementar estrategias educativas que fortalezcan la cultura de la privacidad y el respeto a los derechos individuales en la red (Agustina & Gómez-Duran, 2016).

Se evidenció las dificultades para enfrentar estos delitos debido a la falta de denuncias y a los obstáculos técnicos para recolectar pruebas en un entorno digital, Tamarit (2013) resaltó que la naturaleza virtual de estos delitos complica la identificación de los responsables y la recolección de evidencia suficiente para llevarlos ante la justicia, esto revela la necesidad urgente de fortalecer las estrategias de persecución legal y los protocolos de seguridad en internet, lo que podría reducir la cifra negra de ciberdelitos. Además, la colaboración entre fuerzas policiales y expertos en tecnología es crucial para diseñar métodos efectivos.

La falta de denuncias y la complejidad técnica para demostrar el componente cibernético de estos delitos contribuyen a una cifra negra significativa, es decir, la cantidad de crímenes no registrados en las estadísticas oficiales: según los datos recogidos por Montiel (2016), apenas un 4.5% de las ciber víctimas en España corresponde a menores, pese a que estudios autorrevelados de ciber victimización indican tasas mucho más altas de agresiones en línea; Este fenómeno de invisibilidad no solo afecta a la percepción social de la cibercriminalidad juvenil, sino que también refuerza el sentimiento de impunidad.

La naturaleza transnacional de internet complica la protección de la privacidad, puesto que las leyes nacionales pueden no ser suficientes para frenar estos delitos en un espacio digital sin fronteras: al respecto, Pifarré (2013) sugirió que la rápida evolución de las plataformas digitales dificulta que las legislaciones se adapten con celeridad a las nuevas formas de delito. Esto se traduce en una proliferación de conductas delictivas relacionadas con la privacidad, como la divulgación no autorizada de imágenes íntimas, que afectan a un creciente número de usuarios.

El intercambio de contenido íntimo entre adolescentes en espacios digitales presenta serios riesgos para el derecho a la privacidad, aunque en muchos casos el material se comparte de forma voluntaria, el entorno digital facilita su circulación sin permiso, lo que puede desencadenar actos de ciber violencia, como la pornovenganza o el ciberacoso, estas prácticas se asocian directamente con delitos informáticos y la distribución no consentida de imágenes íntimas vulnera tanto la privacidad, como el bienestar de las personas afectadas (Narvaja & Alonso, 2022).

La exposición de información privada en el ciberespacio facilita que terceros malintencionados accedan y exploten esta información para cometer delitos informáticos, generando un ciclo de vulnerabilidad en el que los jóvenes se convierten tanto en víctimas como en agentes de cibercrímenes lo que desencadena en conflictos legales y que estos llegan a incrementar la carga procesal de investigación en los países (Montiel, 2016).

La relación entre sexting y delitos informáticos es cada vez más notable, existe la posibilidad de que estas prácticas facilitan que terceros malintencionados tengan acceso a material privado, el cual puede ser utilizado sin el consentimiento del propietario para actividades ilegales. Agustina & Gómez-Duran (2016) destacaron que el sexting puede ser

el umbral para múltiples formas de victimización digital, donde los delincuentes se aprovechan de la confianza depositada por los usuarios; estas conductas no solo violan la privacidad de los involucrados, sino que además representan un riesgo legal y emocional que puede tener consecuencias graves a largo plazo.

Se destaca la disparidad entre la frecuencia de delitos informáticos reportados y la gravedad que perciben las víctimas, particularmente en casos donde el ciberacoso y la violación de la privacidad pueden ser percibidos como “juegos” o actos sin mayores consecuencias, esta trivialización de la ciber victimización, especialmente en contextos de juventud, tiende a inhibir la denuncia y a normalizar comportamientos que pueden escalar a delitos más serios, como la sextorsión y el chantaje a partir de imágenes íntimas (Montiel, 2016).

Los resultados muestran la importancia de contar con un marco legal sólido y políticas preventivas orientadas a la protección de la privacidad digital, especialmente entre adolescentes, la difusión no autorizada de contenido íntimo revela la conexión entre la vulneración de derechos de privacidad y el incremento de delitos informáticos, lo que transforma el espacio virtual en un lugar de posible exposición no solo emocional, sino también legal, ante situaciones de pornovenganza y ciberacoso, se plantea la necesidad de una respuesta integral que incluya educación en derechos digitales.

Así también la sensibilización sobre los riesgos y responsabilidades en el uso de la privacidad en línea y respaldo jurídico para quienes son víctimas de ciberviolencia, la educación en el uso responsable de la tecnología y la intervención temprana desde el ámbito escolar y familiar son esenciales para reducir el impacto de estos delitos y preservar la seguridad de los jóvenes en el ámbito digital (Narvaja & Alonso, 2022).

El sexting no solo implica la violación de la privacidad personal, sino que también abre las puertas a diversos delitos informáticos, como el ciberacoso y la sextorsión. La falta de conocimiento sobre la seguridad digital y la exposición constante en redes sociales incrementan el riesgo de que los jóvenes se vean afectados. Por lo tanto, es fundamental promover una educación digital que enfatice la importancia de proteger la privacidad en línea y desarrolle estrategias preventivas para mitigar las amenazas relacionadas con el uso irresponsable de tecnologías de la información (Agustina y Gómez-Durán, 2016).

Es crucial también que los esfuerzos preventivos se enfoquen en la educación digital de jóvenes y adultos, promoviendo la importancia de una gestión cuidadosa de la información personal en línea; la integración de programas educativos sobre seguridad digital en las instituciones, en colaboración con organismos de seguridad y expertos en tecnología, podría reducir la incidencia de estos delitos y reforzar la conciencia sobre los riesgos asociados al uso irresponsable de las redes, queda claro que solo a través de una combinación de estrategias preventivas y punitivas se podrá avanzar en la protección efectiva (Tamarit, 2013).

Los hallazgos muestran que la cibercriminalidad relacionada con la violación de la privacidad entre los jóvenes está marcada por una alta cifra negra y por una percepción de impunidad, la falta de denuncias y el bajo porcentaje de resolución de estos delitos resaltan la necesidad de campañas de sensibilización y de mejoras en el sistema de justicia para abordar de manera efectiva los delitos informáticos juveniles. Montiel Juan (2016), comprender la magnitud de este fenómeno es esencial para implementar medidas preventivas que protejan los derechos de los adolescentes y promuevan una cultura de seguridad digital.

Los hallazgos de Pifarré (2013) subrayan la vulnerabilidad del derecho a la privacidad en el contexto de internet y redes sociales, especialmente ante la falta de un marco legal suficientemente robusto y unificado, la autora sugiere que la respuesta penal es una herramienta fundamental, pero insuficiente si no se implementa en conjunto con políticas de educación digital y un marco de cooperación internacional; la situación actual demanda la formulación de estrategias que aborden de manera integral la seguridad y la privacidad en línea, creando un entorno digital más seguro para los usuarios y minimizando la incidencia de los delitos informáticos en la vida cotidiana.

Los resultados obtenidos destacan la vulnerabilidad de los jóvenes frente a la violación de la privacidad en entornos digitales, subrayando la necesidad de una respuesta estructurada y colaborativa, Tamarit (2013) sugirió que, aunque el sistema penal juega un rol esencial en la sanción de ciberdelitos, esto no es suficiente para enfrentar la complejidad de los riesgos digitales actuales. La falta de denuncias y los desafíos técnicos en la recolección de evidencia son obstáculos significativos que limitan la efectividad de la justicia en estos casos, lo cual acentúa la urgencia de un marco legal más adaptado al entorno virtual.

Factores de riesgos y consecuencias del sexting

El sexting, aunque frecuentemente consensuado, implica riesgos significativos, especialmente entre jóvenes, debido a la posibilidad de que el contenido íntimo sea difundido sin autorización, este riesgo se incrementa con factores como la falta de educación digital, la presión social y el anonimato de las redes, que facilitan el acceso, como la distribución de imágenes privadas, las consecuencias de estas prácticas incluyen daños emocionales, como ansiedad, depresión, y problemas legales, por lo que en algunos casos puede tratarse de material ilegal, afectando la reputación y el bienestar de las personas involucradas (Narvaja, 2019).

La práctica del sexting ha sido reconocida como un comportamiento de riesgo, especialmente entre adolescentes y jóvenes, debido a las implicaciones psicológicas y sociales que puede acarrear el estudio de Chacón-López et al. (2016) resalta que los jóvenes con baja autoestima o dificultades emocionales tienden a involucrarse en el sexting, lo que puede llevar a consecuencias negativas como la ansiedad, la depresión y el aislamiento social. Estos jóvenes perciben el sexting como una forma de autoafirmación o aceptación en su grupo social, sin considerar que la exposición de contenido íntimo.

El sexting se asocia con diversos factores de riesgo que incrementan la vulnerabilidad de los jóvenes frente a la ciber victimización, se evidencia el sexting puede actuar como un umbral hacia formas de victimización como el acoso y el chantaje; una vez compartido, como resultado se genera que el contenido se vuelva difícil de controlar; esto es especialmente preocupante en el caso de adolescentes, quienes pueden no ser plenamente conscientes de las posibles repercusiones (Agustina & Gómez-Duran, 2016).

El sexting en adolescentes está relacionado con la exposición a situaciones de vulnerabilidad y riesgo emocional, el estudio de Rodríguez-Castro et al. (2020) indica que el 52.8% de los adolescentes ha participado en el envío de contenido íntimo, siendo el envío de mensajes eróticos mucho más frecuente que el de fotos o vídeos. Esta práctica aumenta el riesgo de sufrir consecuencias psicológicas y sociales, especialmente cuando el contenido es difundido sin consentimiento, lo cual provoca ansiedad y daña la autoestima del joven.

El sexting se ha convertido en una práctica común entre adolescentes, y su realización voluntaria puede desencadenar problemas emocionales significativos cuando el contenido íntimo se difunde sin consentimiento según Resett (2019) encontró que el sexting aumenta el riesgo de desarrollar síntomas depresivos y de ansiedad, pues las víctimas sienten una pérdida de control sobre su privacidad, lo que afecta su autoestima y genera un ambiente de vulnerabilidad emocional; este impacto emocional puede influir en la salud mental de los adolescentes a largo plazo, incrementando su susceptibilidad a otros problemas psicológicos.

Así mismo el sexting implica un riesgo significativo de ser coaccionado o chantajeado para compartir más contenido íntimo. En el estudio, el 11.6% de los adolescentes reportó haber sido presionado para enviar contenido erótico, y el 5.5% afirmó haber sido chantajeado posteriormente Rodríguez-Castro et al. (2020). Estos comportamientos ejercen una presión psicológica intensa, particularmente sobre las chicas, quienes suelen enfrentar juicios sociales más severos y estigmatización en comparación con sus compañeros varones.

El sexting, aunque percibido por algunos jóvenes como una forma de expresión personal o afectiva, conlleva múltiples riesgos, la falta de control sobre el contenido compartido en línea aumenta la vulnerabilidad de los participantes frente a violaciones de la privacidad y ciberdelitos, la relación entre el sexting y los problemas psicológicos también fue consistente con estudios que reportaron efectos negativos significativos en la salud emocional de las víctimas (Walker et al., 2019).

El fenómeno del sexting en adolescentes ha mostrado tener un impacto significativo en la salud mental y el rendimiento académico, especialmente cuando la privacidad de las imágenes es violada, según Hernández et al. (2022), el sexting puede llevar a consecuencias psicológicas graves, como ansiedad y baja autoestima, cuando el contenido compartido se difunde sin consentimiento. Este tipo de experiencia puede afectar profundamente la percepción personal y la confianza de la víctima, desencadenando un estrés emocional significativo.

Otro factor de riesgo identificado en el estudio es la relación entre el sexting y la victimización en línea, pues muchos jóvenes que comparten contenido íntimo se ven expuestos al cyberbullying y a la manipulación por parte de adultos o compañeros. Resett (2019) resaltó que esta vulnerabilidad no solo afecta la percepción de seguridad en entornos digitales, sino que también

genera un estado de estrés persistente, el cual interfiere con el rendimiento académico y las relaciones interpersonales de los jóvenes afectados.

El sexting puede conducir a situaciones de vulnerabilidad a largo plazo, en las que el contenido compartido se convierte en una herramienta de control o extorsión. En varios casos documentados, las imágenes y mensajes íntimos terminan en manos de terceros, lo que aumenta el riesgo de ser víctimas de acoso o chantaje. Esta difusión no autorizada afecta considerablemente la reputación y el bienestar emocional de los jóvenes involucrados, quienes experimentan sentimientos de vergüenza, ansiedad y pérdida de control sobre su intimidad (Chacón-López et al., 2016).

Los bajos niveles de privacidad y modestia se identificaron como factores que contribuyen a una mayor predisposición hacia el sexting, según (Agustina & Gómez-Duran, 2016), los jóvenes con actitudes permisivas hacia la exposición personal en redes sociales y con una tendencia a normalizar la pornografía presentan tasas más altas de involucrarse en el envío de contenido íntimo. Esta actitud hacia el sexting no sólo los expone a riesgos, sino que también fomenta un ambiente en el que este tipo de prácticas se perciben como aceptables y sin consecuencias graves.

Además, el estudio señala que los adolescentes que practican sexting son más propensos a involucrarse en conductas de riesgo, como interacciones con adultos en línea, lo que aumenta la posibilidad de grooming y otros tipos de acoso digital. Según Resett (2019), estos comportamientos de riesgo están asociados con un bajo nivel de autocontrol y una menor conciencia sobre los riesgos que implica compartir contenido íntimo en plataformas digitales además de el poco manejo que los padres de los menores de edad en algunos casos ejercen de para los mismos, con el cuidado de los sitios web que visitan.

Además, el estudio de Hernández et al. (2022) indicó que las víctimas de sexting experimentan síntomas de estrés académico, manifestado en dificultades de concentración y una disminución notable en su rendimiento académico. Estos efectos se ven agravados cuando los adolescentes enfrentan acoso psicológico de sus compañeros, quienes a menudo juzgan y estigmatizan a las víctimas, creando un ambiente escolar hostil que limita su interacción social y su desempeño académico.

Desde una perspectiva jurídica, los riesgos asociados al sexting exigen una revisión exhaustiva de los marcos legales actuales para garantizar

una protección adecuada a las víctimas y sancionar con firmeza a quienes transgreden la privacidad digital, la regulación de estas prácticas necesita de un enfoque integral, que contemple tanto la prevención mediante la educación digital como el establecimiento de normativas claras y específicas que penalicen la difusión no autorizada de contenido íntimo, la adecuación del derecho a estas realidades contemporáneas permitirá no solo brindar protección y justicia a las víctimas sino prevenir futuros incidentes (Narvaja, 2019).

El entorno familiar también juega un papel crucial en la resiliencia frente a los efectos del sexting, la investigación de Hernández et al. (2022) mostró que una comunicación abierta y un apoyo emocional sólido en el hogar pueden ayudar a mitigar el impacto del estrés generado por el sexting. Sin embargo, cuando las relaciones familiares son tensas o faltan estrategias de afrontamiento adecuadas, los adolescentes afectados pueden experimentar sentimientos de aislamiento y desesperanza, aumentando su vulnerabilidad a trastornos emocionales.

Otro hallazgo relevante es la correlación entre la falta de supervisión parental y el aumento en la prevalencia del sexting entre los adolescentes, (Agustina & Gómez-Duran, 2016) destacaron que la supervisión y la comunicación adecuada en el entorno familiar pueden actuar como factores de protección, pues ayudan a los jóvenes a entender los límites y las consecuencias de sus acciones en entornos digitales.

Otro factor de riesgo relevante identificado en el estudio es el consumo de sustancias como alcohol y drogas, que incrementa la impulsividad y reduce el juicio crítico, facilitando la difusión de contenido íntimo sin valorar las posibles repercusiones. Los autores destacan que el sexting, en estos casos, no solo responde a un acto impulsivo, sino que está motivado por la presión de grupo y la búsqueda de aprobación, lo cual aumenta la vulnerabilidad a ser víctima de chantaje y otros delitos cibernéticos. Además, la falta de educación y concienciación en el manejo de las redes sociales y la privacidad digital deja a los jóvenes expuestos a la manipulación de su información personal (Chacón-López et al., 2016).

Los hallazgos evidencian que el sexting, lejos de ser una simple moda juvenil, es una práctica que conlleva serios riesgos emocionales y sociales, especialmente cuando se combina con factores de vulnerabilidad como la baja autoestima y el consumo de sustancias, la exposición a estas conductas de riesgo subraya la necesidad de estrategias de prevención y

educación digital, promoviendo la conciencia sobre los peligros del sexting y la importancia de la privacidad en entornos virtuales.

Estos resultados enfatizan la necesidad de implementar medidas preventivas y educativas orientadas a reducir los factores de riesgo asociados al sexting; la sensibilización sobre la importancia de la privacidad y las consecuencias de la exposición de la intimidad digital debe formar parte de los programas de educación digital, especialmente entre adolescentes, además, los padres juegan un rol fundamental en la protección de sus hijos al fomentar prácticas de supervisión y conversación abiertas sobre el uso responsable de las tecnologías y redes sociales.

Los resultados sugieren que el sexting, especialmente cuando deriva en la difusión no consentida de contenido íntimo, tiene implicaciones psicológicas y académicas serias en adolescente; la falta de control sobre las imágenes compartidas incrementa el riesgo de ciber victimización y afecta directamente la autoestima y el rendimiento de las víctimas, este estudio subraya la importancia de implementar programas educativos sobre el manejo de la privacidad en entornos digitales y de promover la sensibilización en el ámbito escolar y familiar para ofrecer apoyo adecuado a los jóvenes en situación de vulnerabilidad.

Los hallazgos reflejan la complejidad de las consecuencias psicológicas y sociales del sexting en adolescentes, especialmente cuando el contenido se distribuye sin consentimiento; la investigación de Resett (2021) subrayó la necesidad de abordar este tema desde una perspectiva preventiva, promoviendo una educación digital que sensibilice a los jóvenes sobre los riesgos y las implicaciones de estas conductas en su bienestar emocional y social. Además, es fundamental que padres y educadores estén informados y preparados para ofrecer el apoyo necesario a los adolescentes que puedan estar expuestos a estas experiencias.

Los resultados sugieren que el sexting en adolescentes no solo está asociado con la expresión de la sexualidad, sino también con factores de riesgo que comprometen la salud emocional y la privacidad de los involucrados. La coacción y el chantaje se destacan como consecuencias graves que afectan especialmente a las chicas, quienes enfrentan un mayor estigma social. La investigación de Rodríguez-Castro et al. (2021) subrayó la importancia de implementar programas educativos que promuevan un uso responsable de las tecnologías y fortalezcan la conciencia sobre la privacidad digital, protegiendo así la integridad de los jóvenes.

Estrategias de control parental

La investigación de González (2018) también sugirió que el uso de aplicaciones de control parental puede ser útil como complemento de la supervisión directa. Estas herramientas tecnológicas permiten limitar el acceso a contenidos inapropiados y ofrecen a los padres la posibilidad de monitorear la actividad de sus hijos en redes sociales. Sin embargo, su uso debe ser moderado y acompañado de un diálogo abierto, para que los adolescentes comprendan que estas medidas buscan su bienestar y no una invasión a su privacidad.

En cuanto al control parental, los resultados reafirmaron la importancia de un equilibrio en la supervisión. Las estrategias basadas en la confianza y el diálogo resultaron más eficaces que las prácticas autoritarias, debido a que fomentaron la autorregulación y un uso más responsable de internet por parte de los adolescentes (Symons et al., 2018). Sin embargo, se destacó la necesidad de complementar estas estrategias con educación digital que promueva la comprensión de los riesgos asociados al sexting y al uso irresponsable de las plataformas digitales.

La supervisión parental es una de las estrategias clave para reducir la incidencia del sexting entre adolescentes; a su vez, permite a los padres conocer y limitar el uso de dispositivos digitales y redes sociales, según el estudio de Domínguez et al. (2014) resaltó que el monitoreo activo de las actividades en línea y una comunicación abierta y constante pueden ayudar a los adolescentes a entender los riesgos asociados con el sexting y a evitar comportamientos impulsivos o influenciados por la presión social. Este tipo de supervisión implica tanto el conocimiento de las aplicaciones y redes que utilizan los jóvenes como la orientación sobre el uso adecuado de estas herramientas.

El control parental en el uso de internet resulta esencial para reducir los riesgos asociados al sexting entre adolescentes, según el estudio de Sureda et al. (2010), muchos padres aplican restricciones de tiempo de conexión y limitan el acceso a ciertas páginas, lo cual reduce la exposición de los jóvenes a contenidos inapropiados; este tipo de normativas temporales y de acceso funcionan como medidas preventivas que ayudan a mitigar la posibilidad de que los adolescentes compartan o accedan a contenido íntimo no adecuado para su edad.

La supervisión parental juega un papel crucial en la reducción del sexting entre adolescentes, especialmente cuando se implementa mediante

estrategias educativas y de concientización, según González (2018), los padres que dialogan abiertamente sobre los riesgos de compartir contenido íntimo y establecen normas claras de uso digital logran una mayor efectividad en la prevención de conductas de riesgo. Estas conversaciones fomentan en los adolescentes una conciencia más profunda sobre las consecuencias de sus acciones en línea, generando un ambiente de confianza en el hogar.

El control parental sobre el uso de dispositivos móviles es una estrategia crucial para prevenir prácticas de riesgo, como el sexting, entre adolescentes. Según Martínez & Echauri, (2014), los padres deben establecer normas claras sobre el uso del celular, incluyendo horarios y restricciones de acceso a ciertas aplicaciones y redes sociales. Este tipo de límites reduce las oportunidades para que los jóvenes participen en comportamientos riesgosos y fomenta una navegación más consciente.

Por otro lado, el fomento de un ambiente de comunicación abierta dentro del hogar es esencial para fortalecer el control parental. Según García Martínez y Fabila Echauri (2014), cuando los adolescentes se sienten cómodos discutiendo temas sensibles con sus padres, como el sexting y la privacidad en línea, es menos probable que se involucren en conductas riesgosas. Este tipo de comunicación fomenta la confianza y permite que los jóvenes comprendan los riesgos de compartir contenido íntimo, así como las consecuencias potenciales de la exposición en el entorno digital.

Respecto al control parental, los resultados sugirieron que las estrategias de supervisión contribuyeron a reducir la participación en actividades riesgosas en línea, siempre y cuando se aplicaran de manera equilibrada. Las prácticas autoritarias o excesivas llevaron a que los adolescentes busquen ocultar sus actividades, mientras que una supervisión basada en la confianza y el diálogo demostró ser más efectiva (Mendoza, 2020). Por lo tanto, la educación digital y la promoción de hábitos saludables en el uso de internet aparecieron como factores clave en la prevención del sexting.

Existe la necesidad de mejorar la alfabetización digital de los padres para que puedan establecer normas informadas y efectivas sobre el uso de internet en el hogar, muchos padres carecen de los conocimientos necesarios para abordar de manera eficiente el control de internet, lo cual indica la urgencia de programas formativos que les permitan ejercer una mediación digital adecuada y de apoyo de manera que estos puedan supervisar los actos que realizan sus menores hijos para con sitios webs no permitidos para su correcto desarrollo (Sureda et al., 2010).

La mediación restrictiva, donde los padres establecen normas sobre el contenido y tipo de aplicaciones permitidas, resulta efectiva para reducir el riesgo de sexting. Martínez & Echauri (2014) explicaron que, al limitar el acceso a ciertas redes sociales y aplicaciones de mensajería, los padres pueden minimizar las oportunidades para que los adolescentes participen en la difusión de contenido íntimo. Esta estrategia, sin embargo, debe aplicarse con sensibilidad para evitar que los jóvenes perciban el control como una invasión de su privacidad, lo cual podría disminuir la efectividad de la medida.

Por otro lado, el control técnico, como el uso de filtros y aplicaciones de monitoreo, es una herramienta complementaria que ayuda a los padres a gestionar el acceso de sus hijos a contenidos inapropiados, este tipo de control, aunque útil, debe integrarse con un enfoque de mediación que promueva el diálogo y la confianza; no obstante, la falta de comunicación puede llevar a que los adolescentes perciban estas medidas como invasivas, reduciendo su efectividad (Moreno-Carmona et al., 2021).

Los resultados revelan que, aunque muchos padres implementan controles básicos, una cantidad significativa de adolescentes accede a internet sin restricciones, lo cual incrementa su exposición a riesgos. Este acceso autónomo, particularmente en adolescentes de 15 a 16 años, sugiere que el control parental tiende a disminuir con la edad, a pesar de que los riesgos no desaparecen. Los investigadores destacan que este relajamiento en las normas puede dejar a los jóvenes vulnerables frente a prácticas como el sexting, resaltando la necesidad de una supervisión continua y de estrategias adaptadas a cada etapa de desarrollo para fortalecer el rol protector de los padres en el uso de tecnologías digitales.

El fomento de una relación cercana y de confianza entre padres e hijos es esencial para prevenir conductas de riesgo. El estudio subraya que aquellos adolescentes que perciben apoyo y comprensión por parte de sus padres tienen menos probabilidades de involucrarse en prácticas como el sexting. Este apoyo se manifiesta en la disponibilidad de los padres para hablar abiertamente sobre temas delicados, como la sexualidad y los riesgos de compartir contenido en línea, promoviendo así una mayor consciencia y responsabilidad en el uso de los medios digitales (Domínguez et al., 2014).

Además, el estudio destaca la importancia de la alfabetización digital de los padres, quienes deben estar al tanto de las tecnologías y plataformas que usan sus hijos, según Martínez & Echauri (2014), la falta de

conocimiento digital puede limitar la efectividad del control parental, por lo que es fundamental que los padres reciban orientación para adaptarse a los desafíos de la era digital y proteger mejor a sus hijos.

Además, Sureda et al. (2010) destacaron la importancia del acompañamiento parental durante la navegación en internet, especialmente en edades tempranas. Los resultados indican que los jóvenes que navegan en presencia de un adulto tienen una menor propensión a involucrarse en actividades de riesgo, como el sexting. Este acompañamiento, aunque es menos frecuente en adolescentes mayores, fomenta una cultura de responsabilidad y supervisión que reduce la probabilidad de exposición a situaciones vulnerables.

El control parental juega un papel fundamental en la reducción del sexting entre adolescentes, y las estrategias de mediación activa y restrictiva son clave en este sentido; el estudio de Moreno-Carmona et al. (2021) encontró que los padres que participan activamente en las actividades digitales de sus hijos, discutiendo abiertamente los riesgos y estableciendo reglas claras, logran reducir la probabilidad de que sus hijos se involucren en prácticas de sexting. Esta participación activa fomenta una comprensión más clara de las consecuencias de compartir contenido íntimo, generando mayor conciencia y responsabilidad.

Otro aspecto fundamental es el control psicológico adecuado, evitando prácticas intrusivas que afecten negativamente la relación familiar. señalan que el control psicológico excesivo, caracterizado por intentos de manipulación o coerción emocional, puede ser contraproducente, como fomenta una atmósfera de desconfianza. En cambio, el establecimiento de normas claras y justas respecto al uso de tecnologías y a la privacidad en internet contribuye a un entorno de respeto mutuo, donde los adolescentes se sienten apoyados y más propensos a seguir las indicaciones de sus padres (Domínguez et al., 2014).

Además, la mediación restrictiva, que implica establecer límites en el uso de internet y regular el acceso a ciertos contenidos, también se asocia con una menor prevalencia de conductas de riesgo digital, incluido el sexting. Moreno-Carmona et al. (2021) señalan que cuando los padres limitan el tiempo de conexión y supervisan las actividades en línea, los adolescentes tienden a evitar el sexting y otras prácticas peligrosas, esta estrategia es particularmente efectiva cuando se combina con una comunicación frecuente sobre la privacidad y los riesgos de internet.

Los resultados del estudio indican que el control parental efectivo en la prevención del sexting depende de un equilibrio entre supervisión, apoyo emocional y comunicación abierta, es crucial que los padres no solo controlan las actividades en línea de sus hijos, sino que también fortalezcan el diálogo y la confianza. Como concluyen Domínguez et al. (2014), una relación familiar basada en el respeto y el apoyo puede reducir significativamente las conductas de riesgo en adolescentes, promoviendo un uso responsable de la tecnología.

Los resultados de Moreno-Carmona et al. (2021) demostraron que el control parental efectivo en la prevención del sexting requiere una combinación de mediación activa, restrictiva y técnica. La educación digital dentro del hogar, junto con límites claros y la supervisión constante, fomenta un ambiente seguro donde los adolescentes desarrollan un sentido de responsabilidad y autonomía en su comportamiento en línea. Es fundamental que los padres promuevan una comunicación abierta para que los jóvenes comprendan los riesgos y se sientan respaldados en el uso seguro de la tecnología.

Los resultados obtenidos por Sureda et al. (2010) refuerzan la importancia de un control parental equilibrado, combinando la supervisión directa y el establecimiento de normas claras para proteger a los adolescentes de los riesgos digitales como el sexting. La alfabetización digital de los padres emerge como una herramienta crucial para que puedan entender y manejar el entorno digital de manera informada, promoviendo así un uso seguro y responsable de la tecnología entre los jóvenes.

Los hallazgos de Martínez & Echaury (2014) subrayan que el control parental efectivo en la era digital requiere una combinación de límites claros, supervisión activa y educación continua en tecnología. La alfabetización digital de los padres no solo facilita una supervisión más efectiva, sino que también ayuda a construir una relación de confianza con sus hijos, incentivando un uso responsable de las tecnologías.

Los resultados presentados por González (2018) hacen mención a la importancia de un enfoque balanceado en el control parental, donde la supervisión y la educación digital se combinan con un diálogo abierto y de confianza. Los padres no solo deben implementar normas y restricciones, sino también acompañarlos en el uso de las tecnologías.

CONCLUSIONES

- El análisis del fenómeno del sexting resalta su complejidad como práctica digital en expansión, con implicaciones legales, sociales y emocionales significativas. Aunque inicialmente consensuada, esta práctica conlleva riesgos considerables debido a la posibilidad de difusión no autorizada de contenido íntimo, lo que vulnera derechos fundamentales como la privacidad. Entre las consecuencias destacan la ansiedad, depresión y afectaciones a la autoestima, especialmente en adolescentes y jóvenes.
- La investigación subraya la importancia de un enfoque integral que combine educación digital, prevención y estrategias familiares, en términos educativos, es crucial sensibilizar sobre las repercusiones legales, emocionales y sociales del sexting. Por otro lado, la participación activa de los padres mediante supervisión equilibrada y comunicación abierta emerge como una estrategia eficaz para mitigar los riesgos. El control parental debe promover la confianza y establecer límites claros en el uso de dispositivos digitales, evitando enfoques autoritarios que puedan generar secretismo.
- Adicionalmente, se identifica la necesidad de políticas públicas robustas que fortalezcan la alfabetización digital y fomenten una cultura de respeto hacia la privacidad en línea. En este contexto, la colaboración entre instituciones educativas, organismos de seguridad y familias resulta indispensable para construir un entorno digital más seguro.
- Finalmente, el estudio concluye que el sexting no debe ser trivializado ni abordado únicamente desde la perspectiva punitiva. En su lugar, se requiere un enfoque preventivo y educativo que contemple las dinámicas culturales, tecnológicas y emocionales involucradas, promoviendo así un uso responsable de las tecnologías y protegiendo a los sectores más vulnerables de la sociedad.

REFERENCIAS

- Agustina, & Gómez-Duran, E. (2016). Factores de riesgo asociados al sexting como umbral de diversas formas de victimización. Estudio de factores correlacionados con el sexting en una muestra universitaria. *IDP. Revista de Internet, Derecho y Política*, 22, 21-47.
- Alonso-Ruido, P., Rodríguez-Castro, Y., Lameiras-Fernández, M., & Martínez-Román, R. (2018). El Sexting a través del discurso de adolescentes españoles. *Saúde e Sociedade*, 27(2), 398-409.

- Bisquerra, R. (2004). Metodología de la investigación educativa. La Muralla.
- Chacón-López, H., Barriga, J. F. R., Carretero, Y. A., & Cara, M. J. C. (2016). Construcción Y Validación De La Escala De Conductas Sobre Sexting (ecs). *Revista Española de Orientación y Psicopedagogía*, 27(2), 99-115.
- Chacón-López, H., Caurcel-Cara, M. J., & Romero-Barriga, J. F. (2019). Sexting en universitarios: Relación con edad, sexo y autoestima. *Suma Psicológica*, 26(1), 1-8.
- CONAPOC. (2020). *La ciberdelincuencia en el Perú*. <https://cdn.www.gob.pe/uploads/document/file/5948093/5270009-diagnostico-situacional-multisectorial-sobre-la-ciberdelincuencia-en-el-peru.pdf>
- Domínguez, M., Ocampo, D. B., & Martínez, J. L. C. (2014). Control Parental E Intento De Suicidio En Adolescentes Mexicanos. *Revista Colombiana de Ciencias Sociales*, 5(2), 240-252.
- Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 8(1), Article 9. <https://doi.org/10.5817/CP2014-1-9>
- Gabriel-Ortega, J. (2017). Cómo se genera una investigación científica que luego sea motivo de publicación. *Journal of the Selva Andina Research Society*, 8(2), 155-156.
- González, P. (2018). Erotización infantil y gramáticas afectivas: Discursos sobre la infancia en la era 2.0 en Argentina. *Sexualidad, Salud y Sociedad (Rio de Janeiro)*, 31, 101-118.
- Hernández, M., Fernández, M. del C. R., & Martínez, I. (2022). Consecuencias psicológicas del sexting y relación con el estrés académico. *MEDISAN*, 26(4). <https://www.redalyc.org/journal/3684/368472483008/>
- Hernández-Sampieri, R., Fernández, C., & Baptista, P. (2018). Metodología de la investigación (6ª ed.). McGraw Hill.
- Ley de delitos informáticos., No. 30096 (2013). [https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCCF05258316006064AB/\\$FILE/6_Ley_30096.pdf](https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCCF05258316006064AB/$FILE/6_Ley_30096.pdf)

- Martínez, V. G., & Echauri, A. M. F. (2014). Nomofilia Vs. Nomofobia, Irrupción Del Teléfono Móvil En Las Dimensiones De Vida De Los Jóvenes. Un Tema Pendiente Para Los Estudios En Comunicación. *Razón y Palabra*, 86. <https://www.redalyc.org/articulo.oa?id=199530728048>
- Mendoza, K. (2020). Parental control in digital environments: Promoting responsibility or fostering secrecy? *Journal of Family Studies*, 26(2), 215-230. <https://doi.org/10.1080/13229400.2019.1706418>
- Montiel, J. (2016). Cibercriminalidad social juvenil: La cifra negra. *IDP. Revista de Internet, Derecho y Política*, 22, 108-120.
- Moreno-Carmona, N. D., Marín-Cortés, A., Cano-Bedoya, V. H., Sanabria-González, J. A., Jaramillo-Suarez, Á. M., & Ossa-Ossa, J. C. (2021). Mediaciones parentales y uso de internet por niños, niñas y adolescentes colombianos. *Interdisciplinaria*, 38(2), 275-290.
- Narvaja, M. (2019). Sexting: Percepciones de estudiantes tucumanos sobre motivaciones y riesgos. *Ciencia, Docencia y Tecnología*, 30(59), 127-147.
- Narvaja, M., & Alonso, M. (2022). Análisis de la participación y la disposición hacia el sexting en estudiantes secundarios/as de Tucumán. *Revista Sobre La Infancia y La Adolescencia*, 23, 14-31. <https://doi.org/10.4995/reinad.2022.14675>
- Narvaja, M., & De Piero, J. (2016a). Prácticas Juveniles Éxtimas: Sexting Y Vlogging [1]. *Aposta. Revista de Ciencias Sociales*, 69, Article 69.
- Narvaja, M., & De Piero, J. (2016b). Prácticas Juveniles Éxtimas: Sexting Y Vlogging [1]. *Aposta. Revista de Ciencias Sociales*, 69, 239-270.
- Pifarré, M. (2013). «Internet y redes sociales: Un nuevo contexto para el delito». *IDP. Revista de Internet, Derecho y Política*, 16, 40-43.
- Ponce, O. A., Pagán Maldonado, N., & G. Galán, J. (2018). Investigación no experimental y generalización: Bases epistemológicas de las corrientes actuales. *IV Congreso Virtual Internacional sobre Innovación Pedagógica y Praxis Educativa INNOVAGOGÍA 2018: libro de actas. 20, 21 y 22 de marzo 2018, 2018, ISBN 978-84-09-00794-3*, 223. <https://dialnet.unirioja.es/servlet/articulo?codigo=7309529>

- Resett, S. (2019). Sexting en adolescentes: Su predicción a partir de los problemas emocionales y la personalidad oscura. *Escritos de Psicología - Psychological Writings*, 12(2), 93-102.
- Rodríguez-Castro, Y., Alonso-Ruido, P., González-Fernández, A., Lameiras-Fernández, M., & Faílde-Garrido, J.-M. (2020). Validación de la Escala de Comportamientos de Sexting en Adolescentes: Prevalencia y Consecuencias Asociadas. *Psicología Educativa*, 27(2), 177-185.
- Rodríguez-Otero, L., & Cerros-Rodríguez, E. (2021). El sexting como vía de materialización de la violencia: Prácticas y consecuencias en alumnado universitario de Nuevo León y Jalisco. *Revista Criminalidad*, 63(3), 203-214. <https://doi.org/10.47741/17943108.305>
- Sureda, J., Comas, R., & Morey, M. (2010). Menores y acceso a Internet en el hogar: Las normas familiares. *Comunicar*, XVII(34), 135-143.
- Symons, K., Ponnet, K., Emmery, K., Walrave, M., & Heirman, W. (2018). Parental knowledge of adolescents' online content and contact risks. *Journal of Youth and Adolescence*, 47(2), 233-246. <https://doi.org/10.1007/s10964-017-0715-3>
- Tamarit, J. M. (2013). Crónica de la III Jornada de Criminología UOC-CEFJE: Ciberdelito y Victimización. *IDP. Revista de Internet, Derecho y Política*, 16, 91-93.
- Tavares, A., Falcke, D., & Pereira, C. (2019a). Sexting en la adolescencia: Percepciones de los padres. *Ciencias Psicológicas*, 13(1), Article 1.
- Tavares, A., Falcke, D., & Pereira, C. (2019b). Sexting en la adolescencia: Percepciones de los padres. *Ciencias Psicológicas*, 13(1), 19-31.
- Walker, S., Sancí, L., & Temple-Smith, M. (2019). Sexting: Young women's and men's views on its nature and origins. *Journal of Adolescence*, 75, 130-141. <https://doi.org/10.1016/j.adolescence.2019.06.007>

EL TELETRABAJO EN LATINOAMÉRICA

Marco A. Chávez- Argomedo¹

RESUMEN

La investigación aborda el teletrabajo en Latinoamérica, teniendo como objetivos el desempeño de las modalidades del teletrabajo, en el caso de Latinoamérica, el teletrabajo se organiza en diversas modalidades que buscan adaptarse a las necesidades de los trabajadores y a las políticas de cada organización, se analiza también la normatividad y las tendencias del teletrabajo en Latinoamérica, estas tendencias en el teletrabajo muestran un crecimiento sostenido en su adopción a nivel global, impulsado por los beneficios en competitividad y flexibilidad que aporta a las empresas y a los trabajadores, especialmente en sectores tecnológicos y de servicios, donde la presencia física no es un requisito indispensable. Así también unificar la importancia que desempeña el teletrabajo en el ámbito laboral. El trabajo se desarrolló en un enfoque cualitativo con el fin de lograr un acercamiento al tema del teletrabajo en Latinoamérica, además el tipo de investigación fue básica y descriptiva, obteniendo un análisis de información bibliográfica de artículos científicos.

Palabras clave: Teletrabajo, Derecho, Laboral, Latinoamérica

¹ Mchavezal@upao.edu.pe

Programa de estudio de Derecho, Universidad Privada Antenor Orrego

ABSTRACT

The research addresses teleworking in Latin America, having as objectives the performance of the modalities of teleworking, in the case of Latin America, teleworking is organized in various modalities that seek to adapt to the needs of the workers and the policies of each organization, it is analyzed. Also the regulations and trends of teleworking in Latin America, these trends in teleworking show sustained growth in its adoption at a global level, driven by the benefits in competitiveness and flexibility that it brings to companies and workers, especially in technological and industrial sectors. services, where physical presence is not an essential requirement. Also unify the importance that teleworking plays in the workplace. The work was developed in a qualitative approach in order to achieve an approach to the topic of teleworking in Latin America. Furthermore, the type of research was basic and descriptive, obtaining an analysis of bibliographic information from scientific articles.

Keywords: Teleworking, Law, Labor, Latin America

INTRODUCCIÓN

La incorporación de nuevas tecnologías ha generado transformaciones significativas en el ámbito del trabajo subordinado, tales como el incremento del trabajo autónomo y la redistribución de empleos a favor del sector servicios. Estas innovaciones están modificando la estructura tradicional del trabajo subordinado, promoviendo, entre otros aspectos, un mayor uso de contratos a plazo fijo. Los cambios sociales impulsados por factores como el avance tecnológico representan una oportunidad para que las empresas adopten modelos de organización (Sánchez, 2021).

Soto et al. (2024) mencionaron que el teletrabajo es una de las más recientes transformaciones de la concepción del trabajo, surge del pensamiento de flexibilidad laboral e incorpora los avances de las tecnologías de la información a la necesidad imperiosa de ser más competitivos y productivos. Estas transformaciones dieron inicio a un fenómeno laboral que acrecienta en la última década.

Martínez (2012) argumentó que el teletrabajo está revolucionando la concepción tradicional de que las personas deben salir de casa y trasladarse a un lugar específico para cumplir con sus responsabilidades laborales. Ahora, es posible trabajar desde cualquier ubicación siempre que se disponga de una computadora y conexión a internet; este fenómeno requiere una revisión de los aspectos económicos, administrativos; como legales, lo que obliga a las organizaciones y gobiernos a adaptarse a esta nueva forma de trabajo y sus implicaciones.

Las tecnologías emergentes influyen y reconfiguran la organización empresarial, impulsando la adopción de estructuras más flexibles para optimizar costos y elevar considerablemente la competitividad. En el contexto postindustrial, las empresas ajustan su producción de forma diversificada según las demandas del mercado, enfocándose en cumplir su objetivo empresarial, ya sea a través de la producción de bienes o la prestación de servicios, este enfoque está alineado con altos estándares de calidad y autonomía operativa, lo que exige una mano de obra más cualificada y preparada para los cambios; asimismo en este proceso de especialización, se emplean técnicas de externalización y descentralización del trabajo (kahale, 2003).

Vanegas et al., (2023) señaló que los fisiócratas franceses del siglo XVIII consideraban que solo el trabajo agrícola era realmente productivo, mientras que veían a los comerciantes y al clero como clases improductivas, que no creaban riqueza. El liberalismo económico introdujo el concepto de la división del trabajo, mientras que el marxismo puso énfasis en el valor del trabajo y examinó la plusvalía que este género. Por otro lado, el keynesianismo sostenía que el empleo era clave para generar demanda agregada, por lo que el Estado debía intervenir para mantener en marcha la economía.

Para finales del siglo XX, el concepto de trabajo cambió bajo un enfoque neoliberal, en el que se busca que la mano de obra sea eficiente para reducir costos y alcanzar la mayor productividad posible. Este modelo promueve la flexibilidad laboral en términos de horarios, sueldos, contrataciones y despidos, lo que ha incrementado la precariedad laboral; como resultado, se observa un aumento en la cantidad de personas que recurren a la economía informal, desempeñando empleos sin contar con cobertura (Rodríguez, 2007).

En el Perú, el teletrabajo está regulado por la Ley 30.036 y su reglamento correspondiente, el Decreto Supremo No. 017-2005. Esta forma de empleo, que se aplica tanto en el ámbito público como en el privado, se caracteriza por el uso de tecnologías para la realización de actividades laborales, diferenciándose del trabajo a domicilio, que generalmente involucra tareas manuales y cuenta con su propia normativa, el teletrabajo se desarrolla en un marco de subordinación, sin la presencia física del trabajador y mediante el empleo de tecnologías (Ramírez et al., 2021).

El objetivo del artículo es abordar la evolución del teletrabajo en el contexto del desarrollo social y económico, analizando diversos aspectos.

Se examinan sus modalidades del teletrabajo, incluyendo también las implicaciones de la normatividad en el ámbito del derecho laboral y las tendencias del mercado laboral. Además, se estudia la importancia del trabajo remoto y su efectividad y productividad.

METODOLOGÍA

Esta investigación tuvo un enfoque cualitativo con el fin de lograr un acercamiento al tema del teletrabajo en Latinoamérica, como sus modalidades y tendencias en el ámbito laboral, así también en la normatividad que esta rige sobre el trabajo, el diseño de investigación fue no experimental- descriptivo además el tipo de investigación fue básica (García , 2016).

El trabajo se desarrolló en un tiempo de 4 meses teniendo una ardua investigación descriptiva, apoyándose de bibliografía de artículos científicos en cuanto concierne a el teletrabajo.

La técnica se limitó a la revisión bibliográfica de diferentes artículos científicos como; Redalyc, scopus, scielo, de esta forma se estableció una base de datos con 30 referencias, las cuales se emplearon en la redacción este artículo, marcando los objetivos más relevantes como las modalidades del teletrabajo, las tendencias del teletrabajo, la normatividad del teletrabajo y la importancia del trabajo remoto.

RESULTADOS

Modalidades del teletrabajo

En el caso de Latinoamérica, el teletrabajo se organiza en diversas modalidades que buscan adaptarse a las necesidades de los trabajadores y a las políticas de cada organización, la modalidad de teletrabajo suplementario es una de las más comunes, en la cual el trabajador divide su tiempo entre el hogar y la oficina, este modelo permite una supervisión periódica en la empresa y facilita el seguimiento de los procesos de seguridad y salud en el trabajo (SST), lo cual es crucial para garantizar el cumplimiento de las normativas en ambientes de teletrabajo (Valero-Pacheco & Riaño-Casallas, 2020).

En Colombia, el teletrabajo ha adoptado modalidades como el autónomo, suplementario y móvil, cada una diseñada para satisfacer distintos tipos de

trabajo y necesidades de flexibilidad, la modalidad autónoma, que permite al trabajador desempeñar sus funciones desde el hogar, ha mostrado beneficios en términos de equilibrio entre la vida personal y laboral, sin embargo, esta modalidad plantea el desafío del aislamiento, lo que puede disminuir la integración del trabajador en la cultura organizacional y afectar su bienestar emocional y productividad a largo plazo (Cifuentes-Leiton & Londoño-Cardozo, 2020).

La clasificación de las modalidades de teletrabajo en función de la ubicación, tiempo y estatus laboral permite comprender la flexibilidad de esta modalidad, los teletrabajadores primarios, cuya labor se centra en el hogar y cuentan con todos los recursos necesarios, enfrentan beneficios en cuanto a ahorro en desplazamientos y mejora de la calidad de vida. Sin embargo, el aislamiento y la posible desconexión con la cultura de la empresa pueden afectar su motivación y sentido de pertenencia (Martínez, 2012).

Otra modalidad es el teletrabajo autónomo, en la cual el trabajador opera completamente desde su hogar o cualquier lugar externo a la empresa, utilizando herramientas digitales para cumplir con sus tareas, este tipo de teletrabajo se observa principalmente en áreas tecnológicas y administrativas, donde la naturaleza del trabajo permite una menor supervisión física, las empresas que optan por este modelo deben implementar estrategias de comunicación y monitoreo efectivas para manejar los riesgos laborales a distancia (Valero-Pacheco & Riaño-Casallas, 2020).

La modalidad suplementaria, que permite alternar entre el espacio de trabajo físico y el hogar, ofrece una solución a la desconexión y facilita la interacción con el equipo en la oficina, esto es particularmente relevante en roles donde la supervisión o el contacto periódico con otros trabajadores es necesario, no obstante, el éxito de esta modalidad depende de la disposición de los empleadores para adaptarse a las necesidades de los trabajadores, ofreciendo herramientas y condiciones que permitan una adecuada transición entre ambos entornos (Cifuentes & Londoño, 2020).

Los teletrabajadores sustanciales combinan trabajo remoto con días presenciales en la oficina, lo cual les permite mantener vínculos sociales y un sentido de pertenencia más fuerte, esta modalidad es ideal para roles que requieren interacción periódica y permite a las empresas maximizar la eficiencia operativa, no obstante, su éxito depende de políticas claras

que regulen la frecuencia y condiciones de cada modalidad, así como del acceso a tecnología adecuada en ambos entornos (Martínez, 2012)

El teletrabajo móvil permite que el trabajador realice sus actividades desde distintos lugares, sin una ubicación fija, este tipo es común entre empleados de sectores como ventas y consultoría, que requieren movilidad; sin embargo, este modelo presenta desafíos adicionales para la gestión de SST, pues el entorno de trabajo cambia constantemente, lo que requiere de protocolos específicos para garantizar la seguridad y salud del trabajador en múltiples ubicaciones (Valero & Riaño, 2020)

El teletrabajo móvil, utilizado por aquellos cuya labor requiere desplazamientos constantes, aporta una gran flexibilidad al permitir que los trabajadores realicen sus actividades desde cualquier lugar mediante el uso de dispositivos y conectividad remota, esta modalidad, aunque dinámica, presenta desafíos específicos en cuanto a la regulación de horarios y condiciones laborales. La necesidad de una normativa más clara es vital para proteger los derechos de estos trabajadores, quienes deben contar con garantías sobre (Cifuentes & Londoño, 2020).

En el teletrabajo marginal, que es intermitente y poco regular, el trabajador realiza solo ciertas tareas en modalidad remota, conservando el esquema laboral tradicional en otros aspectos, aunque este tipo de teletrabajo brinda flexibilidad, se enfrenta a retos en términos de integración y rendimiento. A menudo, el acceso a equipos y soporte tecnológico es limitado, y la productividad puede verse afectada por la falta de un entorno estable de trabajo remoto (Martínez, 2012).

Teletrabajo a domicilio, se realiza, en vez de realizarlo en la oficina, estos trabajos de baja cualificación, como entrada de datos, mecanografía o desglose de formularios, mayoritariamente realizados por mujeres. Las condiciones laborales son a menudo poco favorables, en ello los trabajadores están aislados y excluidos de representación sindical y pesar de su condición de empleados por cuenta ajena son tratados más bien como si fueran autoempleados.

Otra modalidad relevante es el teletrabajo autónomo, en la cual el trabajador gestiona sus tiempos y recursos desde su hogar o un espacio propio. En este esquema, el teletrabajador asume la responsabilidad de los costos operativos, como el acceso a internet y los consumibles. Esta modalidad, cada vez más popular en sectores de consultoría y freelance, permite una

gran autonomía, fomentando la innovación y la autogestión. Sin embargo, al no contar con las garantías de un contrato formal (Martínez, 2012).

Las modalidades de teletrabajo en Colombia y Latinoamérica representan un avance en la flexibilidad laboral, pero cada una presenta retos específicos para el cumplimiento de las normativas de seguridad y salud en el trabajo, la necesidad de adaptar los sistemas de gestión a las condiciones de teletrabajo, mediante medidas de monitoreo remoto y promoción de buenas prácticas, es esencial para asegurar un entorno seguro y saludable, independientemente de la modalidad adoptada por la organización. (Valero & Riaño, 2020).

La diversidad de modalidades de teletrabajo en Colombia evidencia un esfuerzo por adaptar el marco laboral a las exigencias actuales, pero la regulación enfrenta desafíos significativos en su aplicación. La normativa actual suele favorecer al empleador, otorgándole flexibilidad para determinar las condiciones del teletrabajo, lo que puede dejar al trabajador en una posición vulnerable. Es crucial que el diseño de políticas públicas sobre teletrabajo contemple no solo la productividad y eficiencia, sino también el bienestar y derechos de los teletrabajadores (Cifuentes & Londoño, 2020).

Las modalidades de teletrabajo reflejan una tendencia hacia la flexibilización del trabajo, adaptándose a las necesidades de eficiencia y competitividad de las organizaciones. Sin embargo, la falta de una regulación específica y homogénea genera ambigüedades que pueden comprometer los derechos laborales y el bienestar de los teletrabajadores. La adopción de políticas que garanticen condiciones de trabajo equitativas y apoyen la motivación de los teletrabajadores es crucial para que esta modalidad sea sostenible y beneficiosa tanto para empleados como para empleadores (Martínez, 2012).

En Latinoamérica y especialmente en Colombia, el teletrabajo se organiza en diversas modalidades para adaptarse tanto a las necesidades de los empleados como a las políticas de cada organización. Una de las formas más comunes es el teletrabajo suplementario, en el que los trabajadores dividen su tiempo entre el hogar y la oficina. Este modelo permite una supervisión periódica en la empresa, facilitando el seguimiento de los procesos de seguridad y salud en el trabajo (SST), lo cual es esencial para asegurar el cumplimiento de las normativas en los ambientes de teletrabajo.

Normatividad del teletrabajo

La normatividad en torno al teletrabajo ha evolucionado en respuesta a distintas necesidades y contextos, comenzando como una política interna en las empresas y luego transformándose en una medida regulada para el trabajo remoto en casos específicos. Inicialmente, el teletrabajo surgió en Estados Unidos en la década de 1970 como una alternativa para reducir el consumo de energía y mitigar los efectos de la crisis del petróleo, promoviendo el trabajo desde casa a través de tecnología básica (Roig & Pineda, 2020).

El análisis del teletrabajo dentro del marco del capitalismo de vigilancia revela una profunda transformación en la relación laboral, donde la autonomía y flexibilidad aparentes ocultan mecanismos de monitoreo constante. Con la expansión del teletrabajo durante la pandemia de COVID-19, las empresas han implementado software de vigilancia para controlar el rendimiento y comportamiento de sus empleados. Esta práctica no solo implica una supervisión estricta, sino que también facilita la extracción de datos personales (Roncal, 2021).

El teletrabajo ha evolucionado como una opción viable en la era digital, impulsado por el acceso a las Tecnologías de la Información y la Comunicación (TIC), este modelo laboral, que facilita la independencia geográfica y la reducción de costos, ha permitido que muchas empresas en países desarrollados adopten prácticas flexibles. Sin embargo, en América Latina, la implementación del teletrabajo es limitada y enfrenta barreras culturales y de infraestructura, lo que frena su expansión y potencial impacto en la economía regional (Osio, 2010).

El crecimiento de las tecnologías de la información impulsó nuevas normativas para el teletrabajo en Europa, donde el Acuerdo Marco Europeo de Teletrabajo de 2002 definió esta modalidad como una forma de organización laboral vinculada al uso de TIC. Este acuerdo, aunque no vinculante, sentó las bases políticas para el teletrabajo al señalar sus beneficios, como la modernización organizacional y la conciliación entre vida laboral y familiar, aunque sin que este último aspecto fuera el objetivo principal (Roig & Pineda, 2020).

El uso de tecnologías como DeskTime y Kickidler permite a las empresas monitorear en tiempo real las actividades de los empleados, categorizando su productividad y registrando cada acción realizada en sus dispositivos, estas herramientas de vigilancia eliminan prácticamente la frontera entre

el ámbito privado y laboral, generando una dinámica de supervisión continua que lleva al trabajador a autoevaluarse constantemente para evitar sanciones o despidos, este fenómeno introduce una nueva dimensión de explotación (Roncal, 2021).

Los beneficios del teletrabajo se extienden desde el ahorro en transporte hasta una mayor calidad de vida para los trabajadores, entre las ventajas también se incluye la capacidad de las empresas de acceder a talento especializado sin restricciones geográficas. Este enfoque permite una optimización de recursos que mejora la competitividad de las empresas, especialmente en pequeñas y medianas empresas que pueden optar por teletrabajadores sin invertir en infraestructura física costosa. Además, el teletrabajo facilita el acceso laboral para personas con discapacidades, (Osio, 2010).

En 2020, la pandemia de COVID-19 impulsó una regulación más estricta del teletrabajo en muchos países, como España, donde el teletrabajo se prioriza como medio para mantener las operaciones empresariales y minimizar los riesgos de contagio. Esta normativa temporal estableció el teletrabajo como una opción obligatoria en algunos sectores, impulsando la necesidad de crear estándares sobre el derecho a la desconexión y la provisión de recursos por parte de los empleadores (Roig & Pineda, 2020).

Además, el capitalismo de vigilancia afecta la calidad de vida y la salud mental de los trabajadores al exigirles estar disponibles y activos en todo momento, incluso en sus hogares, según Byung Chul Han, esta modalidad de control convierte la flexibilidad laboral en una “coacción fatal”, donde el trabajador debe estar permanentemente conectado. Foucault también advirtió sobre los efectos de estos sistemas de control, describiéndolos como una extensión del panóptico, que vigila sin que el individuo sepa cuándo es observado (Roncal, 2021).

A nivel socioeconómico, el teletrabajo ha demostrado tener un impacto positivo en la distribución de la población, pues reduce la necesidad de migración hacia grandes ciudades para acceder a oportunidades laborales. Esto contribuye a disminuir el congestionamiento urbano y los problemas asociados al crecimiento desmedido de las áreas metropolitanas. Además, fomenta el desarrollo económico en localidades más pequeñas, permitiendo que las personas trabajen desde su lugar de residencia (Osio, 2010).

La evolución de la normativa sobre el teletrabajo ha demostrado que esta modalidad de empleo es una herramienta clave para adaptar el mercado

laboral a las exigencias del mundo digital, sin embargo, la regulación actual aún presenta limitaciones en términos de protección de derechos y establecimiento de condiciones uniformes para los teletrabajadores, las normativas, especialmente aquellas surgidas a raíz de la pandemia, han impulsado medidas temporales para el teletrabajo, aunque sin abordar de manera integral aspectos críticos como el derecho a la desconexión (Roig & Pineda, 2020).

Para los trabajadores, el teletrabajo representa una oportunidad de conciliar la vida laboral con la personal, brindando autonomía y flexibilidad en la organización de sus actividades, no obstante, también enfrenta retos como el aislamiento social y la necesidad de adaptar el hogar a las exigencias de un entorno laboral, esta modalidad exige competencias específicas en el manejo de TIC y una gran autodisciplina, elementos fundamentales para sostener la productividad en un ambiente sin supervisión física directa (Osio, 2010).

El capitalismo de vigilancia en el contexto del teletrabajo redefine los límites tradicionales de privacidad y control en el entorno laboral. Aunque el teletrabajo permite a los empleados cierta flexibilidad, la implementación de software de monitoreo ha intensificado el control sobre sus actividades, exacerbando las dinámicas de explotación y precarización, esto plantea desafíos éticos y legales sobre la privacidad y el derecho a la desconexión, debido a que los trabajadores no solo ven invadido su espacio personal (Roncal, 2021).

En el contexto europeo, aunque el Acuerdo Marco Europeo de Teletrabajo de 2002 reconoce ciertos beneficios del teletrabajo, como la conciliación laboral y familiar, esta política no ha sido implementada con suficiente rigor para resolver problemas estructurales de derechos laborales en cada país, a nivel estatal, como en el caso de España, la normatividad es aún limitada y fragmentada, dejando en manos de cada empresa o sector la implementación de medidas específicas, lo cual no asegura condiciones equitativas para todos los trabajadores remotos (Roig & Pineda, 2020).

La adopción del teletrabajo en América Latina evidencia tanto su potencial transformador como sus limitaciones, aunque su implementación puede contribuir a la descentralización laboral y a una mejor distribución geográfica de oportunidades de empleo, las barreras estructurales y culturales impiden su masificación, la infraestructura tecnológica y el soporte legal son áreas críticas que deben reforzarse para consolidar el teletrabajo como una práctica estable y accesible (Osio, 2010).

La normatividad en torno al teletrabajo ha evolucionado a lo largo del tiempo, adaptándose a diversas necesidades y contextos. Comenzó como una política interna en las empresas y, con el tiempo, se transformó en una medida regulada para el trabajo remoto en casos específicos. El teletrabajo tuvo sus orígenes en Estados Unidos en la década de 1970, cuando se vio como una alternativa para reducir el consumo de energía y mitigar los efectos de la crisis del petróleo. En aquella situación, se promovió el trabajo desde casa utilizando tecnología básica.

Tendencias del teletrabajo en el mercado laboral

Las tendencias en el teletrabajo muestran un crecimiento sostenido en su adopción a nivel global, impulsado por los beneficios en competitividad y flexibilidad que aporta a las empresas y a los trabajadores, el avance en las Tecnologías de la Información y Comunicación (TIC) ha facilitado que esta modalidad de trabajo se expanda, especialmente en sectores tecnológicos y de servicios, donde la presencia física no es un requisito indispensable (Guzmán & Abreo, 2017).

El teletrabajo ha generado una transformación en las relaciones laborales, en especial al analizarse desde una perspectiva de protección y reforma, la modalidad de teletrabajo actual, heredera de prácticas de trabajo a domicilio, retoma elementos de autonomía en la gestión laboral, aunque enfrenta problemas de falta de fiscalización, lo que favorece la precarización, la ausencia de supervisión presencial fomenta la descentralización del trabajo y el aislamiento del trabajador, limitando su acceso a los derechos de representación y su capacidad de acción colectiva (Lenguita, 2010).

La regulación del teletrabajo en el ámbito jurídico-laboral se caracteriza por su constante evolución ante los cambios tecnológicos y la flexibilidad que exige el mercado laboral, a nivel general, el teletrabajo permite a los empleados realizar sus funciones fuera del espacio físico de la empresa, utilizando herramientas digitales para cumplir con sus responsabilidades, esta modalidad ha generado desafíos para el Derecho Laboral, especialmente en la definición de derechos y obligaciones entre el teletrabajador y el empleador (Kahale, 2003)

Otra tendencia importante es la adopción del teletrabajo como una herramienta de inclusión laboral. A nivel global, el teletrabajo ha sido promovido como una alternativa que facilita el acceso al mercado laboral a personas en situación de discapacidad o con limitaciones de movilidad,

esta modalidad permite que las empresas diversifiquen sus plantillas, al tiempo que promueve la igualdad de oportunidades, este enfoque ha sido adoptado principalmente en Europa, con políticas de apoyo que fomentan la empleabilidad de grupos vulnerables a través del teletrabajo (Guzmán & Abreo, 2017).

La implementación del teletrabajo ha sido aprovechada para la externalización productiva y la subcontratación, lo que puede conllevar a una situación de “dumping social,” donde los teletrabajadores, al estar en regiones o bajo regímenes laborales diferentes, trabajan en condiciones menos protegidas, este modelo permite a las empresas reducir costos laborales, pero introduce una vulnerabilidad que se agrava en contextos de crisis económica, donde el teletrabajo se convierte en una alternativa de contratación sin garantías plenas de protección (Lenguita, 2010).

En cuanto a los derechos de los teletrabajadores, existen vacíos normativos que dificultan garantizar condiciones laborales equitativas aunque el teletrabajo ofrece beneficios como la flexibilidad y la reducción de desplazamientos, también plantea riesgos de aislamiento y falta de supervisión, estos factores pueden llevar a una menor protección frente a riesgos laborales, como el estrés o el desgaste profesional, en algunos países, la legislación laboral ha intentado llenar estos vacíos mediante la regulación parcial del teletrabajo en los contratos a domicilio (Kahale, 2003).

Finalmente, el teletrabajo está asociado con el desarrollo de competencias digitales en los empleados, que se vuelven indispensables en este modelo laboral, las habilidades en gestión del tiempo, comunicación virtual y uso de herramientas colaborativas se han convertido en competencias críticas para los teletrabajadores. Esta necesidad impulsa a las empresas a invertir en la capacitación de su personal para optimizar la productividad y facilitar la adaptación a un entorno de trabajo digitalizado (Guzmán & Abreo, 2017).

Adaptación y expansión del teletrabajo: En los últimos años, el teletrabajo ha ganado relevancia como una modalidad laboral flexible que responde a las demandas de un mercado cada vez más tecnológico. Esta tendencia ha crecido especialmente en sectores donde las tareas pueden gestionarse de manera remota mediante herramientas digitales, permitiendo a las empresas optimizar recursos y reducir la necesidad de espacios físicos (Kahale, 2003).

Además, el teletrabajo ha impulsado la atomización y la individualización de las relaciones laborales, disminuyendo la cohesión del colectivo de trabajo y, con ello, su poder sindical. Este modelo laboral, aunque brinda flexibilidad y autonomía, también expone al teletrabajador a condiciones de fragilidad laboral, pues el aislamiento dificulta la defensa de derechos colectivos. La atomización se traduce en una relación laboral más desigual, en la que los trabajadores están sujetos a condiciones impuestas unilateralmente por el empleador (Lenguita, 2010).

La implementación de regulaciones específicas para el teletrabajo enfrenta retos adicionales debido a la naturaleza flexible e individualizada de esta modalidad, la descentralización productiva y el outsourcing se han vuelto prácticas comunes, lo que genera una relación laboral fragmentada y difusa entre el teletrabajador y la empresa, esta estructura de externalización y subcontratación complica la definición de obligaciones de ambas partes y fomenta la dispersión de los trabajadores, dificultando su organización colectiva y limitando su capacidad para exigir derechos laborales (Kahale, 2003).

Las tendencias del teletrabajo reflejan un cambio estructural en el mercado laboral, donde la tecnología y la flexibilidad laboral son esenciales para la competitividad empresarial. A medida que el teletrabajo se consolida, las empresas deben adaptarse no sólo en términos de infraestructura, sino también en sus políticas de gestión de talento y desarrollo de competencias digitales, la implementación de programas de teletrabajo permite a las organizaciones optimizar sus recursos y acceder a una fuerza laboral global (Guzmán & Abreo, 2017).

El avance del teletrabajo, aunque útil para la economía moderna, plantea retos significativos para la protección de los derechos laborales. La externalización y la falta de regulación homogénea permiten a las empresas operar con flexibilidad, pero esto también socava la estabilidad laboral y dificulta la acción sindical. En este contexto, se vuelve crucial establecer un marco normativo internacional y nacional que considere la precarización que puede acompañar al teletrabajo y que refuerce la protección de los teletrabajadores (Lenguita, 2010).

La falta de una regulación clara y específica para el teletrabajo subraya la necesidad de adaptar el Derecho Laboral a las nuevas formas de organización laboral, la regulación del teletrabajo no solo debe enfocarse en proteger los derechos individuales de los teletrabajadores, sino también

en establecer estándares que contemplen la protección contra riesgos como el aislamiento y la excesiva flexibilidad que puede derivar en precarización laboral, la creación de un marco legal uniforme (Kahale, 2003).

La falta de una regulación clara y específica para el teletrabajo subraya la necesidad de adaptar el Derecho Laboral a las nuevas formas de organización laboral, la regulación del teletrabajo no solo debe enfocarse en proteger los derechos individuales de los teletrabajadores, sino también en establecer estándares que contemplen la protección contra riesgos como el aislamiento y la excesiva flexibilidad que puede derivar en precarización laboral (Kahale, 2003).

Una tendencia importante en la evolución del teletrabajo es su adopción como una herramienta de inclusión laboral. A nivel global, el teletrabajo ha sido promovido como una alternativa que facilita el acceso al mercado laboral a personas en situación de discapacidad o con limitaciones de movilidad. Esta modalidad permite a las empresas diversificar sus plantillas, al mismo tiempo que fomenta la igualdad de oportunidades. Este enfoque ha sido particularmente adoptado en Europa, donde se han implementado políticas de apoyo que fomentan la empleabilidad de grupos vulnerables a través del teletrabajo

Importancia legal del trabajo remoto

La incorporación del teletrabajo en las organizaciones ha sido promovida como una medida para mejorar la movilidad en zonas urbanas, porque permite reducir tanto la frecuencia como la duración de los desplazamientos entre el hogar y el lugar de trabajo, a pesar de los beneficios potenciales, el teletrabajo no ha sido adoptado de manera amplia ni por empresas ni por empleados, limitando así su capacidad para generar mejoras significativas en la movilidad en las ciudades (Verano et al., 2014).

La crisis sanitaria de COVID-19 puso en evidencia la falta de una regulación específica sobre teletrabajo en el sector público español, obligando a establecer normativas urgentes. A partir de esta necesidad, se ha desarrollado un marco legal en las distintas comunidades autónomas, priorizando la continuidad de los servicios públicos en contextos de crisis y potenciando la eficiencia y la modernización en la función pública (Rastrollo, 2022).

La investigación explora cómo factores organizacionales, como el apoyo de la gerencia y la cultura de capacitación, influyen en la capacidad de

los empleados para adaptarse al teletrabajo durante la pandemia, la rápida transición al teletrabajo, sin una preparación previa, obligó a empleados y empresas a enfrentar desafíos relacionados con la tecnología, el ambiente de trabajo en el hogar y la conciliación con responsabilidades personales (Ortiz et al., 2024).

Varios países de América Latina, como Argentina, Costa Rica, Colombia y México, han avanzado en la creación de normativas para regular el teletrabajo, cubriendo vacíos jurídicos y adaptando sus leyes laborales a las nuevas modalidades de trabajo a distancia, estas regulaciones permiten establecer lineamientos claros sobre los derechos y deberes de empleadores y teletrabajadores, brindando una mayor seguridad laboral y protecciones específicas para quienes trabajan desde casa (Jiménez, 2013).

Las legislaciones autonómicas han comenzado a incorporar el teletrabajo como una herramienta no solo para la conciliación, sino también para mejorar la eficiencia y la innovación en la administración pública. El teletrabajo se considera estratégico para reducir desplazamientos, contribuir al desarrollo sostenible y optimizar la gestión de recursos en las administraciones, promoviendo una cultura de trabajo basada en resultados (Rastrollo, 2022).

La implementación del teletrabajo enfrenta ciertos retos, como la falta de una definición estandarizada y la variedad de modalidades existentes, entre las que se incluyen el trabajo domiciliario, el itinerante y el realizado en telecentros, aunque el teletrabajo puede reducir los desplazamientos hacia el centro laboral, también puede dar lugar a otros, como viajes por motivos de ocio o incluso por relocalización residencial hacia zonas más alejadas, lo cual contrarresta parte de sus beneficios para la movilidad urbana (Verano et al., 2014).

La implementación del teletrabajo enfrenta desafíos específicos en el sector público, especialmente en lo que respecta a la compatibilidad con las “necesidades del servicio”, que condicionan la posibilidad de trabajar a distancia, además, las normativas autonómicas limitan el acceso a esta modalidad según el tipo de puesto, excluyendo aquellos que requieren una presencialidad constante, como atención al público y funciones de coordinación o dirección (Rastrollo, 2022).

En Colombia, la Ley 1221 de 2008 regula y promueve el teletrabajo como una estrategia para crear empleo, la ley asegura la igualdad de condiciones

salariales y el acceso a la seguridad social para los teletrabajadores, y fomenta el desarrollo de infraestructura y apoyo en zonas vulnerables y geográficamente apartadas, asimismo, establece una red de apoyo que reúne a instituciones públicas y privadas para impulsar el teletrabajo y brindar apoyo técnico y normativo a los empleados y empleadores (Jiménez, 2013).

Se destaca que el apoyo gerencial es esencial para que los empleados perciban un ambiente favorable al teletrabajo, la investigación sugiere que las empresas que brindan capacitaciones efectivas y apoyo en la adaptación tecnológica facilitan el rendimiento de sus empleados, a su vez, la cultura de capacitación permite a los trabajadores adquirir habilidades necesarias para desempeñarse en esta modalidad de trabajo remoto, incrementando su motivación y rendimiento (Ortiz et al., 2024).

Para que el teletrabajo tenga éxito, es fundamental considerar aspectos organizacionales, sociodemográficos y de desplazamiento, el apoyo de la organización y la disponibilidad de tecnología adecuada son esenciales, al igual que contar con un espacio de trabajo adecuado en el hogar y la posibilidad de compatibilizar la vida laboral y familiar, sin embargo, se ha encontrado que el tiempo de desplazamiento en sí mismo no es el principal motivador para optar por el teletrabajo (Verano et al., 2014).

Los empleados que disponen de mayor autonomía en su trabajo muestran una mejor adaptación al teletrabajo, dado que pueden gestionar sus tareas y horarios con mayor flexibilidad. La comunicación eficaz entre gerentes y empleados es también fundamental para asegurar que los trabajadores comprendan sus responsabilidades y objetivos, lo que facilita un desempeño satisfactorio (Ortiz et al., 2024).

Argentina y Costa Rica destacan por sus normativas específicas sobre teletrabajo, en Argentina, las leyes incluyen protecciones en temas de intimidad del teletrabajador y asignan al empleador la responsabilidad sobre el equipo de trabajo. También se garantiza el derecho de reversibilidad, permitiendo que los teletrabajadores puedan regresar a la modalidad presencial si lo desean, en Costa Rica, las normativas abarcan aspectos como la accesibilidad y la inclusión de grupos vulnerables (Jiménez, 2013).

Las normativas han introducido sistemas de control y evaluación que se basan en objetivos y resultados más que en la supervisión de la presencia física, para adecuarse a la naturaleza del teletrabajo. Asimismo, se establece

el derecho a la desconexión digital y se han creado órganos de seguimiento en varias comunidades autónomas para supervisar la implementación y efectividad de esta modalidad (Rastrollo, 2022).

La adopción efectiva del teletrabajo depende del respaldo de políticas claras y del apoyo organizacional, teniendo en cuenta las necesidades específicas de cada empresa y trabajador, las instituciones gubernamentales pueden desempeñar un papel clave al proporcionar directrices y estímulos para que el teletrabajo se adopte de manera generalizada, maximizando así su impacto en la reducción del tráfico y la mejora de la movilidad en áreas urbanas (Verano et al., 2014).

La capacidad de adaptación se convierte en un factor crucial para los empleados; a su vez, les permite manejar el estrés y aprender nuevas tareas en un contexto de trabajo remoto, la adaptabilidad se ve influida por la percepción de apoyo recibido y por el nivel de competencias personales desarrolladas, ayudando a los trabajadores a mantener su rendimiento en circunstancias de emergencia, como la pandemia (Ortiz et al., 2024).

La normativa asegura la igualdad de derechos para los empleados que trabajan, incluyendo la provisión de equipos y la protección de datos. La formación continua y específica en competencias digitales es esencial para que los empleados puedan adaptarse al entorno digital, considerando que esta modalidad debe contribuir a su desarrollo profesional dentro de la función pública (Rastrollo, 2022).

La implementación exitosa del teletrabajo requiere contar con políticas claras y un respaldo organizacional que considere las particularidades de cada empresa y empleado. En este contexto, las entidades gubernamentales tienen un papel fundamental al ofrecer orientaciones y estímulos que fomenten la adopción generalizada de esta modalidad laboral, lo que contribuiría significativamente a disminuir la congestión vehicular en zonas urbanas.

CONCLUSIONES

- En América Latina, las formas de teletrabajo han experimentado un avance hacia una mayor flexibilidad laboral. Se destacan diversas modalidades, entre ellas el teletrabajo autónomo, el teletrabajo móvil, el teletrabajo marginal y el teletrabajo a domicilio. Cada una de estas modalidades refleja cómo las condiciones laborales se han adaptado para ofrecer mayor libertad en términos de ubicación y horario, permitiendo

a los trabajadores organizar sus labores de acuerdo con sus necesidades y el contexto en el que operan.

- Se ha demostrado que el teletrabajo ha surgido como una herramienta esencial para promover la inclusión en el ámbito laboral, facilitando el acceso al empleo para personas con discapacidades o restricciones de movilidad. Esta modalidad no solo permite a las empresas ampliar la diversidad de su personal, sino que también favorece la igualdad de oportunidades en el entorno laboral.
- Se ha llegado a la conclusión de que la evolución de las normativas sobre el teletrabajo ha permitido que el mercado laboral se ajuste a las exigencias del entorno digital. No obstante, las regulaciones actuales resultan insuficientes en cuanto a la salvaguarda de los derechos de los trabajadores a distancia y la creación de condiciones laborales estandarizadas. Las normativas aplicadas, en su mayoría como respuestas provisionales ante la pandemia, no han abordado de forma integral aspectos esenciales, como el derecho a la desconexión, lo que resalta la necesidad urgente de una legislación más sólida y duradera en este ámbito.
- Se estableció que la legislación vigente asegura la igualdad de derechos para los teletrabajadores, cubriendo aspectos como la provisión de equipos y la protección de la información. Asimismo, resulta crucial que los empleados reciban capacitación constante y especializada en habilidades digitales, es por ello que esta modalidad de trabajo debe contribuir a su crecimiento profesional en el sector público, favoreciendo su adaptación y evolución en el ámbito digital.

REFERENCIAS

- Cifuentes, D. M., & Londoño, J. (2020). Teletrabajo: El problema de la institucionalización. *AiBi Revista de Investigación, Administración e Ingeniería*, 8(1). <https://doi.org/10.15649/2346030X.749>
- García, V. H. G., & Martínez, R. M. (2016). Ausentismo laboral y salud: Estudio de su importancia en el teletrabajo. *RETOS. Revista de Ciencias de la Administración y Economía*, 6(11), 13-25.
- Guzmán, A., & Abreo, C. (2017). Las habilidades del teletrabajador para la competitividad. *Forum Empresarial*, 22(2), 5-30.

- Jiménez, A. (2013). Análisis comparativo de normativas de teletrabajo en América Latina. *RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, 4(7), 200-222.
- Kahale, D. (2003). Teletrabajo: Regulación jurídico-laboral. *Gaceta Laboral*, 9(3), 397-416.
- Kahale, D. T. K. (2003). Teletrabajo: Regulación jurídico-laboral. *Gaceta Laboral*, 9(3), 397-416.
- Lenguita, P. (2010). Las relaciones de teletrabajo: Entre la protección y la reforma. *Argumentos*, 23(64), 245-263.
- Martínez, R. (2012). El teletrabajo como tendencia del mercado laboral. *RETOS. Revista de Ciencias de la Administración y Economía*, 2(4), 143-156.
- Martinez, R. M. (2012). El teletrabajo como tendencia del mercado laboral. *RETOS. Revista de Ciencias de la Administración y Economía*, 2(4), 143-156.
- Ortiz, M., Candelaria, G. L., & Ortiz, J. G. R. (2024). Factores que impactan el desempeño laboral: Estudio sobre la adaptabilidad al teletrabajo inducido por el evento del COVID-19. *Revista Academia & Negocios*, 10(1), 121-144.
- Osio, L. O. (2010). El Teletrabajo: Una opción en la era digital. *Observatorio Laboral Revista Venezolana*, 3(5), 93-109.
- Ramírez Velásquez, J. C., Tapia Tapia, H. E., Vega Abad, C. R., & Villagómez, M. (2021). Teletrabajo en Sudamérica: Un desafío jurídico frente al covid-19. *Revista Venezolana de Gerencia*, 26(94), Article 94.
- Rastrollo, J. (2022). Una función pública estratégica: El teletrabajo en la Administración Autonómica. Análisis jurídico-administrativo. *Revista de Estudios de la Administración Local y Autonómica. Nueva época*, 18, 236-252.
- Rodriguez, M. R. (2007). El teletrabajo en el mundo y Colombia. *Gaceta Laboral*, 13(1), 29-42.
- Roig, R., & Pineda-Nebot, R. (2020). El teletrabajo y la conciliación: Dos políticas públicas diferentes. *GIGAPP Estudios Working Papers*, 7(182-189). <http://www.gigapp.org/ewp/index.php/GIGAPP-EWP/article/view/203>

- Roncal, X. (2021). Teletrabajo y capitalismo de vigilancia. *Telos*, 23(1), 177-192.
- Sanchez vera, M. C. S. (2021). La innovación tecnológica y el teletrabajo: Un análisis crítico desde los derechos humanos (Ecuador). *Revista Latinoamericana de Antropología del Trabajo*, 5(10). <https://www.redalyc.org/journal/6680/668070945008/>
- Soto, M. O., Candelaria, G. L., & Ortiz, J. G. R. (2024). Factores que impactan el desempeño laboral: Estudio sobre la adaptabilidad al teletrabajo inducido por el evento del COVID-19. *Revista Academia & Negocios*, 10(1), 121-144.
- Valero, I. C., & Riaño, M. I. (2020). Teletrabajo: Gestión de la Seguridad y Salud en el Trabajo en Colombia. *Archivos de Prevención de Riesgos Laborales*, 23(1). <https://doi.org/10.12961/aprl.2020.23.01.03>
- Vanegas, M. C. V., Bustos, J. M. B., Brrientos, C. B., & Durán, J. P. (2023). Compromiso laboral y condiciones individuales en teletrabajo durante la pandemia por Covid-19 en México. *Entreciencias: Diálogos en la Sociedad del Conocimiento*, 11(25), Article 25. <https://www.redalyc.org/journal/4576/457672025010/>
- Verano, D., Falcón, H. S., & Cabrera, S. S. (2014). El teletrabajo y la mejora de la movilidad en las ciudades. *Investigaciones Europeas de Dirección y Economía de la Empresa*, 20(1), 41-46.

EL HACKEO Y LA CIBERSEGURIDAD EN LA LEGISLACIÓN PERUANA: ANÁLISIS NORMATIVO Y DESAFÍOS FRENTE A LAS AMENAZAS DIGITALES

Leandro N. Delgado-Palacios¹

RESUMEN:

La rápida expansión de la tecnología en diversos sectores ha transformado la sociedad, pero también ha generado nuevas amenazas, como el ciberdelito y el hackeo. Estos riesgos han impulsado a los países a reforzar sus marcos normativos y estrategias de ciberseguridad, en Perú, el hackeo se enfrenta desde una perspectiva multidisciplinaria, incluyendo sanciones penales y medidas preventivas. A pesar de los avances legislativos, como la Ley N° 30096 y el Decreto Legislativo N° 1412, aún existen limitaciones en la infraestructura y los recursos para combatir estos delitos, la ciberseguridad no solo debe enfocarse en la sanción penal, sino también en la prevención y el fortalecimiento de un entorno digital seguro, apoyado por una cultura digital sólida y educación en ciberseguridad.

Palabras clave: Ciberdelito, delito, seguridad, normativa, legislación, delito informático.

¹ ldelgadop1@upao.edu.pe

Programa de Estudio de Derecho, Universidad Privada Antenor Orrego.

ABSTRACT:

The rapid expansion of technology in various sectors has transformed society, but it has also generated new threats, such as cybercrime and hacking. These risks have prompted countries to strengthen their regulatory frameworks and cybersecurity strategies. In Peru, hacking is faced from a multidisciplinary perspective, including criminal sanctions and preventive measures. Despite legislative advances, such as Law No. 30096 and Legislative Decree No. 1412, there are still limitations in the infrastructure and resources to combat these crimes. Cybersecurity should not only focus on criminal sanctions, but also on prevention and strengthening a safe digital environment, supported by a strong digital culture and cybersecurity education.

Keywords: Cybercrime, crime, security, regulations, legislation, computer crime.

INTRODUCCIÓN

Hasta el año 2024, la tecnología ha experimentado un crecimiento exponencial que ha impactado prácticamente todos los aspectos de la sociedad y el cambio constante abre nuevos horizontes de desarrollo en la aplicación de diversos campos, desde la economía y la educación hasta la salud y la seguridad; sin embargo, con el avance tecnológico también emergen nuevas amenazas, como el ciberdelito, el hackeo y las estafas digitales. Estos desafíos han obligado a los países a implementar medidas para proteger a los ciudadanos y las instituciones, ajustando sus marcos normativos y reforzando las estrategias de ciberseguridad.

Las nuevas tecnologías, especialmente la informática, no solo nos ayudan a hacer las mismas cosas de siempre de manera más rápida y eficiente, sino que también crean actividades completamente nuevas, algunas de estas pueden ser problemáticas porque afectan la convivencia pacífica entre las personas. La informática no se limita a ser una herramienta para mejorar lo que ya conocemos; también genera situaciones nuevas que, en muchos casos, ponen en aprietos a los sistemas legales, pues estos no siempre están preparados para enfrentarse a las realidades que surgen con estos avances (Arocena, 2012).

Es necesario identificar las diversas amenazas del ciberataque como parte de una forma sistematizada de hacer un golpe directo a la infraestructura crítica de un país, además, como muestra de ello, el 90% de los participantes en una encuesta del Computer Security Institute empleaba antivirus en sus redes, sin embargo, el 85% de sus sistemas había sido atacado por virus,

en la misma encuesta, el 89% tenía instalados firewalls, y el 60% sistemas de detección de intrusos; sin embargo, el 90% había sufrido brechas de seguridad, y el 40% intrusiones desde el exterior (Puime, 2009).

Los ataques informáticos en América Latina abarcan hackeos a correos electrónicos, plataformas de redes sociales y sistemas de banca virtual, entre otros. Adicionalmente, se abordó la situación del hackeo a Yahoo en 2014, en el que se extrajeron datos de más de 500 millones de cuentas, entre ellas nombres, correos electrónicos y cuestiones de seguridad. Este acontecimiento demostró la vulnerabilidad de las estrategias de seguridad en grandes corporaciones tecnológicas, poniendo de manifiesto la urgencia de implementar políticas de ciberseguridad más rigurosas (Reyna & Olivera, 2016).

Verdesoto (2007) argumentó que el hacking ético promueve la identificación y mejora de la seguridad informática en las redes de negocios. Describió técnicas como el “footprinting” y el “scanning”, fundamentales para prevenir ataques y robustecer los sistemas de protección. Además, resaltó que el uso de estas estrategias posibilita a las compañías prever los vectores de ataque más habituales y ajustarse a nuevas amenazas. Enfatizó la relevancia de llevar a cabo auditorías constantes para asegurar la integridad y fiabilidad de las infraestructuras digitales.

A su vez, la promulgación del decreto legislativo N° 1412, brindó un rol importante para el desarrollo y fortalecimiento de la ciberseguridad del país; esto se debe a que en el campo normativo brinda un mecanismo claro para ejecutar una protección de datos personales y crear un entorno digital seguro que brinde interacción directa con el Estado, empresas y ciudadanos; el mencionado decreto establece la obligación de las entidades públicas de adoptar medidas de ciberseguridad para proteger los sistemas de información del Estado, siguiendo los lineamientos de la Secretaría de Gobierno Digital, que actúa como órgano rector en la materia (Congreso de la República, 2013).

El hackeo, como género de la cibercriminalidad, abarca una amplia gama de conductas ilícitas, desde el simple acceso no autorizado hasta la modificación o destrucción de datos; en Perú, este acontecimiento ha sido abordado desde una óptica multidisciplinaria: no sólo con sanciones penales, sino también con medidas preventivas en el ámbito de la ciberseguridad. Este sentido, se presenta como la especie que engloba todas las medidas técnicas, legales y administrativas destinadas a proteger los sistemas y datos frente a posibles ataques.

Como una de las medidas para fortalecer la confianza digital, está el registro Nacional de Incidentes de Seguridad Digital que recoge información sobre los incidentes reportados por proveedores de servicios digitales en todo el país para analizarlos y buscar soluciones, toda la información es confidencial y está bajo la administración de la Secretaría de Gobierno Digital, que se encarga de proteger su integridad y garantizar su disponibilidad, además el Centro Nacional de Seguridad Digital puede compartir estos datos con los responsables del Marco de Seguridad y Confianza Digital siguiendo las leyes vigentes sobre protección de datos personales (Presidencia del Consejo de Ministros, 2020).

La Ley N° 30096, promulgada en el 2013, fue el primer intento por tipificar los delitos informáticos en el Perú; a lo largo de los años, la legislación menciona ha evolucionado para adaptarse a las nuevas modalidades de ciberdelitos, como la modificación del Código Penal mediante la Ley N° 30858, que endurece las penas para ataques que comprometen sistemas de información críticos del Estado y sectores estratégicos.

A pesar de estos esfuerzos, persisten limitaciones en la capacidad para investigar y perseguir estos delitos debido a la falta de infraestructura, recursos y conocimientos especializados en ciberseguridad, siendo así, resulta crucial analizar las medidas adoptadas y las posibles soluciones para enfrentar los ciberdelitos incluso, la ciberseguridad no solo debe enfocarse en sancionar penalmente los delitos, sino también en la prevención y en la creación de un entorno digital seguro; solo a través de un enfoque integral que incluya avances tecnológicos, normativos y administrativos se podrá garantizar la protección de los ciudadanos y la infraestructura crítica del país.

Además, se debe promover una cultura digital entre la población para fomentar comportamientos seguros al interactuar con las tecnologías digitales y la educación en ciberseguridad debe ser una prioridad en los centros académicos, lo que permitirá a las personas comprender cómo prevenir los riesgos asociados con su uso diario de internet y las plataformas digitales; las iniciativas educativas, incluidos los talleres prácticos sobre seguridad informática, pueden reducir significativamente la vulnerabilidad individual y colectiva al ciberdelito.

Para abordar estas problemáticas, este trabajo propone examinar el funcionamiento del hackeo, analizar las amenazas del hackeo y ciberseguridad, identificar los métodos para evitar los ciberdelitos y

analizar la penalización por ciberdelitos. Estos objetivos permitirán una comprensión integral sobre el hackeo y la ciberseguridad que ayudarán a poder establecer parámetros claros.

METODOLOGÍA

La investigación presentada es un estudio cualitativo que se enfoca en el análisis del hacking y la ciberseguridad en el marco del derecho peruano, examinando sus características y normativas fundamentales, este artículo se clasifica como básico y adopta un diseño descriptivo no experimental (Gabriel, 2017). La base del estudio se sustenta en una revisión bibliográfica de leyes pertinentes, como la Ley N° 30096, conocida como la Ley de Delitos Informáticos, así como en doctrinas especializadas en el ámbito de la ciberseguridad; se utilizaron fichas bibliográficas, lo que facilitó la sistematización del conocimiento existente y permitió un análisis más exhaustivo de los temas abordados.

El diseño metodológico fue no experimental y descriptivo, lo que significa que no se manipularon variables ni se realizaron intervenciones en el objeto de estudio. En su lugar, se buscó describir las características del hacking, los riesgos asociados, y la ciberseguridad, siguiendo un enfoque basado en la observación de información secundaria y la identificación de patrones relevantes.

Asimismo, analizó las amenazas del hackeo y ciberseguridad, finalmente, se analizó la adecuación de la legislación peruana, así como los métodos para evitar el hacking que llegan a ser eficientes en la realidad social y siendo uno de los mayores problemas que ocurren hasta la fecha.

Este análisis proporcionó una visión más clara sobre las fortalezas y debilidades del marco legal peruano frente a las ciber-amenazas y el ciberdelito en el país; además, subrayó la necesidad de fomentar una cultura de ciberseguridad entre los ciudadanos y las organizaciones, lo que incrementa la conciencia sobre los riesgos asociados al uso de tecnologías digitales.

RESULTADOS Y DISCUSIÓN

Funcionamiento del hackeo.

Espinoza (2018) indicó que el hackeo como uno de los delitos informáticos o delitos cibernéticos se caracterizan por ser delitos de cuellos blancos así también llamado debido a que determinadas personas con conocimientos especializados y técnicos pueden cometerlos, siendo así también el sujeto activo de estos delitos cualquier persona con dominio en lenguajes de programación, redes informáticas, ingeniería social, etc. El sujeto pasivo se le consideraría en estos casos cualquier persona natural o jurídica.

En el ámbito jurídico, el hackeo autorizado permite a las autoridades emplear software espía para acceder de manera remota a sistemas informáticos de sospechosos en investigaciones criminales, esta práctica, regulada en países como España bajo la Ley Orgánica 13/2015 y el artículo 588 septies (a)(1) de la LEC, representa una medida innovadora pero también controvertida debido al nivel de intrusión que supone en la privacidad de las personas, la naturaleza clandestina del procedimiento, al realizarse sin el conocimiento del afectado, y la posibilidad de extenderse en el tiempo (Blanco, 2021).

El hackeo es una práctica cada vez más difícil de controlar, aunque se han implementado sanciones severas, la responsabilidad penal sigue siendo un desafío; no obstante, también deben sancionarse a quienes facilitan o financian el hackeo, esta situación resalta la urgencia de regular tecnologías como la Inteligencia Artificial (IA), que puede ser utilizada para realizar intrusiones no autorizadas, y subraya la necesidad de un marco legal adecuado para proteger a la sociedad de estos riesgos (Moran, 2021).

El acceso no autorizado a sistemas informáticos, que implica la entrada ilegal a redes o dispositivos; la alteración o daño intencional a la integridad de los datos; la afectación deliberada de la integridad de los sistemas; el contacto con menores con fines sexuales mediante tecnología (grooming); la interceptación ilícita de datos durante su transmisión; el fraude llevado a cabo mediante herramientas informáticas; la suplantación de identidad para obtener información o recursos de manera fraudulenta. Estos delitos representan diversas formas de hackeo que afectan la seguridad digital y exigen respuestas tanto técnicas como legales (Espinoza, 2018).

El uso de hackeo como herramienta de investigación enfrenta dificultades cuando se aplica en contextos internacionales como el spyware, las

investigaciones pueden requerir acceso a servidores ubicados fuera del país, lo cual complica el proceso debido a la jurisdicción y las diferencias en la regulación de ciberdelitos, este aspecto destaca la necesidad de cooperación entre países para regular el hackeo estatal y facilitar el acceso a la información digital (Blanco, 2021).

El empleo del hackeo como herramienta de investigación presenta obstáculos significativos en contextos internacionales dado que muchas investigaciones necesitan acceder a servidores ubicados en otros países lo que genera complicaciones por cuestiones jurisdiccionales y diferencias en la normativa sobre ciberdelitos esta situación pone de relieve la importancia de establecer una cooperación internacional más sólida que permita regular el hackeo estatal y agilizar el acceso a información digital crucial para investigaciones relacionadas con el crimen organizado.

El hackeo planteó un reto creciente para el derecho debido a la rápida evolución de las técnicas y la dificultad de regular las actividades en el ciberespacio, si bien se han implementado marcos normativos buenos, la IA ahora también plantea dificultades por lo que debido a su alta especialización de conocimientos técnicos sirva de ayuda al hacking a los ciberdelincuentes (Moran, 2021).

El hackeo presentó un desafío creciente para el derecho debido a la rápida evolución de las técnicas y la complejidad de regular actividades en el ciberespacio aunque se han establecido marcos normativos para enfrentarlo es imprescindible crear leyes más específicas y efectivas que respondan a las nuevas formas de ciberdelitos la colaboración internacional y el refuerzo de la ciberseguridad resultan esenciales para abordar el hackeo de manera integral.

Blanco (2021) planteó que el hackeo autorizado judicialmente representó un avance significativo en la investigación criminal, permitiendo el acceso a datos clave sin comprometer la seguridad física de los investigadores, no obstante, el uso de spyware estatal plantea desafíos éticos y jurídicos, especialmente en términos de privacidad y derechos fundamentales para que el hackeo se mantenga como una herramienta legítima y proporcional.

El hackeo se ha convertido en uno de los delitos cibernéticos más comunes, caracterizado por su dependencia de habilidades técnicas avanzadas como programación, redes informáticas e ingeniería social, las personas que poseen estos conocimientos pueden ser responsables de realizar este tipo

de actividades, mientras que las víctimas pueden ser tanto individuos como empresas. Este tipo de delitos muestra el impacto que tienen en diversos ámbitos, desde la privacidad personal hasta la seguridad institucional.

Jiménez (2022) estudió el progreso de los delitos cibernéticos y sugirió tácticas fundamentadas en la formación constante y la actualización de los sistemas de seguridad para reducir los peligros. En su análisis, resaltó la importancia de una estrecha cooperación entre los gobiernos y las compañías para evitar estos crímenes cibernéticos. Es esencial una acción conjunta entre el sector público y privado para robustecer la protección frente a las amenazas digitales.

Los resultados evidenciaron que el hackeo constituye una amenaza directa para las instituciones tecnificadas al revelar la fragilidad de los sistemas sociotécnicos que dependen de infraestructuras digitales a medida que las instituciones adoptan más tecnología en sus actividades se vuelven vulnerables a ataques capaces de comprometer información sensible y alterar su funcionamiento esta situación resalta la urgencia de ajustar las políticas de seguridad para salvaguardar estos sistemas frente a accesos no autorizados.

En el ámbito judicial, el uso de hackeo autorizado ha permitido acceder a sistemas informáticos de sospechosos en investigaciones criminales, utilizando herramientas como el software espía, aunque esta práctica facilita la obtención de pruebas clave, genera debate por el nivel de invasión que implica en la privacidad y derechos fundamentales, además, su carácter clandestino y la posibilidad de aplicarse por largos periodos de tiempo plantea un delicado balance entre garantizar la seguridad pública y proteger las libertades individuales.

Los ciberdelitos relacionados con el hackeo, como el acceso no autorizado a sistemas, la manipulación de datos, el fraude o la suplantación de identidad, representan un riesgo creciente para la seguridad digital, estos delitos, que afectan tanto a personas como a organizaciones, son cada vez más sofisticados y requieren respuestas legales y tecnológicas más robustas, además, el uso indebido de tecnologías avanzadas como la inteligencia artificial añade una capa de complejidad, subrayando la necesidad de establecer marcos normativos claros que respondan a estas amenazas.

INTERPOL (2020) estudió la forma en que los ciberdelincuentes modificaron sus técnicas durante la pandemia de COVID-19, centrándose en los ataques de ransomware y phishing, que se dirigieron particularmente a

infraestructuras vitales y sectores de salud. Repuso cómo los criminales se aprovecharon de la incertidumbre provocada por la crisis para intensificar sus acciones, impactando tanto a entidades públicas como a corporaciones privadas.

El hackeo es un peligro que implica la penetración no permitida en sistemas con el objetivo de acceder, alterar o sustraer información. El progreso tecnológico ha elevado la complejidad de estos ataques, dificultando así las acciones preventivas. Actualmente, los ciberdelincuentes emplean herramientas sofisticadas, como la inteligencia artificial, para llevar a cabo ataques más complicados de identificar.

Este fenómeno no solo representa un desafío técnico, sino también moral y jurídico, dado que implica infracciones a la privacidad y a la seguridad. Es necesario un enfoque que fusione los progresos tecnológicos con una normativa legal adaptable que posibilite una defensa más eficaz.

Amenazas del Hackeo y Ciberseguridad

Arocena (2012) afirmó que, el hackeo es el delito de acceso de manera ilegítima a un sistema informático; además de los ataques tradicionales, el hackeo incluye técnicas avanzadas que constituyen una modalidad de ilicitud que se manifiesta de manera informática vulnerando así la exclusividad y la intimidad además de que el tipo legal nos explica sobre una conducta que vulnera los derechos a la intimidad y privacidad con lo que toda persona cuenta.

La hipertextualidad en la literatura digital puede inspirar métodos legales para segmentar y proteger datos en sistemas de información, como dividir contenido en nodos seguros y encriptados, en el ámbito jurídico, esta estrategia podría incluir leyes que obliguen a las empresas a segmentar sus datos sensibles, dificultando el acceso no autorizado, al dispersar los datos en “capas de acceso,” se podría establecer un estándar legal para mejorar la seguridad y dificultar la manipulación ilícita, ofreciendo así un método regulado de prevención contra ciberdelitos (Machín & Gazapo, 2016).

El hackeo en Perú representa una amenaza significativa para la ciberseguridad porque implica la irrupción no autorizada en sistemas y redes informáticas con el fin de acceder, manipular o destruir información, los ataques de hackeo han evolucionado y ahora pueden formar parte de redes de delincuencia organizada, donde varios actores colaboran para ejecutar ciberataques a gran escala que afectan tanto a individuos como

a entidades públicas y privadas, este tipo de amenaza cibernética destaca por su capacidad de adaptarse rápidamente a las defensas de seguridad (Santos et al., 2019).

Guaña (2023) sostuvo que el aprendizaje supervisado es un método crucial en la ciberseguridad, dado que posibilita a los sistemas detectar patrones predictivos y reaccionar de manera proactiva ante potenciales amenazas. Además, enfatizó que fusionar este método con análisis en tiempo real puede potenciar de manera notable la efectividad de las defensas digitales. Además, resaltó la relevancia de dotar estos sistemas de información actualizada para preservar su exactitud ante nuevas amenazas.

La capacidad de manipulación en la literatura digital reflejó la importancia de regular los accesos no autorizados y la alteración de datos en el derecho penal. Incluir delitos de manipulación de datos bajo las leyes de ciberseguridad es fundamental para sancionar cualquier intento de alterar o destruir información de forma ilegal; en este sentido, el derecho debe considerar los tipos de hackeo que permiten manipular información, estableciendo penas para quienes comprometan la integridad de datos y sistemas (Blanco, 2021).

El crecimiento de las amenazas relacionadas con el hackeo pone en evidencia la necesidad urgente de fortalecer la ciberseguridad, adoptando medidas proactivas que permitan identificar y neutralizar vulnerabilidades antes de que sean explotadas, la colaboración internacional y la modernización constante de los sistemas de defensa son esenciales para hacer frente a las redes de delincuencia organizada que operan en el ciberespacio, las cuales se benefician de la falta de uniformidad en las normativas y las limitaciones de recursos en las infraestructuras de seguridad (Machín & Gazapo, 2016).

Symantec (2014) notó que las tasas de infección por malware en América Latina son notablemente altas, con países como Venezuela y Brasil liderando las estadísticas. Su investigación ofrece recomendaciones para reducir el impacto de estas amenazas, destacando la importancia de invertir en tecnologías preventivas. Además, resaltó que es vital instruir a los usuarios acerca de buenas prácticas digitales para disminuir el efecto del malware en la zona.

CIBERNOS (2024) subrayó el valor de los instrumentos de seguridad en redes como acciones esenciales para evitar ataques informáticos. Afirmó

que la puesta en marcha de sistemas de protección de múltiples niveles, tales como cortafuegos y métodos de cifrado, facilita la reducción de las brechas de seguridad en infraestructuras esenciales. Además, destacó que las pruebas de penetración y simulaciones controladas son técnicas eficaces para detectar vulnerabilidades antes de que sean aprovechadas por los atacantes, resaltando la importancia de actualizaciones continuas y capacitación especializada para los empleados implicados.

La protección por capas, similar a los enlaces en red en los textos digitales, inspira sistemas legales de defensa en los que cada nivel de protección debe cumplir con normativas específicas de ciberseguridad, establecer leyes que obliguen a las instituciones a implementar múltiples capas de seguridad podría mejorar la protección de infraestructura crítica, esto permitiría que el marco legal facilite el diseño de barreras que complican el acceso indebido, protegiendo así sectores vitales en áreas como finanzas, salud y comunicaciones (Santos et al., 2019).

El derecho puede beneficiarse de la replicación de métodos probados en ciberseguridad estableciendo estándares que permitan a las empresas implementar prácticas ya evaluadas en la defensa contra ciberdelitos la legislación puede incorporar criterios mínimos de seguridad como encriptación obligatoria y segmentación de datos para todos los sectores que manejan información sensible estos estándares proporcionan un marco común que ayudaría a reducir la vulnerabilidad a ciberataques y estandarizaron la defensa digital (Arocena, 2012).

Riquelme et al. (2024) señalaron que los hackeos masivos a empresas como Microsoft, Google y Apple demuestran la falta de preparación frente a riesgos cibernéticos avanzados. Estos acontecimientos enfatizan la necesidad de aplicar estrategias de ciberseguridad más integrales y proactivas para proteger la información sensible de usuarios y entidades. Además, subrayan que numerosas compañías no invierten los recursos necesarios para modernizar sus sistemas de seguridad. Esto las vuelve susceptibles a métodos de ataque cada vez más sofisticados, tales como el phishing y ransomware. Así pues, fomentar una cultura empresarial enfocada en la seguridad digital es crucial para lidiar con los peligros del contexto actual.

La formación en ciberseguridad debería considerarse un derecho y una responsabilidad para todos los empleados de sectores sensibles la legislación podría requerir programas obligatorios de capacitación en

ciberseguridad similar a la educación en prevención de riesgos laborales de este modo el derecho se posiciona como un recurso preventivo en la lucha contra los ciberdelitos asegurando que todos los usuarios comprendan las prácticas básicas de protección de datos y evitando la propagación de vulnerabilidades (Álvarez & Montoya, 2020).

Así como la literatura digital permite expandirse de forma dinámica las leyes de ciberseguridad deben incluir la obligación de hasta el año 2024 que los sistemas de seguridad conforme evolucionen las amenazas estas leyes podrían exigir que las organizaciones mantengan sus sistemas al día con las últimas tecnologías y prácticas de seguridad esta flexibilidad garantiza que los sistemas jurídicos puedan respaldar tecnológicamente a las empresas en sus esfuerzos de ciberseguridad y evitar que se conviertan en objetivos de ciberdelincuentes (Arocena, 2012).

La interconexión de distintos elementos como la transmedialidad en literatura inspira la cooperación en defensa cibernética las leyes de ciberdelitos deberían promover la colaboración entre sectores privados gobiernos y agencias internacionales para crear redes de protección integradas estas redes impulsadas por marcos legales de cooperación mejorarían la capacidad de respuesta ante amenazas que afectan a varios países y sectores permitiendo así una defensa más completa contra los ciberdelitos globales (Gamón, 2017).

En el ámbito de la ciberseguridad el derecho puede fomentar una cultura de participación y responsabilidad compartida mediante leyes que obliguen a reportar actividad sospechosa estas normativas fortalecerán el control y la vigilancia creando una red de usuarios que apoyen en la detección de ciberdelitos así el derecho se convierte en un medio para involucrar a todos los usuarios de sistemas informáticos en la prevención activa de los ciberataques (Bustillos & Rojas, 2023).

La implementación de códigos y rutas seguras en sistemas digitales inspirada en el control de enlaces en literatura digital puede servir de base para regular el acceso a datos mediante códigos legales establecer leyes que exijan el uso de encriptación avanzada y acceso controlado permitiría restringir la manipulación de la información estas leyes ayudarían a reducir la exposición de los sistemas a accesos no autorizados y mejorarían la integridad y la privacidad de los datos en entornos digitales (Galicia, 2018).

La exigencia legal de tecnologías avanzadas de autenticación, como biometría y doble factor, plantea un equilibrio entre seguridad y privacidad; si bien estas tecnologías refuerzan la protección contra accesos no autorizados, pueden implicar riesgos en el manejo de datos personales sensibles, el desafío para el derecho es establecer estándares que maximicen la seguridad mientras se respeta la privacidad de los usuarios, exigiendo salvaguardias para la gestión de la información biométrica (Bustillos & Rojas, 2023).

Las normativas que definen la responsabilidad de las empresas en ciberseguridad generaron incentivos para adoptar medidas de protección, pero pueden enfrentar resistencia por parte de entidades que ven estas regulaciones como costos adicionales; el reto para el marco jurídico es establecer sanciones efectivas sin desincentivar la innovación, promoviendo un entorno donde las empresas entiendan la ciberseguridad como una inversión esencial y no como una obligación onerosa (Stepke, 2017).

La obligatoriedad de auditorías de ciberseguridad podría mejorar la protección de datos, sin embargo, podría representar una carga operativa para empresas más pequeñas. Si bien las auditorías permiten identificar vulnerabilidades y aumentar la prevención, es importante que las leyes consideren escalas proporcionales según el tamaño y recursos de las empresas, para asegurar que todas las organizaciones, independientemente de su capacidad, puedan cumplir con los requisitos de ciberseguridad de manera efectiva (Bustillos & Rojas, 2023).

La obligatoriedad de auditorías de ciberseguridad puede mejorar la protección de datos al identificar vulnerabilidades, pero representa una carga para las empresas pequeñas que carecen de los recursos necesarios. Es crucial que las leyes sean proporcionales al tamaño y capacidades de cada organización, permitiendo que todas puedan cumplir con los requisitos de ciberseguridad de manera efectiva sin poner en riesgo su operatividad.

Las amenazas del hackeo no se restringen a la infiltración en sistemas, sino que van más allá de modificar datos esenciales, sustraer datos personales y corporativos, y paralizar infraestructuras esenciales. Estos riesgos no solo impactan a personas, sino que pueden perturbar la estabilidad de gobiernos y economías completas. Conforme las infraestructuras digitales se vinculan, se incrementan las posibilidades para que los ciberdelincuentes aprovechen las vulnerabilidades, incrementando así los peligros de ataques

de gran magnitud. El progreso de las amenazas cibernéticas también ha originado redes de ciberdelincuentes estructurados, que funcionan en diversas jurisdicciones, lo que complica aún más la defensa. Por ende, la ciberseguridad debe superar la protección técnica de los sistemas, poniendo también énfasis en la prevención.

Métodos para evitar los ciberdelitos

Para prevenir los ciberdelitos, es fundamental la implementación de políticas de ciberseguridad que incluyan la educación y capacitación constante de los usuarios, así como la modernización de los sistemas y tecnologías de protección, la formación en buenas prácticas de seguridad, como el uso de contraseñas seguras y la autenticación multifactorial, es esencial para reducir las oportunidades de ataque, al mismo tiempo que el monitoreo y la detección temprana de amenazas permiten una respuesta rápida ante posibles incidentes, las medidas preventivas también deben abarcar la creación de entornos digitales seguros que incluyan firewalls y sistemas de encriptación de datos, proporcionando así un nivel adicional de defensa frente a accesos no autorizado (Arocena, 2012).

El Centro de Ciberdelito Europeo, también con la ayuda de EUROPOL, pone en alerta y permiten aumentar canales para prevenir la delincuencia en la red; en muchos países de la Unión Europea, se desarrollan campañas públicas y programas de formación en ciberseguridad, dirigidos tanto a empresas como a ciudadanos. Estas iniciativas ayudan a reducir los riesgos asociados a los ataques de ingeniería social y phishing, fortaleciendo el conocimiento y las prácticas seguras entre los usuarios del ciberespacio (Machín & Gazapo, 2016).

La seguridad de las infraestructuras críticas de información, como sistemas de energía, transporte y comunicaciones, es fundamental para evitar los ciberdelitos, en México, se han implementado protocolos específicos para proteger estos sistemas, pues un ataque cibernético podría afectar seriamente la estabilidad nacional, la estrategia se centra en monitorear constantemente estas infraestructuras y en garantizar su resiliencia mediante sistemas de control avanzados, como el SCADA, que permiten la detección temprana de incidentes (Galicia, 2018).

La implementación de simulaciones y ejercicios de ataque, conocidos como “pruebas de penetración”, es otro método efectivo para prevenir ciberdelitos, porque permite a las organizaciones identificar

vulnerabilidades antes de que sean explotadas, estas pruebas, realizadas de manera periódica, ayudan a mejorar la infraestructura de seguridad al simular escenarios reales de hackeo, lo que fortalece la capacidad de respuesta ante amenazas y permite a los equipos de ciberseguridad ajustar sus estrategias preventivas (Santos et al., 2019).

The Bridge (2024) subrayó que la ética en el hacking ha cobrado importancia como una práctica esencial en la prevención de delitos informáticos. Afirmó que, mediante simulaciones controladas de ataques, las entidades pueden detectar debilidades en sus sistemas y fortalecer sus protecciones antes de que los ciberdelincuentes las exploten. Además, enfatizó la relevancia de la cooperación entre los equipos de seguridad y los centros educativos para potenciar la formación en estas técnicas.

La gestión de riesgos en redes de telecomunicaciones implica identificar vulnerabilidades clave, como los ataques MitM y DoS, y desarrollar un mapa de riesgos. Este proceso permite anticipar las amenazas y establecer controles específicos para proteger la integridad y confidencialidad de los datos, con herramientas como matrices de riesgo, se evalúa la probabilidad de ocurrencia y el impacto de los ataques, permitiendo priorizar medidas de seguridad (Álvarez & Montoya, 2020).

Las infraestructuras críticas, como los sistemas energéticos, financieros y de transporte, han implementado sistemas avanzados de control y monitoreo para prevenir ataques cibernéticos. Estos incluyen protocolos como el uso de software de supervisión SCADA, que permite la gestión remota y segura de los procesos industriales, optimizando la respuesta ante posibles ciberamenazas. Esta tecnología también se combina con la capacitación constante del personal y la colaboración con entidades privadas para fortalecer la defensa contra posibles incidentes (Machín & Gazapo, 2016).

García (2016) estudió la repercusión financiera de los ciberdelitos en América Latina, subrayando que estas acciones ilegales generan costos considerables para la región debido a la ausencia de políticas enfocadas en la reacción adecuada ante incidentes. Sostuvo que, al carecer de una sólida estrategia de ciberseguridad, las naciones experimentan pérdidas financieras que impactan tanto en el sector público como en el privado. Asimismo, enfatizó la relevancia de la colaboración internacional y la creación de marcos regulatorios que faciliten una reacción efectiva frente a estas amenazas digitales.

Uno de los métodos clave para evitar ciberdelitos es fortalecer las capacidades de ciberseguridad a través de la formación de personal y la colaboración entre los sectores público y privado, en México, se están desarrollando programas de capacitación y sensibilización dirigidos a los operadores de infraestructuras críticas y al personal de entidades gubernamentales para que adopten prácticas de seguridad adecuadas y respondan eficazmente ante posibles amenazas (Galicia, 2018).

Otro método eficaz para evitar ciberdelitos es la implementación de sistemas de respuesta rápida ante incidentes de seguridad, como los equipos de defensa cibernética de reacción rápida, estos equipos están diseñados para intervenir de inmediato en caso de amenazas, minimizando el impacto de los ataques y asegurando una recuperación eficiente, la protección de datos también se garantiza mediante el uso de cifrado avanzado y la segmentación de redes, lo cual dificulta el acceso de los atacantes a la información crítica (Machín & Gazapo, 2016).

La adopción de medidas de ciberseguridad de carácter preventivo evidenció su efectividad en la disminución de ciberdelitos, la educación continua sobre ciberseguridad y la modernización de las infraestructuras de defensa son cruciales en un entorno de constante evolución tecnológica, la combinación de estrategias como la capacitación en seguridad digital y el uso de herramientas de protección avanzadas no solo fortalece la capacidad de los individuos y organizaciones para enfrentar los ciberdelitos, sino que también contribuye a la creación de un entorno digital más seguro y confiable (Santos et al., 2019).

La aplicación de pruebas de seguridad permite validar la efectividad de las defensas en las redes móviles, mediante el uso de tecnologías como GNU Radio y programas de captura de datos, se realizan simulaciones de ataques para entender mejor las vulnerabilidades, estas pruebas ayudan a visualizar cómo un atacante podría interceptar o manipular la información, lo que permite ajustar los controles y mejorar las defensas (Álvarez & Montoya, 2020).

Los resultados obtenidos destacan que la prevención de ciberdelitos debe abordarse desde una perspectiva integral, combinando estrategias tecnológicas y educativas, la capacitación constante en buenas prácticas de seguridad, como el uso de contraseñas robustas y sistemas de autenticación multifactorial, no solo fortalece la resiliencia individual frente a ataques, sino que también contribuye a la creación de un entorno digital más seguro,

la modernización de infraestructuras de protección, junto con el monitoreo y la detección temprana de amenazas, se identifica como una herramienta crucial para mitigar riesgos y responder con eficacia a los incidentes.

En términos de colaboración global, se evidencia la importancia de unir esfuerzos entre organismos internacionales, gobiernos y sectores privados para fortalecer la ciberseguridad, las plataformas de alerta y los programas de formación en prevención de ciberdelitos han demostrado ser efectivos para sensibilizar a usuarios y organizaciones sobre los riesgos, particularmente en relación con ataques como phishing e ingeniería social, además, la realización de pruebas de la penetración y simulaciones de ataque permite identificar vulnerabilidades críticas, mejorando las capacidades defensivas y anticipándose a posibles amenazas.

García (2024) analizó el impacto del hacking ético como herramienta para identificar fallos de seguridad en sistemas complejos. Su enfoque incluye simulaciones de ataques auténticos para evaluar la robustez de las defensas presentes. Este procedimiento permite a las organizaciones robustecer sus infraestructuras antes de que ocurran eventos de importancia. Adicionalmente, resaltó que la implementación de equipos multidisciplinarios en estas simulaciones potencia de manera notable la identificación de puntos débiles.

Scariot (2021) resaltó la transformación de los ataques de telecomunicaciones a sistemas digitales, estudiando cómo los phreakers, inicialmente concentrados en redes de telefonía, han pasado sus capacidades a ambientes digitales más sofisticados. Enfatizó que este cambio demuestra la capacidad de los ciberdelincuentes para adaptarse a tecnologías emergentes y presenta desafíos importantes para la seguridad informática, dado que estos ataques aprovechan las vulnerabilidades en sistemas que se encuentran cada vez más interrelacionados. Además, subrayó la importancia de fortalecer las defensas cibernéticas a través de estrategias que fusionen tecnología de punta y formación constante.

La instauración de marcos normativos específicos y de equipos de respuesta rápida son esenciales para combatir los ciberdelitos, en México, la Estrategia Nacional de Ciberseguridad busca establecer leyes claras y coordinar organismos que puedan reaccionar de forma inmediata a incidentes cibernéticos, esto incluye la creación de centros de respuesta a incidentes tecnológicos que faciliten una acción rápida y eficiente ante los ataques, reduciendo el impacto sobre los sistemas nacionales.

Los métodos adoptados para evitar los ciberdelitos en México reflejaron un enfoque integral que abarca la protección de infraestructuras críticas, la capacitación en ciberseguridad y el desarrollo de marcos normativos sólidos. Sin embargo, la rápida evolución de las amenazas cibernéticas plantea la necesidad de hasta el año 2024 constantemente estas estrategias y fortalecer la cooperación internacional.

Entre las recomendaciones para mitigar los riesgos se incluyó la adopción de normativas de seguridad como ISO 27001 y NIST 800-53, así como la capacitación continua de usuarios finales y proveedores de servicios, también es importante que los usuarios configuren herramientas de protección en sus dispositivos y que los proveedores implementen técnicas de inspección profunda de paquetes (DPI) para evitar ataques de denegación de servicio y mejorar la resiliencia de la red.

La protección de las redes móviles requirió una combinación de gestión de riesgos, simulaciones de ataques y políticas de seguridad efectivas, las pruebas de seguridad y la implementación de controles técnicos son fundamentales y esenciales para enfrentar amenazas complejas como los ataques MitM y DoS que son los más conocidos en la actualidad.

La prevención de los ciberdelitos demanda una estrategia holística que fusiona herramientas tecnológicas de vanguardia con una perspectiva educativa y organizacional. Los sistemas de protección, tales como cortafuegos, cifrado de datos y sistemas de identificación de intrusos, son esenciales para evitar ingresos no permitidos y atenuar las consecuencias de los ataques. No obstante, la tecnología en sí misma no basta. Es fundamental que tanto las entidades como las personas reciban capacitación constante en buenas prácticas de ciberseguridad, tales como la utilización de contraseñas robustas, la verificación multifactorial y la identificación de técnicas de ingeniería social. Además, las simulaciones de ataques cibernéticos facilitan la valoración de la efectividad de las acciones de seguridad y la adaptación de las tácticas de prevención. También es necesario que la prevención contemple la constante actualización de los sistemas de seguridad, dado que la actualización de los sistemas de seguridad es indispensable para su prevención.

Penalización por ciberdelitos

Los estados deben enfrentar los ciberdelitos mediante su legislación penal antes de considerar medidas internacionales, asegurando la preservación

de la paz y la seguridad, es crucial que las conductas más graves estén claramente definidas para permitir su enjuiciamiento y sanción, subrayando la seriedad de estos actos. Los ciberdelitos, como el hackeo y otros ataques digitales, representan una amenaza creciente que busca desestabilizar los sistemas legales y la convivencia en sociedades democráticas, las acciones terroristas se enmarcan en la máxima amenaza para las sociedades (Gamón, 2017).

En la legislación ecuatoriana, el hacking no está tipificado como un delito específico, pero ciertas figuras penales pueden considerarse formas de esta práctica, entre ellas están la revelación ilegal de bases de datos, la interceptación de datos sin autorización, la transferencia electrónica ilícita de activos patrimoniales y el daño a la integridad de sistemas informáticos, además, existen delitos relacionados con el patrimonio público, como el acceso no autorizado a sistemas informáticos o de telecomunicaciones y los crímenes contra la información pública. De estas conductas, el ataque cibernético se identificó como el que mejor refleja el comportamiento típico de un hacker (Santos et al., 2019).

La legislación peruana incorporó normativas para enfrentar los ciberdelitos, respondiendo al incremento de amenazas digitales que afectan tanto a individuos como a organizaciones, se han tipificado delitos como el acceso indebido a sistemas informáticos, el fraude informático y el espionaje digital, reflejando una preocupación creciente por el impacto que estos actos pueden tener en la seguridad nacional y en la confianza de los usuarios en los sistemas digitales (Gutierrez et al., 2022).

En respuesta al incremento de ciberdelitos que afectan a las pymes, varios países han fortalecido sus normativas para proteger a estas empresas y sancionar las actividades delictivas en el entorno digital, en regiones como la Unión Europea, las normativas incluyen sanciones significativas contra ciberdelincuentes y fomentan la creación de redes de apoyo para que las pymes cuenten con recursos de ciberseguridad accesibles, estas políticas buscan disminuir la exposición de estas empresas ante delitos como el robo de datos y el sabotaje de sistemas críticos (Bustillos & Rojas, 2023).

Las sanciones por ciberdelitos en Perú están establecidas con el objetivo de disuadir a los infractores y proteger la integridad de los datos personales y empresariales. Entre las medidas más comunes se encuentran las penas de prisión y las multas económicas, las cuales varían en función de la gravedad del delito y de los daños ocasionados, estas sanciones buscan

cubrir un amplio espectro de delitos, desde el robo de información hasta el sabotaje de sistemas críticos (Gutierrez et al., 2022).

Frente al incremento de ciberdelitos en Perú, se han intensificado los esfuerzos de cooperación internacional para crear un marco legal más robusto, Perú ha trabajado en conjunto con otros países y organizaciones internacionales para implementar estándares de ciberseguridad y mejorar su capacidad de respuesta ante amenazas globales, estas colaboraciones buscan no solo compartir experiencias y tecnologías, sino también fortalecer los mecanismos de rastreo y procesamiento judicial, permitiendo una penalización más efectiva de los ciberdelincuentes que operan a través de fronteras (Gutierrez et al., 2022).

La educación en prácticas de ciberseguridad ha tomado un rol fundamental para proteger a las pymes, países como Australia y Estados Unidos han lanzado guías prácticas y programas de formación adaptados, que proporcionan a estas empresas conocimientos básicos sobre la protección de sus sistemas. Estas iniciativas permiten que las pymes, muchas veces con recursos limitados, adopten medidas de seguridad efectivas de forma accesible y preventiva, fortaleciendo así su resiliencia frente a los ataques (Bustillos & Rojas, 2023).

La comparación entre las penalizaciones por ciberdelitos en Perú y otros países, como España, resalta la importancia de contar con marcos normativos que respondan a las características específicas de los crímenes digitales, como la capacidad de operar transnacionalmente y de evolucionar rápidamente, el incremento de sanciones en algunos países refleja un esfuerzo por disuadir estas conductas y proteger los derechos de los usuarios en el ciberespacio, sin embargo, en el caso peruano, aún queda por fortalecer las penas y establecer una legislación.

La colaboración entre países ha sido crucial para enfrentar los ciberdelitos que afectan a las pymes. Acuerdos como el Convenio de Budapest y los programas de la OEA promueven el intercambio de conocimientos y la creación de políticas conjuntas que fortalecen la capacidad de respuesta ante ciberdelitos. La penalización de estos delitos y el apoyo a las pymes dependen en gran medida de este esfuerzo internacional, que permite una respuesta coordinada ante amenazas transfronterizas (Bustillos & Rojas, 2023).

A pesar de los avances legislativos, la aplicación de la ley enfrenta retos significativos, las barreras técnicas y la rápida evolución de los

métodos de hackeo dificultan la detección y persecución efectiva de los ciberdelincuentes, además, la falta de recursos y de personal especializado en ciberseguridad en las instituciones gubernamentales limita la efectividad de la respuesta ante incidentes, lo cual subraya la necesidad de fortalecer tanto las capacidades técnicas como las estrategias de cooperación internacional para combatir los ciberdelitos de manera eficaz (Gutierrez et al., 2022).

Aunque la legislación peruana ha avanzado en la penalización de los ciberdelitos, persisten desafíos en su implementación y efectividad. La rápida evolución de las técnicas de hackeo y las limitaciones en recursos especializados subrayan la necesidad de fortalecer tanto las políticas internas como la cooperación internacional. Integrar un enfoque colaborativo con otros países y organismos permite a Perú alinearse con estándares internacionales, lo que no solo mejora su capacidad para enfrentar ciberdelitos, sino que también promueve un entorno digital más seguro para sus ciudadanos y empresas.

La legislación hasta el año 2024 está reforzando las penas para quienes cometen ciberdelitos, aumentando tanto las sanciones económicas como las penas de prisión. Este enfoque busca disuadir actividades ilegales en el ciberespacio, considerando la gravedad de delitos como el acceso no autorizado y el robo de datos, estas reformas responden a la necesidad de que las leyes sean proporcionales al impacto de los ciberdelitos, alineándose con la creciente dependencia de las tecnologías digitales en todos los sectores (Stepke, 2017).

La legislación en ciberseguridad está evolucionando para penalizar distintos tipos de delitos de manera específica, desde ataques de denegación de servicio hasta fraudes financieros y espionaje digital. Cada uno de estos ciberdelitos implica diferentes riesgos y daños, por lo que las leyes están comenzando a clasificar y penalizar cada tipo según su impacto; esta distinción permite una aplicación más precisa de la justicia y busca abordar de manera integral las diversas amenazas que enfrentan las instituciones y los individuos en el ciberespacio (Espinoza, 2018).

Dado que los ciberdelitos a menudo cruzan fronteras, las leyes nacionales deben coordinarse con marcos legales internacionales para ser efectivas. A través de tratados y acuerdos de cooperación, se permite a los países trabajar juntos para identificar, procesar y penalizar a los ciberdelincuentes que operan en múltiples jurisdicciones. Esta colaboración internacional

facilita la aplicación de sanciones y refuerza la capacidad de los países para proteger sus infraestructuras críticas contra ataques provenientes de actores extranjeros (Bustillos & Rojas, 2023).

La evolución de la legislación en ciberseguridad en Perú refleja una tendencia hacia la penalización específica de diferentes ciberdelitos, lo cual resulta esencial debido a la diversidad de amenazas que enfrenta el país en el ciberespacio. Al clasificar y sancionar ataques como los de denegación de servicio, fraudes financieros y espionaje digital de manera diferenciada, se logra una respuesta más adecuada y precisa ante cada tipo de delito, permitiendo una aplicación más eficiente de la justicia; esto no solo mejora la protección de las instituciones y ciudadanos, sino que también refuerza la confianza en la seguridad digital en un entorno cada vez más vulnerable a estos ataques.

Dado que los ciberdelitos trascienden fronteras, es fundamental que Perú se coordine con marcos legales internacionales a través de tratados y acuerdos de cooperación para hacer frente a estos delitos de manera efectiva. La colaboración con otros países en la identificación, procesamiento y penalización de ciberdelincuentes que operan a nivel global es clave para fortalecer la defensa de la infraestructura crítica del país.

Esta cooperación internacional permite a Perú alinearse con esfuerzos globales, facilitando la aplicación de sanciones y mejorando su capacidad para prevenir y mitigar los riesgos cibernéticos provenientes de actores externos. La penalización de los ciberdelitos ha progresado, pero todavía se encuentra con desafíos significativos en términos de su implementación eficaz.

Es necesario que la legislación se modifique continuamente para hacer frente a las nuevas modalidades de ciberdelitos que emergen con el progreso de la tecnología; los delitos cibernéticos son complejos, y las penalizaciones deben ser proporcionales al perjuicio provocado, teniendo en cuenta tanto el efecto económico como el peligro a la seguridad y la privacidad de las personas.

No obstante, la sanción no solo debe centrarse en sancionar a los transgresores, sino también en evitar estos crímenes a través de la disuasión. Además, frecuentemente los ciberdelincuentes operan en varios países, lo que dificulta la implementación de la ley. Esto convierte la colaboración internacional en esencial para luchar eficazmente contra el ciberdelito, la cooperación es esencial en la tarea de colaborar.

CONCLUSIONES

- El Perú ha progresado en la creación de un marco jurídico para combatir los delitos cibernéticos, resaltando la Ley N ° 30096 y el Decreto Legislativo N° 1412. Estas regulaciones tienen como objetivo salvaguardar la información personal y los sistemas vitales ante las amenazas digitales. No obstante, la escasez de infraestructura, personal técnico y personal especializado restringe la eficacia de estas normativas. Esto pone de manifiesto la importancia de políticas más sólidas que fusionen la penalización penal con acciones preventivas y educativas para establecer un ambiente digital seguro.
- Es esencial fomentar una cultura de ciberseguridad para combatir el hackeo y otros crímenes cibernéticos. Es fundamental implementar programas de educación y talleres prácticos en instituciones académicas y empresas para promover prácticas seguras en el uso de tecnología. Estos esfuerzos deben ser complementados con campañas de concienciación en masa, orientadas a jóvenes y adultos, con el fin de crear conciencia acerca de los peligros en ambientes digitales. Esta perspectiva no solo disminuye la vulnerabilidad de las personas, sino que también potencia la capacidad de resistencia colectiva ante las amenazas, fomentando conductas responsables y la salvaguarda activa de la información.
- Considerando que los delitos cibernéticos no tienen límites, resulta esencial que Perú colabore de cerca con otras naciones y entidades internacionales. Mediante convenios como el Convenio de Budapest, se puede potenciar la habilidad para localizar y sancionar a los ciberdelincuentes, además de implementar normas internacionales de ciberseguridad. Esta colaboración no sólo robustece la reacción frente a ataques, sino que también promueve la confianza en el ambiente digital, esencial para el progreso económico y social.
- La lucha contra el hackeo demanda una perspectiva multidisciplinaria que fusiona leyes, tecnología y educación. Las auditorías periódicas, el uso de tecnologías de protección de vanguardia y la simulación de ataques son instrumentos esenciales para detectar y minimizar las vulnerabilidades. Este enfoque holístico debe estar apoyado por fuertes políticas públicas y un esfuerzo compartido entre el gobierno, el sector privado y la sociedad civil para asegurar la seguridad digital a largo plazo.

REFERENCIAS:

- Álvarez, M., & Montoya, H. (2020). Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos. *Ingeniería y Desarrollo*, 38(2), 279-297.
- Arocena, G. (2012). La Regulación De Los Delitos Informáticos En El Código Penal Argentino. Introducción a La Ley Nacional Núm. 26.388. *Boletín Mexicano de Derecho Comparado*, XLV(135), Article 135.
- Arocena, G. (2012). La Regulación De Los Delitos Informáticos En El Código Penal Argentino. Introducción a La Ley Nacional Núm. 26.388. *Boletín Mexicano de Derecho Comparado*, XLV(135), 945-988.
- Blanco, H. (2021). El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre. *InDret*, 1. <https://doi.org/10.31009/InDret.2021.il.15>
- Bustillos, O., & Rojas, J. (2023). Cómo promueven los estados la ciberseguridad de las pymes. *Interfases*, 17, 21-37.
- CIBERNOS. (2024). *Ciberseguridad: Guía para prevenir ataques cibernéticos*. <https://www.grupocibernos.com/blog/ciberseguridad-guia-para-prevenir-ataques-ciberneticos>
- Congreso de la República. (2013, septiembre 26). *Delitos informaticos*. [https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/\\$FILE/6_Ley_30096.pdf](https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf)
- Espinoza, M. (2018). El Derecho Penal Informático Humano Como Cautela Frente Al Poder Punitivo En La Sociedad De Control. *Revista de Derecho*, 3(2), 233-245.
- Gabriel, J. (2017). Cómo se genera una investigación científica que luego sea motivo de publicación. *Journal of the Selva Andina Research Society*, 8(2), 155-156.
- Galicia, J. (2018). Conceptualización De Una Estrategia De Ciberseguridad Para La Seguridad Nacional De México. *Revista Internacional de Ciencias Sociales y Humanidades, SOCIOTAM*, XXVIII(2). <https://www.redalyc.org/journal/654/65458498003/>

- Gamón, V. P. (2017). Internet, la nueva era del delito: Ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, 20, 80-93.
- García. (2024). *El papel del Hacking Ético en la seguridad informática*. <https://grupocesa.com/el-papel-del-hacking-etico-en-la-seguridad-informatica/>
- Garcia, S. (2016). *Impacto Económico de la Ciberdelincuencia en América Latina*.
- Guaña, J. (2023). *Revolución de la ciberseguridad en la cuarta revolución industrial*. 21/07/2023. [Revolucion_de_la_ciberseguridad_en_la_cuarta_revol.pdf](https://www.revolucionde.com/revolucion_de_la_ciberseguridad_en_la_cuarta_revol.pdf)
- Gutierrez, E. D. L., Gomez, C. M. T., Arcaya, Y. A. E., & Montoya, L. A. G. (2022). Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital. *Innovación y Software*, 3(2), 109-120.
- INTERPOL. (2020). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19*. <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19>
- Jimenez, J. (2022). *Ciberdelincuencia: Evolución y relación con la actual situación de pandemia. Nuevas modalidades y problemáticas*. https://gredos.usal.es/bitstream/handle/10366/150144/TG_Jim%C3%A9nezRozas_Ciberdelincuencia.pdf?sequence=1&isAllowed=y
- Machín, N., & Gazapo, M. (2016). La Ciberseguridad Como Factor Crítico En La Seguridad De La Unión Europea. *Revista UNISCI*, 42, 47-68.
- Moran, A. M. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *Revista IUS*, 15(48), Article 48.
- Presidencia del Consejo de Ministros. (2020). *DECRETO DE URGENCIA No 007-2020*. <https://www.gob.pe/indecopi>
- Puime, J. (2009). *EL CIBERESPIONAJE Y LA CIBERSEGURIDAD*. <https://dialnet.unirioja.es/descarga/articulo/4549946.pdf>

- Reyna, & Olivera. (2016). *Análisis de los Ciberataques Realizados en América Latina*. https://www.researchgate.net/publication/331809038_Analisis_de_los_Ciberataques_Realizados_en_America_Latina
- Riquelme, Aranda, & Salinas. (2024). No se trata de saber si te van a atacar, sino cuándo: Ciberseguridad para empresas. 28/10/2024. <https://www.latercera.com/publiirreportajes/noticia/no-se-trata-de-saber-si-te-van-a-atacar-sino-cuando-ciberseguridad-para-empresas/5JFWFS47UZEU3PAKNQK2U7XALQ/#>
- Santos, M., Barrios, Á., & Vines, P. (2019). El hacking como comportamiento típico en las nuevas formas de delincuencia organizada. *Espiraes revista multidisciplinaria de investigación científica*, 3(26). <https://www.redalyc.org/journal/5732/573263325006/>
- Scariot, N. (2021). *La cultura hacker como filosofía de vida en la era del capitalismo cibernético. Una aproximación al caso en Mendoza*. https://bdigital.uncu.edu.ar/objetos_digitales/17070/47-scariot-ponencia-ed.pdf
- Stepke, F. L. (2017). Institucionalidad Y Bioética: Tecnificación, Mercantilización, Democratización Y Globalización. *Acta Bioethica*, 23(1), 7-8.
- Symantec. (2014). *Tendencias de seguridad cibernética en América Latina y el Caribe*. <https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf>
- The Bridge. (2024). *Hacking Ético, por qué es tan importante*. <https://thebridge.tech/blog/hacking-etico-por-que-es-tan-importante>
- Verdesoto, A. (2007). *Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones*. <https://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf>

IMPACTOS DE LOS MEDIOS DIGITALES Y EL MARCO LEGAL DE LOS DERECHOS DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Brenda Falcón-Alcántara¹

RESUMEN

Todo el avance que se produjo en las tecnologías de información y comunicaciones transformaron la forma en la que las personas se comunican y gestionan sus datos, lo que produjo la urgente necesidad de salvaguardar jurídicamente la privacidad y los datos personales.

En este artículo se analizó no sólo los riesgos que enfrentan las personas al exponer sus datos en línea, sino también aborda el origen que tiene el derecho de privacidad y de datos, así como las normativas que las regulan y desafíos que enfrentan también la protección de menores en el entorno digital.

Palabras claves: protección de datos, privacidad, derechos, normativa, inteligencia artificial.

ABSTRACT

All the advances that occurred in information and communication technologies transformed the way in which people communicate and manage their data, which produced the urgent need to legally safeguard privacy and personal data.

This article analyzed not only the risks that people face when exposing their data

¹ bfalcona1@upao.edu.pe

Programa de Estudio de Derecho, Universidad Privada Antenor Orrego

online, but also addresses the origin of the right to privacy and data, as well as the regulations that regulate them and challenges that also face the protection of minors in the digital environment.

Keywords: data protection, privacy, rights, regulations, artificial intelligence.

INTRODUCCIÓN

Absolutamente todo se encuentra dominado por tecnologías de información y comunicaciones, como prueba de eso, son los constantes inventos de programas y servicios que permiten acceder a las personas a nuevas maneras de comunicarse y relacionarse. Estos progresos tecnológicos son los que han dado lugar a medios digitales, los cuales permiten la gestión automática de la información, creando una necesidad de brindar cierta protección jurídica a los datos personales, resaltando sobre todo aquello que pueda dañar o afectar a la privacidad de éstas.

Este artículo encontró su razón en brindar información que sirva de ayuda, para lo que resulta necesario, tener en cuenta los riesgos del internet, los posibles mecanismos que resulten idóneos para mantener protegidos los datos que son brindados o expuestos en la red, así como también, los diversos modelos de inteligencia artificial que son los encargados de recopilar datos que se encuentren ya sea de manera pública y también privada.

Con esto, Roig (2009) afirmó que en Europa, la privacidad ha quedado enmarcado en el derecho de protección de datos personales, teniendo como punto base, al artículo 18.4 de la constitución española donde se limita el uso de la informática para de ese modo garantizar la identidad personal y familiar de todos los ciudadanos que naveguen en internet y sepan de los posibles peligros a los que se enfrentan.

Entonces, toda la información que se brinde o exponga en el internet, advierte Sobrino (2019), forma parte de la intimidad; por tanto, se puede decir que la intimidad y la vida privada se muestran como el borde entre lo público y lo privado; ahora bien, teniendo en cuenta lo referido, en el derecho, la intimidad resulta ser como la manifestación jurídica socialmente de alto relieve, siendo ésta la base para que se respete y reconozca el espacio restringido que cada persona tiene frente a terceros.

Los medios digitales para Domínguez (2023), no simplemente se han introducido a las vidas de las personas, sino que las han transformado; por eso, es necesario saber cómo poder sacar ventajas de las tecnologías

digitales y a la vez también cómo protegerse de que éstas no lleguen a violentar la privacidad. Demasiadas compañías digitales almacenan los datos personales, en donde algunas plataformas como por ejemplo lo es Facebook, permite que varias personas localicen a sus posibles víctimas para violentarlas, esto supone un gran problema debido a la exposición en esta plataforma.

Así mismo, Gapsalamov et al (2020), señaló que las redes sociales al poseer un alto valor económico hacen que el riesgo a la privacidad aumente, provocando que se busque con mayor intensidad los datos de los usuarios para que se puedan suplantar sus identidades y obtener un provecho generando de esta manera un daño en las personas.

Siendo así, de acuerdo con lo sostenido por Villén-Contreras et al., (2024), es importante destacar que la introducción de tecnologías digitales ha permitido que surja el interés sobre la educación digital y cómo manejarla correctamente para que resulte favorable, recurriendo a la implementación de talleres de formación digital para aprender todo lo referido al uso de las redes sociales, aplicaciones y sitios web donde se suelen colocar datos personales, así como también, fomentar una cultura de respeto y ética.

No obstante, de acuerdo con Sobrino (2019), sólo es hasta casi el término del siglo XIX donde se logró conformar el derecho a la intimidad. El derecho a la privacidad fue reconocido en primer lugar por tribunales americanos y luego por la Declaración Universal de Derechos Humanos, donde se resaltaba la importancia de proteger el espacio privado o íntimo, de la invasión de terceros y también del control en la toma de decisiones que se presentan en ese ámbito.

Es así que lo que se pretende abordar en este artículo, es saber el origen del derecho a la privacidad y protección de datos, las normativas y leyes que la regulan, así como también, los desafíos que éste enfrenta; y conocer los peligros a los que se enfrentan los menores de edad y como se regula su derecho en los cuando se exponen en los medios digitales.

METODOLOGÍA

Esta investigación precisó como objetivo describir los alcances que pueden tener los medios digitales respecto a la protección de datos que se brindan de manera confiada en internet para realizar cualquier tipo de actividad; así mismo, analizar los peligros que existen en la web y saber cómo poder

interactuar de manera segura en la misma teniendo un conocimiento pleno de la educación digital para que no se vulneren los derechos a la privacidad de las personas.

La investigación acogió un enfoque cualitativo, así también denominada también como enfoque interpretativo o naturalista- humanista, que se centra principalmente en estudiar los alcances de la vida en sociedad y de los comportamientos humanos; también, para esta investigación se utilizaron fichas bibliográficas y varias bases de datos de las cuales se obtuvieron la información adecuada, tales como: Redalyc, Ebsco y Google académico, haciendo una exhaustiva revisión bibliográfica de los artículos que se encuentran en dichas plataformas.

Para la investigación se analizaron 30 artículos obtenidos de dichas fuentes, teniendo como diseño uno no experimental-descriptivo y un tipo básico, los mismos que brindaron una respuesta a interrogantes referidos no solo a los impactos de los medios digitales en la protección de datos; sino, también a las diversas normativas internacionales que se encargan de regular los derechos de privacidad y protección de datos, así como también, el origen de los mencionados derechos que a lo largo del tiempo se han desarrollado y que se volvieron muy relevantes por el avance tecnológico en las comunicaciones.

La duración de esta investigación se realizó desde el mes de agosto hasta las últimas semanas de noviembre, obteniendo resultados en base a ciertas interrogantes, empezando por saber qué es y cuál es el origen del derecho a la privacidad y datos; cuáles son los desafíos normativos que enfrenta este derecho ante la incidencia de la inteligencia artificial, qué normativas regulan el derecho de protección de datos y que impactos consigo la normativa que protege la protección de datos de menores de edad y a que riesgos se enfrentan estos por el mal uso del internet.

RESULTADOS

1. Origen del derecho a la privacidad y a la protección de datos

La evolución del derecho a la privacidad y protección de datos para Robles Osollo (2021), significó pasar de ser uno de los derechos más antiguos a ser considerado en estos tiempos una preocupación importante en el mundo moderno; debido a que surgió como una demanda contra la injerencia del Estado en la vida privada de las personas, siendo de esta manera uno de los primeros derechos exigidos al Estado en la historia

Valiéndose así de instrumentos internacionales para ello, tales como Declaración Americana de los Derechos y Deberes del Hombre (1948), Declaración Universal de los Derechos Humanos, Pacto Internacional de Derechos Civiles y Políticos (1966), Convenio Europeo para la Protección de los Derechos Humanos (1950) y la Carta de los Derechos Fundamentales de la Unión Europea (2000).

Para Maqueo Ramírez *et al.* (2017), explicó que el derecho a la vida privada es muy reconocido tanto en sistema globales como regionales, y estuvo consagrado en tratados internacionales tales como la Declaración Universal de los Derechos Humanos (1948, art. 12), el Pacto Internacional de Derechos Civiles y Políticos (1966, art. 17), la Convención sobre los Trabajadores Migratorios (1990, art. 14) y la Convención sobre los Derechos del Niño (1989, art. 16).

Por otro lado, respecto al derecho a la protección de datos, éste no se encontraba expresamente señalado en estos tratados internacionales, sin embargo, en el año 1980, el Consejo de Europa consideró incluirlo en la Convención Europea de Derechos Humanos, pero la idea fue eliminada porque no había suficiente experiencia, y en su lugar se trabajó en el Convenio 108, el cual fue el primer instrumento internacional sobre protección de datos.

Para Calle (2009), los derechos humanos surgieron a partir del siglo XVIII, en dónde se resaltó mucho la intervención de algunos pensadores como Locke y Mill, que a través de sus obras que las personas gozaban de una libertad entendida como aquella facultad de poder decir de todo lo que le pertenece sin la intervención de la sociedad e inclusión el Estado, aun viviendo bajos sus reglas.

Y consecuentemente, este derecho se instituyó como un derecho autónomo e independiente teniendo como principales instrumentos tales como la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Europea para la protección de los derechos humanos y de las libertades fundamentales entre otros más.

Más adelante, se llevó a cabo en diferentes estados la introducción de la protección de datos a sus normativas fundamentales, como por ejemplo lo sucedido con Portugal en su constitución de 1976, y así como también en la Constitución Española de 1978, por ser considerado como un derecho fundamental basado en la dignidad humana.

Por otra parte, para Gómez (2023) señaló que fue en la constitución española de 1978, específicamente en el artículo 18.4, que se reconoció que la ley va a limitar el uso de la informática para así poder garantizar la protección al honor e intimidad personal y también familiar de las personas, así como al ejercicio total de sus derechos.

Es así como, en España ha podido ser posible el reconocimiento de un derecho importante como lo es el de protección de datos y el avance legislativo, debido a que, con esta nueva implementación a su normativa, se pueden brindar respuesta a situaciones en relación a los medios digitales e informática, haciendo posible que los ciudadanos puedan ejercer su derecho a la protección de sus datos personales.

En general el derecho a la protección de datos tiene un reconocimiento constitucional, y este al igual que el derecho a la privacidad están reconocidos tanto en las constituciones latinoamericanas como europeas, como son el caso de las constituciones de Brasil, Argentina, Colombia, Perú, México o Venezuela, las cuales han implementado en sus normativas, leyes específicas que se encargan de velar por los derechos de ciudadanos ante cualquier vulneración a sus datos.

En cuanto al concepto de privacidad, Jiménez (2013) mencionó que el origen del derecho a la privacidad proviene del término inglés Privacy y que se puede relacionar con un aspecto personal reservada que tiene cada ser humano; de la misma manera hizo referencia acerca de una definición más amplia que brindó un juez americano de nombre Cooley a finales del siglo XIX, el cual dijo que la privacidad es el derecho a simplemente estar solo o estar en paz.

Así mismo, para Espinoza (2018), el concepto de privacidad hace referencia a la protección de la información personal y la confidencialidad de las actividades, tanto en la vida individual de una persona como en las acciones colectivas de grupos o empresas. De esta manera, es necesario que, con el uso de los diferentes medios digitales, se tenga mucho más miramiento respecto a la información que se comparte en estas.

También, para Serrano *et al.* (2017) mencionó que respecto al continente Europeo, el derecho a la protección de los datos personales y el derecho a la privacidad son reconocidos pero como derechos distintos; debido a que varias constituciones de algunos países de este continente acogen esta distinción en ambos derechos.

Además, también señala que mediante la Carta de los Derechos Fundamentales la cual fue adoptada en el año 2000, se estableció claramente que estos derechos son reconocidos de manera separada; especificando que en el artículo 7 se garantiza el derecho a la vida privada y familiar; y en su artículo 8, señalaba claramente que cada persona tiene derecho a que sus datos personales sean protegidos.

Para Roca (2020), señaló que fue en el sistema anglosajón, donde la privacidad se consideraba un derecho importante y fundamental que salvaguarda la personalidad de las personas; y que la protección de datos

es el medio para asegurar que este derecho se tutele, lo que significa que las leyes encargadas de la protección de datos van a ser la que salvaguarden la privacidad de las personas y prevengan los abusos referidos a la información personal, lo que quiere decir que, si alguien usa tus datos de manera indebida o ilegal, está violando tu privacidad

Es así como, el derecho a la privacidad les brinda a las personas la facultad de decidir sobre el manejo de su vida en general, por ello, se puede definir a este derecho como el poder que tienen las personas frente a terceros que quisieran intervenir en sus vidas, esto incluye incluso al propio Estado; además, ese derecho permite que las personas puedan decidir sobre con quienes comparten su espacio privado y que parte de este es público o no a través de los medios digitales, los cuales no solo han cambiado las formas de comunicarse, sino que cada vez van desarrollándose mucho más.

Por tanto, se entiende que el derecho de protección de datos brinda a las personas o usuarios el poder de decidir sobre cómo manejan su información en todos los medios digitales, desde el momento en que las exponen hasta el momento en que deciden quitar toda su información; aunque si bien es claro, este derecho no se encuentra reconocido explícitamente en la Declaración Universal de Derechos Humanos, en su artículo 12, donde se hace referencia de la limitada intervención del Estado en la vida privada de las personas, si representa un importante antecedente para este nuevo derecho como lo es el de la protección de datos.

Este derecho se ha implementado en muchos países latinoamericanos, tal es el caso por ejemplo el de México, que implementado en su normativa de nivel constitucional para todas las personas el derecho de protección de datos y que además también anudado dos leyes secundarias, como lo es la Ley Federal de Protección de Datos Personales en Posesión de los

Particulares de 2010 y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de 2017.

Por otra parte, el avance tecnológico que se ha logrado puede complicar que se garantice el cumplimiento del derecho a la privacidad y protección de datos expuestos en los medios digitales, esto se debe a la exposición de la información personal en estos medios; además, los diversos sistemas de Inteligencia Artificial (IA) pueden llegar a vulnerar este derecho y tomar esa información sin tener en consideración con el consentimiento y conocimiento del dueño de aquellos datos.

De esta manera, se advierte que el avance especialmente en este ámbito de la IA, dificulta que se pueda garantizar el derecho a la privacidad y a la protección de datos, porque mucha de la información obtenida es sin el consentimiento de los dueños de dicho datos, es por ello que los Estados de los diversos países a nivel latinoamericanos como europeos, han crearon diversas normativas específicas que aborden los retos que plantea la tecnología, así como también promover la conciencia y educación en torno a los derechos de protección de datos y fomentar una cultura de respeto hacia la información personal de todos.

2. Desafíos normativos del derecho a la protección de datos

Para Castroverde (2017) significó un desafío importante que afronta el derecho a la protección de datos, está relacionado con el ámbito territorial de aplicación a esta norma, debido a que el internet como tal es un entorno virtual donde las reglas tradicionales no pueden ser introducidas de manera fácil. Respecto a ello, en el año 1996 John P. Barlow, decía que veía a él internet como un espacio que no tenía fronteras y donde las personas podían hacer lo que quieran si estaban sujetas a leyes, las cuales no tenían cabida en este espacio puramente virtual.

Para Sánchez (2024), mencionó que el derecho a la protección de datos enfrenta retos muy complejos, en donde las personas viven una lucha constante por proteger sus datos dentro del mundo digital el cual cambia de manera constante, mencionando como las más principales a la falta de sistemas de ciberseguridad los cuales deben de mantenerse actualizados para poder enfrentar problemas emergentes, la falta de educación respecto a la ciberseguridad y último, la urgente necesidad de que las personas tengan conciencia y no expongan sus datos en medios digitales.

Teniendo en cuenta ello, es se pudo evidenciar que existe una conexión entre el derecho a la privacidad con el derecho a la protección de datos, esto se debe a que la protección de datos es diferente al derecho a la protección a la propia imagen, a la intimidad y al honor, porque aquel derecho básicamente se enfoca en el poder de manejo que tienen las personas sobre sus datos en las diversas plataformas digitales.

Además, es muy importante señalar que es fundamental la protección de este derecho, debido a que tutela las relaciones de las personas y son estas mismas que pueden acudir ante un organismo administrativo autónomo, ya sea para solicitar protección por haber sufrido una vulneración a este derecho o para solicitar el inicio de una investigación que tenga como finalidad imponer una sanción a los responsables.

Por tanto, la protección tanto a la privacidad como a la protección de datos de las personas en el internet genera constantes retos y sobre todo esto ocurre porque es considerado como un derecho fundamental y por ende esto implica que su tutela haya generado mayor preocupación frente a todos los peligros que ocurren en los medios digitales y en el internet en general; como por ejemplo falta de consciencia de las personas al brindar sus datos en internet, los peligros de la transmisión de datos a terceros, y la subestimación de la IA a la hora de inferir datos y reconocer la identidad del individuo mediante la elaboración de perfiles.

Por otro lado, de acuerdo a Alonso (2014), señaló varios retos que enfrenta el derecho a la protección de datos, advirtiendo cinco riesgos importantes. En primer lugar, señaló que uno de los retos está referido al conocimiento que las personas tienen sobre el control de sus datos, debido a que por una parte se cree necesario que las personas posean información detallada al momento de aceptar cualquier tratamiento que se le vaya a dar a sus datos, pero, sin embargo, ocurre que no siempre las personas leen todas las condiciones de privacidad y las que sí lo hacen muchas veces no logran entender políticas.

De esta manera, se genera un debate, en donde se discute si es mejor ofrecerle al usuario un texto completo y difícil de comprender; o si, un texto más corto y con lenguaje sencillo, para que así lo pueda leer y lo entienda; sin embargo, cabe la posibilidad también que con esta opción se puedan generar vacíos legales o incluso imprecisiones respecto a las políticas.

Pero, más allá de lo que respecta a si los usuarios leen o no las políticas, aún existe un problema adicional acerca del alcance en su consentimiento, y se trata de la finalidad, es decir, de acuerdo con el artículo 6 de la RGPD, solo se va a considerar como lícito el tratamiento de datos cuando el usuario haya brindado su consentimiento para fines específicos, por ello es necesario que la finalidad del uso de datos sea de manera clara y precisa para evitar cualquier vulneración a los derechos que usuario posee.

En segundo lugar, hay otro problema muy notorio y tiene que ver con los datos de las personas o usuarios que ya se encuentran en el ciberespacio, aunque si bien es cierto, en algunos casos los usuarios están sujetos a contratos en donde hay un compromiso respecto a la

eliminación de los datos después de un tiempo establecido. Pero simplemente la sola existencia de los perfiles de los usuarios genera que, aunque estos dejen de constantemente estar nutridos de información, podrían seguir habilitados para uso y hasta actualizarse de una manera más moderada como por ejemplo la recopilación de otros datos importante para la satisfacción de un servicio.

En tercer lugar, es importante destacar también que, en muchas oportunidades la privacidad no depende tan siquiera de los datos que brinde el usuario; y que se puede llegar a acceder a la información que no está expuesta del usuario, solo basta con solo tomar dicha información a través de un contacto que se encuentra en una red social. Respecto a esto, se analiza que los datos que los usuarios plasman como por ejemplo respecto al año de egresado, de su profesión e incluso domicilio, también se puede obtener la misma información, pero un usuario que no haya expuesto nada.

En cuarto lugar, existe un problema relacionado con lo que podría llamarse una “remuneración apropiada”, en donde básicamente el tema se centra qué cuánto deberían recibir las personas o usuarios como indemnización por todos los datos personales que recaban las plataformas digitales mientras éste haga uso de tales plataformas,

Por esto, incluso Meta (empresa que es dueña de Facebook e Instagram) pensó solicitar a los usuarios un costo de 13 euros al mes, para que puedan ingresar a sus redes sociales y esto servirá como una forma de compensación para ellos mismos ante la posible vulneración que sufra este último y que de alguna manera pueda cubrirse dicha indemnización a través del pago mensual.

Sin embargo, se tuvo que tener en cuenta que existe libertad para que las empresas establezcan los precios que quieren manejar sus negocios, es así que, entre Facebook y Netflix existen una gran comparación y diferencia, respecto que este último al igual que Facebook también les cobra a sus clientes el costo de 13 euros mensualmente, pero lo que lo diferencia de las redes sociales es la producción de contenido de alta calidad, mientras que por el otro lado, en Facebook e Instagram, el contenido es realizado por los propios usuarios,

Y por último lugar, existe un problema referido a los montos que establecen estas plataformas digitales antes mencionadas (Facebook, Instagram, etc.), para que los usuarios puedan acceder, debido a que se le impone a pagar o a no poder usarlas en ningún caso, sin tener la posibilidad de que puedan pagar una tarifa más baja por un servicio con menos beneficios.

Ante esto, es necesario que las empresas beneficien más a los usuarios, al permitir que sean ellos los que decidan qué planes de suscripción eligen y cuanto pagan por ello; así como también qué datos están dispuestos a compartir porque de así, si no aceptaran compartir sus datos, no renunciarían totalmente a al uso de estas plataformas.

De esta manera se podría beneficiar a que muchas más personas no abandonen las plataformas, dejando al libre albedrío de cada uno de ellos la elección que mejor se acomode a sus necesidades y salvaguarda sobre su privacidad, ganando ambas partes, equilibrando beneficios económicos para las empresas de estas plataformas y no vulnerando los derechos los usuarios.

Sin embargo, el problema principal se halló en que las personas no le prestan mucha importancia a su privacidad, esto se debe a que generalmente, piensan que compartir algunos datos en el internet no generara ningún problema, y esto no es del todo cierto, porque mientras menos personas cuiden su información, aumentará más el riesgo de que se utilice de forma inadecuada.

Esta falta de preocupación por la privacidad hace que muchas personas compartan información acerca de miedo, gustos, trabajo, familia y hasta incluso, datos de cuentas bancarias; y es donde la IA entra a cobrar relevancia, porque será ésta que recopila toda esa información la cual puede terminar en manos inescrupulosas y generar daños al titular de aquellos datos.

Teniendo en cuenta esto, es importante señalar que las normativas incluyendo leyes que existen para proteger la privacidad y protección de datos van a funcionar siempre y cuando sean las propias personas las encargadas de cuidar sus datos, teniendo mucho más miramiento al momento de navegar por internet y compartir datos.

Esto se debe a que muchas veces se cree que los datos personales no son valiosos ni peligrosos de compartir, siempre y cuando estos no afecten temas dinerarios o económicos. Pero, con el avance tecnológico, a través de la IA se pueden obtener toda esa información secreta, lo que va a generar que se sepa información personal de todo tipo, es por ello por lo que se incentiva a las personas a ser conscientes de todos los riesgos al conectarse por internet sin tomar todas las precauciones posibles.

Y solo se podrá tener conciencia, a través de una adecuada educación de la importancia que tiene el saber manejar los medios digitales, los peligros que en estas se encuentran y los datos que se brindan para realizar operaciones de cualquier tipo, siempre siendo precavidos en la aceptación de cualquier ventana emergente que aparezca mientras se está navegando en el internet.

Además, existe la necesidad de adaptar y fortalecer las normativas de los mencionados derechos, debido a que su regulación protege a los usuarios de transgresiones a su privacidad y promueve el uso ético de la información por parte de las corporaciones priorizando así la dignidad y libertad de las personas en el mundo digital que evoluciona constantemente.

3. Normativas regulan el derecho de protección de datos

Respecto a las normativas que regulan el derecho a la protección de datos para Macén (2021), expresó que el RGPD, el cual empezó a aplicarse en el año 2018 y es considerada una de los reglamentos a nivel mundial más importantes y reconocidas de la Unión Europea; en donde exclusivamente existen normas relacionadas a la protección de datos, garantizando de esta manera que las personas puedan circular sus datos de forma segura en los medios digitales y transferirlos entre países distintos.

Para Mañas (2016), señaló que la Unión Europea decidió fortalecer sus leyes acerca de la protección de datos y es por ello que creó un reglamento (RGPD) para que todos los países miembros de este lo puedan utilizar en sus legislaciones sin necesidad de que lo adapten, sino simplemente lo cumplan tal cual está establecido, y de esta manera no haya confusiones ni interpretaciones distintas, asegurando que los derechos de las personas este protegidas de manera uniforme.

Según Gómez (2023), el Reglamento El Reglamento General de Protección de Datos (RGPD) es la principal ley en toda Europa que se encarga de proteger los datos personales de las personas, su aprobación fue en el año 2016, pero se empezó a aplicar el 25 de mayo del 2018, reemplazando a la Directiva 95/46/CE. Este reglamento es muy importante y se aplica en todos los países perteneciente a la Unión Europea, debido a que en muchas oportunidades incluso se encuentra sobre las leyes nacionales, con ciertas excepciones.

El RGPD no solo se encarga de proteger los datos personales, sino que también salvaguarda el derecho a la privacidad, el respeto a la vida, al honor, y a la protección de la identidad de las personas, sin embargo, cabe la posibilidad que en ciertas circunstancias pueda afectar otro tipo de derechos, tales como el derecho de compartir y acceder a información o como el de la libertad de expresión.

Ahora bien, Giménez & Domenech (2018), mencionaron que este reglamento trae consigo mejoras relevantes que sirven para proteger los datos en esta época digital, señalando de esta manera algunas reglas importantes como:

1. **Consentimiento explícito:** se menciona en este reglamento que todas las organizaciones deben tener por parte de las personas un permiso claro y directo, siendo este consentimiento otorgado de una manera libre y muy bien informado; teniendo como invalido, un consentimiento indirecto o implícito.
2. **Derecho del usuario sobre sus datos:** Las personas o usuarios que hacen uso de los medios digitales, tienen derecho poder ver, corregir, borrar (lo que se conoce como el “derecho al olvido”), limitar y hasta transferir sus datos personales de manera libre y sin presiones.
3. **Notificación sobre caso de violación en la seguridad:** La normativa señala que se debe mantener informado al usuario en el caso de que, si por alguna violación o falla de seguridad y se vean afectados los datos personales de los mismo, es de completa obligación de las organizaciones o empresas avisar a las autoridades y usuarios afectados en un plazo máximo de 72 horas.
4. **Protección de los datos desde la estructura:** las empresas u organizaciones están obligadas a poder configurar sus sistemas y procesos para que puedan proteger los datos de los usuarios desde

el momento inicial y además deben anotar toda aquella actividad relacionada que ocurra con los datos personales.

5. **Responsabilidad de protección:** están obligadas las organizaciones o empresas a tomar las medidas necesarias para poder salvaguardar los datos personales de los usuarios y tomar responsabilidad en el caso que no cumplan con estas normas.
6. **Protección en la transferencia de datos fuera de la Unión Europea:** Las organización o empresas que envíen datos personales fuera de la Unión Europea deben tener precaución de que se mantengan estos datos seguros y se rijan por las normas del RGPD.
7. **Delegado de protección de datos (DPO):** Es disposición del RGPD que obliga a que todas las entidades públicas o privadas, determinen a un DPO, quien será la persona que se verá encargada de poder vigilar si las normas de protección de datos son cumplidas a cabalidad.
8. **Imposición de sanciones severas:** El RGPD señala que serán sancionadas aquellas organización o empresas que no cumplan con el reglamento, aplicando las sanciones más fuertes, con la finalidad de proteger los derechos fundamentales tanto como la privacidad, así como el de protección de datos.

El derecho a la protección de datos regulado en el RGPD de la Unión Europea ha generado un impacto en otros países de Latinoamérica específicamente; este reglamento ha tratado de unir y estandarizar aquellas normas que protegen este derecho para asegurar de esta forma que se pueda ofrecer a las personas una protección sólida y de esta manera reducir la inseguridad jurídica ante su vulneración.

Con esta unificación de normas, se busca que las empresas u organizaciones tengan un patrón adecuado para salvaguardar el mencionado derecho, y más aún en los casos de transferencia de datos que se realizan de manera internacional y para lo cual deben estar completamente regidos a los establecido respecto a protección.

Por tanto, partiendo por la finalidad que tuvo consigo el RGPD, el cual fue brindar un alto nivel de protección para las personas que viven dentro de la Unión Europea, garantizando de esta forma que se respete el derecho a la privacidad de datos personales en cualquier transacción que esta realice en cualquier plataforma digital a la que se conectó.

Es así cómo; este reglamento tuvo por objetivo que se redujeran todas leyes existentes relacionadas a salvaguardar el derecho a la protección de datos en los diversos estados que conforman la Unión Europea, debido a que esta proliferación aumenta la falta de su cumplimiento, así como también promovía la inseguridad jurídica.

Y se consiguió esta unificación de las normas que a través del RGPD, el cual ofreció a las personas titulares del derecho a la protección de datos, no se vean vulnerados sus derechos con las diversas interpretaciones que le puedan dar en cada caso particular las autoridades competentes, sino que, se rijan completamente a los establecido por aquel reglamento.

Por otro lado, Rueda (2012), mencionó que así mismo como existe el RGPD en la Unión Europea; en Latinoamérica, existen ciertos países que han adoptado sus propias normas de protección de datos personales, tomando en muchos casos particularidades de la normativa europea, en ese sentido se puede hacer una comparación de los países latinoamericanos al respecto:

1. **Argentina y Uruguay:** Estos países son reconocidos porque dentro de su legislación se puede apreciar que ha tomado como modelo a la RGPD de la Unión Europea manteniendo de esta manera un patrón alto, lo que permite también que se puedan transferir datos desde la Unión Europea hacia estos países sin necesidad de tener un respaldo adicional.
2. **Colombia:** Es con la Ley 1581 que Colombia tiende a asemejarse a la RGPD, pero prohíbe totalmente con esta ley que los países que no tengan una buena protección se pueda establecer transferencias de datos, excepto que cumplan con requisitos específicos; buscando de esta manera evitar que los datos personales puedan verse afectados en posesión de entidades que no cuentan las adecuadas medidas de protección.
3. **México y Perú:** Perú con la Ley 29733, ha establecido normas que exigen ciertas medidas de seguridad y confidencialidad acerca de la afluencia transfronteriza de datos; mientras que México con su Ley Federal de Protección de Datos Personales en Posesión de los Particulares, aprueba que las transferencias de datos internacionales puedan darse entre encargados y responsables del tratamiento de datos.
4. **Brasil:** A través de su Ley 13.709, la cual sigue de ejemplo al RGPD sobre todo respecto a la transferencia de datos internacionalmente,

requiriendo que se cumplan ciertos requisitos para salvaguardar la protección. Esta Ley obliga a que los países que recepcionan estos datos brindan un nivel alto de protección, tal y como se ve establecido por los principios del RGPD.

Los niveles de protección que posee el RGPD de la Unión Europea ha influenciado de manera beneficiosa en Latinoamérica; debido que, por una parte, estos países pueden tomar como referencia al RGPD mejorando el comercio internacional con la Unión Europea. Además, estas normas traen consigo que las personas puedan confiar en el manejo de sus datos, reduciendo que se vulneren su derecho de protección de datos evitando abusos en la recolección y uso de estos.

El RGPD es un reglamento de referencia a nivel mundial respecto a la protección de datos, buscando que se pueda brindar el máximo nivel de protección a los titulares de este derecho tan importante y fundamental pero principalmente asegurando la seguridad jurídica para todas las personas que hacen uso de los medios digitales.

4. Protección de datos de menores de edad y riesgos a los que se enfrentan

Respecto a la protección de datos para menores, para Díaz (2019), señaló que la protección de menores está basada en el principio de su interés superior, el cual fue señalado en la Cumbre Mundial de Protección Infantil de 1990, en donde se afirmó en que era una prioridad esencial proteger a los niños como muestra para la estabilidad y el progreso de la humanidad. Así mismo, señaló que, en la convención de los derechos del niño, se estableció que, debido a la inmadurez innata de los niños, necesitan mayor cuidado y protección porque son más propensos a estar expuestos al peligro.

Para Rodríguez (2018), señaló que la protección de datos de los menores de edad que navegan en internet, tiene como principal objetivo proteger sus intereses y evitar que se vulneren sus derechos, para ello, es necesario aplicar el principio del interés superior del menor, el cual alude que cualquier sea el acto o decisión que afecte directamente el bienestar de los niños, debe priorizar siempre lo que le hace bien a ellos, antes de cualquier otro interés.

Para Gómez (2023), menciona que este derecho está regulado en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) de España, el cual suplementa al RGPD de la Unión

Europa; esta ley considera que estado de vulnerabilidad que caracteriza a los menores, requiere de una protección de datos especial para los mismos, incluyendo de esta manera el “derecho digital de los menores” que navegan en internet.

De acuerdo con el art.84 de la LOPDGDD, son responsables de que los menores utilicen de manera equilibrada los medios digitales, los padres o los tutores de estos, para que de esta manera se conserve su dignidad y no se vulneren sus derechos. Además, también en el artículo 92 se resalta la importancia del interés superior del menor en los que respecta a la transmisión de sus datos y todo lo que realice en las redes sociales, para lo cual se necesita un consentimiento directo y teniendo en cuenta siempre el bienestar del menor antes que otro tipo de interés, como puede ser el de los colegios educativos.

Respecto al consentimiento que deben brindar los menores, el RGPT determina la edad mínima que debe tener el menor para que puedan ofrecer su consentimiento al uso de sus propios datos, y es de 16 años, y solo son en ciertas circunstancias que esta ley consiente cambiar hasta los 13 años a algunos Estados. Además, con la finalidad de salvaguardar la privacidad de los menores, tanto empresas como organizaciones deben de acoger medidas de seguridad muy buenas, para evitar que la información que es brindada por los menores de edad resulte transgredida.

Para Guillén (2015), señaló respecto a la obtención y cesión de los datos en los menores de edad que, existe un límite netamente legal para que estos puedan dar su consentimiento sobre el uso de sus datos y el cual está establecido únicamente a los 14 años, y que por el contrario de acuerdo al RGPD, los niños que sean menores de 13 años solo podrán dar su consentimiento a través de su padre o tutor.

Por otra parte, es importante resaltar la importancia que toma la educación digital dentro de este marco en protección a los menores, debido a que es necesario fomentar el uso responsable y seguro de las Tecnologías de Información y Comunicación (TIC), señalando de esta manera que es en el art. 83 de la LOPDGDD, en donde se exige que la enseñanza dentro de los centros educativos brinde información acerca del manejo de los medios digitales, teniendo este una perspectiva inclusiva; empezando por los docentes quienes deban tener esta formación y que pueden informar sobre aquello a los menores.

Esta enseñanza hacia los menores en sus centros educativos es vital, debido a que son ellos los que más riesgos corren al utilizar los medios digitales, viéndose expuestos su seguridad y hasta incluso la de su familia; por ello, los riesgos a los que se enfrentan son los siguientes:

1. **Aislamiento social:** Esto se produce porque el uso excesivo de dispositivos y redes sociales en los menores puede llegar a ser más importante que realizar otro tipo de actividades, tales como el deporte, la lectura, canto; provocando sobrepeso, sedentarismo y una grave adicción al uso de tecnologías.

Para Urbina (2021), afirmó que el aislamiento social puede afectar de manera muy negativa el bienestar psicológicos de los niños, debida a la poca interacción física que tienen con otras personas y a causa de esto, ellos pueden llegar a experimentar emociones como la tristeza, desesperanza o inseguridad; además de mostrar comportamientos que normalmente no ocurrirían normalmente.

2. **Acceso a sitios web inapropiados:** Los menores experimentan mucha curiosidad relacionada a lo nuevo, y es que mediante esta sensación pueden recurrir a contenidos de índole sexual o violentos, aunque de alguna manera haya programas para poder bloquear el acceso a ese tipo de páginas.

Para García-Piña (2008), los niños y adolescentes que acceden de manera fácil al internet, se llegan a encontrar con contenido violento y sexual que muchas veces son enviado en forma de spam(correos no deseado), lo cual puede generar interés en la sexualidad de manera prematura; así como también generar una adicción a navegar constantemente en la web y que desencadenaría en necesitar apoyo psicológico eventualmente.

3. **Cyberbullying:** este es un tipo de acoso muy parecido al bullying, la diferencia radica en que solo ocurre en el medio digital; y mediante perfiles falsos, permite que los acosadores maltraten a través de insultos en las páginas web a los menores, provocando que se afecte su autoestima, ansiedad y se termine alejando de todas las personas.

Para Hernández & Solano (2012), el cyberbullying consistió en utilizar las plataformas digitales, tales como correos electrónicos, mensajes de texto, o redes sociales para maltratar o acosar a una persona con el objetivo de hacerle mucho daño; incluyendo comportamientos como

amenazas, insultos, discriminación, que con realizados de forma anónima y eso dificulta que la persona agredida pueda identificar al agresor.

4. **Grooming:** Hace referencia al acoso que vive un menor por parte de un adulto manipulándolo para recibir contenido de índole sexual; muchas veces los menores no se dan cuenta de este tipo de abuso y no lo toman en cuenta por muchos factores, como el miedo, amenazas, vergüenza, etc.

Para Santisteban *et al.*(2017), consideró que el grooming online, es realizado por una persona adulta, la cual utiliza las tecnologías de información(TIC) o medios digitales para persuadir, manipular y victimizar sexualmente a un menor, valiéndose de información de contenido sexual del menor obtenida por éste.

5. **Sexting:** Básicamente se trata del intercambio de contenido sexual que realizan los menores, sin tener en cuenta que una vez compartido, aquello puede resultar en un acoso o extorsión por la otra parte, afectando de esta manera la estabilidad emocional del menor.

Para Caldera (2013), determino que el termino sexting combina dos palabras, la primera “sex” (sexo) y la segunda “texting” (mensajes enviados), refiriéndose así al envío de videos o fotos que tienen contenido sexual, a través de los celulares.

Dichas imágenes suelen ser recreadas por la misma persona que es protagonista en ella o hasta incluso pueden ser robadas; por ello es muy importante tener en cuenta factores como el origen de la imagen, el contenido en ella, la edad del protagonista y la identidad de este.

6. **La no privacidad:** Esto se ve reflejado en la información que suele colocar el menor en cualquier medio digital o red social, tales como la dirección de su casa o número celular, permitiendo de esta manera que personas malas puedan obtener esta información y hacerles daño; por ello, es necesario revisar las opciones de privacidad para proteger los datos sensibles.

Para Acedo *et al.* (2016), consideró que debido a los cambios que ha tenido la sociedad, la mayoría de niños utilizan de manera constante las nuevas tecnologías, incluso convirtiéndose en adictos a estas, poniendo en una situación de riesgo su privacidad; y eso se debe

la información que comparten en algunas plataformas sin tener en cuenta los peligros que corren al exponerse de esa forma.

7. **Contacto con extraños:** Esto se produce porque en internet es muy fácil la creación de perfiles falsos, lo cual permite que acosadores puedan mantener contacto con menores de edad, con la finalidad de aprovecharse de los mismos, a través de engaños y manipulaciones.

Para Catalina-García et al. (2014), considero que los adolescentes son los asumen mayores riesgos respecto al contacto con desconocidos en internet, y eso se debe a que buscan amigos nuevo o intenta coquetear, aceptando así solicitudes de personas que no conocen en sus redes sociales con esos propósitos, y esta es una de las principales causa que provocan situaciones peligrosas como el acoso o posibles amenazas para ellos mismos.

Se resaltó la importancia acerca de la necesidad de que tanto los centros educativos como los padres puedan supervisar y encaminar a los menores en el uso responsable de los medios digitales, para que de esta manera puedan aprovechar de todos los beneficios que les brinda la tecnología para su desarrollo educativo y recreativos, pero sin dejar de lado las precauciones necesarias acerca de la información que brindar a ciertas páginas y que pueden provocarles algún perjuicio, vulnerando sus derechos.

También, resultó de gran importancia señalar que el derecho a la protección de datos en menores dentro de la tecnología digital es un aspecto muy delicado en la sociedad, porque se normaliza el uso del internet y demás medios digitales para niños; es por ello, resulta primordial el papel que juegan los padres y también los centros educativos para salvaguardar los derechos de los menores.

Ahora bien, dentro del contexto digital que se vive, se pudo identificar que más del 90% de los menores ya manejan con mucha rapidez los medios digitales, siendo usuarios activos dentro del internet, y esto, no solo mostró un aspecto de entretenimiento, sino que la exposición sin miramientos por parte de los éstos, puede afectar de forma negativa su desarrollo y bienestar, debido a los peligros que existen en el internet.

Y es respecto a ello lo más preocupante, debido a que los peligros que enfrentan los menores en el internet al usar los medios digitales, pueden provocar daños irreparables; por ejemplo, como el ciberbullying y el grooming que afectan gravemente su autoestima, la forma de comportarse y hasta incluso puede afectar a su rendimiento escolar.

Además, el acceso que tienen los menores a redes sociales es cada vez más común, haciéndolos más propensos a sufrir cualquier tipo de abusos por parte de personas anónimas, que se esconden en perfiles falsos, para entablar alguna amistad con ello y de esta forma ganarse su confianza, para luego manipularlos y forzarlos a realizar acciones que no desean.

También resultó importante el recalcar que el sexting y la transmisión de contenido de índole sexual el cual no siempre es autorizado por el menor, requieren de un miramiento mayor; y esto se debe, a la falta de conciencia que pueden tener los menores al exponerse brindando imágenes con alto contenido sexual, porque no analizan que pueden verse involucrados en una situación extorsiva, situación que puede provocar depresión y llevarlo al aislamiento total ante la vergüenza de las posibles divulgación acerca de su contenido.

Y, por último, resultó importante señalar también, la facilidad que pueden tener los menores para acceder a páginas inadecuadas e interactuar muchas veces con extraños, porque a pesar de que existan ciertos mecanismos que sirven para bloquear ese tipo de páginas, la verdad es que muchos menores saben incluso como evadir aquellos sistemas. Es por ello, que resulta necesaria la educación que puedan recibir todos los menores respecto al uso de medios digitales, teniendo presente siempre los riesgos al que son propensos y evitar efectos negativos.

Es por ello, que el reconocido derecho de la protección de datos en menores resulta de mucha importancia para el desarrollo de una sociedad correcta y libre de abusos, respetándose los unos a otros, pero en especial a los menores de edad, debido a que son éstos lo que demandan mayor atención a la salvaguarda de sus derechos y evitando de esta manera que se vean vulnerados por situaciones que pueden generarse problemas graves en sus vidas.

CONCLUSIONES

- En este artículo se logró comprender el origen del derecho a la privacidad y a la protección de datos, determinando que ambos derechos se han consolidado en el siglo XX con el Convenio Europeo para la protección de derechos humanos y en la Convención Americana de los Derechos Humanos.

- Además, se logró identificar los desafíos que enfrenta la normativa del derecho a la protección de datos, encontrándose principalmente al respecto; a la falta de conciencia por parte de los usuarios respecto de los peligros a los que se ven expuestos cuando utilizan o manejan sus datos sin precauciones y cómo interfiere la IA en la recolección de los mismos sin el conocimiento de los titulares.
- También se logró examinar al Reglamento General de Protección de Datos (RGPD) que es la principal ley que se encarga de proteger los datos personales de las personas y cómo ésta se ha transformado en un referente a nivel mundial; influenciando de manera positiva en la normatividad de algunos países latinoamericanos mejorando principalmente la confianza de los usuarios y en la seguridad jurídica.
- Finalmente, también se logró explicar el derecho a la protección de datos de menores de edad y a que riesgos se ven expuestos, saltándose el grooming y el cyberbullying como los principales; además de la importancia que tienen tanto los centros educativos como los padres para supervisar y encaminar a los menores en el uso responsable de los medios digitales.

REFERENCIAS

- Acedo, Á., Platero Alcón, A., Acedo Penco, Á., & Platero Alcón, A. (2016). La privacidad de los niños y adolescentes en las redes sociales: Referencia especial al régimen normativo europeo y español, con algunas consideraciones sobre el chileno. *Revista chilena de derecho y tecnología*, 5(2), 63-94. <https://doi.org/10.5354/0719-2584.2016.42557>
- Alonso, C. (2014). Protección de datos en la esfera privada. retos y perspectivas del marco legislativo europeo. Recuperado 8 de noviembre de 2024, de https://diposit.ub.edu/dspace/bitstream/2445/214356/1/TFM_CeciliaAlonso_ProteccionDatos.pdf
- Caldera, M. I. F. (2013). *Sexting: nuevos usos de la tecnología y la sexualidad en adolescentes*.
- Calle, S. B. (2009). Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia. *Precedente Revista Jurídica*, 119-136. <https://doi.org/10.18046/prec.v0.1459>

- Castroverde, D. C. (2017). *Los retos de la protección de datos en internet. caso google spain y derecho al olvido (I)*.
- Catalina-García, B., López De Ayala López, M. C., & García Jiménez, A. (2014). Los riesgos de los adolescentes en Internet: Los menores como actores y víctimas de los peligros de Internet. *Revista Latina de Comunicación Social*, 69, 462-485. <https://doi.org/10.4185/RLCS-2014-1020>
- Diaz Luis, A. (2019). *Tratamiento de datos de los menores de edad en las Redes Sociales*. Recuperado 20 de noviembre de 2024, de <https://riull.ull.es/xmlui/bitstream/handle/915/23568/Tratamiento%20de%20datos%20de%20los%20menores%20de%20edad%20en%20las%20Redes%20Sociales.pdf?sequence=1&isAllowed=y>
- Domínguez Horner, A. (2023). Privacidad es poder. *Tópicos. Revista de Filosofía*, 66, 519-525. <https://doi.org/10.21555/top.v660.2656>
- Espinoza, A. I. M. (2018). Empresa y privacidad: El cuidado de la información y los datos personales en medios digitales. *Revista IUS*, 12(41), 293-310.
- Gapsalamov, A. R., Akhmetshin, E. M., Bochkareva, T. N., & Vasilev, V. L. (2020). «Digital Era»: Impact on the Economy and the Education System (Country Analysis). *Utopía y Praxis Latinoamericana*, 25(Esp.10), 170-186.
- García-Piña, C. (2008). Riesgos del uso de internet por niños y adolescentes. Recuperado 20 de noviembre de 2024, de <https://www.redalyc.org/pdf/4236/423640313006.pdf>
- Giménez, A. O., & Domenech, J. J. G. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. *Revista de la Facultad de Derecho*, 44, 1-35.
- Gómez, C. G. (2023). *Protección de datos, menores de edad y redes sociales*.
- Guillén Catalán, R. (2015). Los retos de la sociedad ante la protección de datos de los menores. ISSN: 2070-8157, pp. 324-343.
- Hernández Prados, M. Á., & Solano Fernández, I. M. (2012). CIBERBULLYING, UN PROBLEMA DE ACOSO ESCOLAR. *RIED. Revista Iberoamericana de Educación a Distancia*, 10(1). <https://doi.org/10.5944/ried.1.10.1011>

- Jiménez, D. L. (2013). Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital: Apreciaciones desde el Derecho español. *Estudios Constitucionales*, 11(2), 575-614.
- Macén, A. G. (2021). El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea. *CUADERNOS DE DERECHO TRANSNACIONAL*, 13(2), Article 2. <https://doi.org/10.20318/cdt.2021.6256>
- Mañas, J. L. P. (2016). *I. INTRODUCCIÓN. HACIA UN NUEVO MODELO EUROPEO DE PROTECCIÓN DE DATOS*.
- Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de derecho (Valdivia)*, 30(1), 77-96. <https://doi.org/10.4067/S0718-09502017000100004>
- Robles Osollo, A. G. (2021). El derecho a la privacidad y la protección de datos personales transfronterizos. *Revista Eurolatinoamericana de Derecho Administrativo*, 8(1), 35-60. <https://doi.org/10.14409/redoeda.v8i1.9543>
- Roca, A. P. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, 108, Article 108. <https://doi.org/10.5944/rdp.108.2020.27998>
- Rodríguez, A. C. (2018). *Protección de Datos: Especial incidencia en los menores y el uso de las redes sociales*.
- Roig, A. (2009). E-privacidad y redes sociales. *IDP. Revista de Internet, Derecho y Política*, 9, 42-52.
- Rueda Gómez, D. (2012). Regulaciones nacionales e internacionales en materia de protección de datos personales. retos globales en la actual era digital. Recuperado 8 de noviembre de 2024, de <https://repositorio.uniandes.edu.co/server/api/core/bitstreams/b15eb3d0-9657-4485-bc89-c6606f970da6/content>
- Sánchez Díaz, M. F. (2024). Inteligencia artificial generativa y los retos en la protección de los datos personales. *Estudios en derecho a la información*, 18, 179-205.

- Santisteban, P. de, Gámez-Guadix, M., Santisteban, P. de, & Gámez-Guadix, M. (2017). Estrategias de persuasión en grooming online de menores: Un análisis cualitativo con agresores en prisión. *Psychosocial Intervention*, 26(3), 139-146. <https://doi.org/10.1016/j.psi.2017.02.001>
- Serrano, I., Pérez, J. P., & Mora-Martínez, E. O. (2017). *MARÍA JOSÉ JORDÁN PALET*.
- Sobrino García, I. (2019). Protección De Datos Y Privacidad. Estudio Comparado Del Concepto Y Su Desarrollo Entre La Unión Europea Y Estados Unidos. *Revista de Derecho UNED*, 25, 687-713.
- University of Hull, UK, & Urbina García, M. Á. (2021). –1–año 12 | número 22 | enero-junio 2021 | ISSN 2007-2171 Young Children's Well-being: Social Isolation During The COVID-19 Lockdown and Effective Strategies. *Diálogos sobre Educación*, 0(22). <https://doi.org/10.32870/dse.v0i22.781>
- Villén-Contreras, R., Agreda-Montoro, M., & Rodríguez-Moreno, J. (2024). Perfil Competencial del Profesorado Andaluz en Seguridad Digital: Evaluación de la Protección de Datos y Privacidad de acuerdo con el Marco de Competencias Digitales para la Ciudadanía (DigComp 2.2). *Pixel-Bit, Revista de Medios y Educación*, 70, 123-142. <https://doi.org/10.12795/pixelbit.104153>

■

IMPACTO DE LA TECNOLOGÍA EN LA ADMINISTRACIÓN DE JUSTICIA

Sofía L. Dionicio-Moreno¹, Brisa P. Montoya-Ramos²,
Yanella L. Navarro-Chira³, Kiara M. Rivera-Vasquez⁴,
Aileen C. Saldaña-Ramírez⁵, Y Kiara C. Tapia-Alzamora⁶.

INTRODUCCIÓN

La adecuada gestión de la justicia es una de las responsabilidades más complejas e indispensables que tiene el Estado, en su papel de poder público, además de ser un componente clave del sistema legal, la obligación de proteger los derechos de los ciudadanos, asegurando que las leyes se implementen de manera equitativa y eficiente. No obstante, su sistema de justicia convencional muestra fallos debido a su operación, manifestándose en la gestión física de documentos jurídicos y la ejecución única de audiencias, lo que provoca procedimientos lentos, costosos e ineficientes.

Con un sistema judicial insuficiente se deriva un sinnúmero de dificultades operativas; por ello, han surgido cambios modernos mediante soluciones tecnológicas que impulsan una transición hacia la conocida e-justicia. Respecto a ello, Fabri (2024) señaló que numerosos tribunales se encuentran con obstáculos debido a las deficiencias en los sistemas de administración

1 sdioniciom1@upao.edu.pe

2 bmontoyar2@upao.edu.pe

3 ynavarroc2@upao.edu.pe

4 kriverv1@upao.edu.pe

5 asaldanar6@upao.edu.pe

6 ktapiaa2@upao.edu.pe

Programa de Estudio de Derecho, Universidad Privada Antenor Orrego

legal, dificultando tanto el acceso a la justicia como afectando a litigantes que se defienden a sí mismos y a las personas vulnerables.

Frente a estos obstáculos, se sugiere emplear varias herramientas tecnológicas en tareas básicas y actividades relacionadas con la justicia, reconociendo el cambio significativo en el manejo de datos y documentos legales, así como en métodos de comunicación vinculados al proceso y la evidencia; es así que, el término justicia digital busca utilizar la tecnología para ayudar a mejorar el sistema legal y alcanzar resultados que, de otro modo, serían difíciles de lograr (Sacoto & Cordero, 2021).

La justicia digital se caracteriza por el uso de plataformas tecnológicas que permiten optimizar la tramitación de procesos y mejorar la eficacia al momento de impartir justicia. Sacoto & Cordero (2021) sostuvieron que las Tecnologías de la Información y Comunicación (TIC) han redefinido los procesos judiciales, abriendo nuevas oportunidades para que se cumplan y respeten las garantías, derechos fundamentales y principios procesales que protegen a las personas en dichos procesos.

Estas transformaciones tecnológicas son diversas y colaboran entre sí para generar mayores beneficios facilidades a los operadores del derecho y a la ciudadanía cuando se encuentren en un conflicto jurídico, dentro de estas innovaciones está la Inteligencia Artificial (IA), como indicó Reiling (2020) juega un papel muy importante porque se adapta a diferentes necesidades y ayuda a que el derecho sea más eficiente y accesible para todos, en este sentido, la tecnología permite desarrollar sistemas que faciliten la resolución de casos de manera más clara y efectiva.

Gracias a la modernización, el sistema automatizado ha logrado adentrarse en el derecho, generando que los procesos sean mucho más eficientes. Según Cárdenas (2021), manifestó que aparte de ofrecer mayor celeridad, manejo más completo de la jurisprudencia y acceso a normas legales, el uso de robots como jueces; también ofrece un mayor apoyo para erradicar la corrupción, así como evitar influencias sospechosas, ya sean políticas, económicas o sociales.

Esto abre la puerta a un sistema de justicia eficaz y confiable para todos, sin embargo, tal evolución debe ser tratada con responsabilidad y atendiendo siempre la finalidad del sistema judicial sin quebrantar los derechos fundamentales. Como bien señaló Fabri (2024), una estrategia más efectiva sería considerar la implementación de un proceso de revisión rápida que se

habilite cuando la tecnología esté a punto de introducirse para constatar un entorno probatorio que no vulnere los derechos y valores fundamentales.

Botero et al. (2024) expresaron que es fundamental el reconocimiento de la era digital en todo el ordenamiento jurídico, incorporando un marco legal que integre y regule de manera adecuada las tecnologías como la IA en los procesos judiciales, para brindar al sistema judicial mayor celeridad y optimización en las funciones diarias indispensables en la administración de justicia. Este tratamiento hacia una justicia digital, debe tener un enfoque íntegro que regule el uso de la IA en la justicia asegurando la protección de derechos fundamentales.

Sin embargo, en la práctica, existe un gran debate sobre el cumplimiento de este tratamiento acorde al derecho, pues persisten desventajas y riesgos que no han sido tratados correctamente y que deberían ser prioridad en su desarrollo. Uno de ellos es que, el uso de la Inteligencia Artificial en el sistema judicial presenta retos éticos, que como consecuencia genera perjuicios sociales y decisiones injustas si no se corrigen tales sesgos, por ello es fundamental moderar los algoritmos para asegurar decisiones que no sean discriminatorias (Demertzis et al., 2023).

Este uso indebido que compromete la ética debería erradicarse, pues la IA debe ser considerada como una herramienta o complemento para conocer y comprender diversas cuestiones, no para dejar de lado los principios fundamentales o reemplazar el propio criterio del abogado o de un juez en la toma de decisiones. Un caso canadiense reveló que un abogado presentó citas jurisprudenciales falsas generadas por ChatGPT, pero las retiró al enterarse (Tamošiūnienė et al., 2024).

En consecuencia, se requiere un refuerzo institucional que pueda garantizar la seguridad y la fiabilidad profesional cuando se desarrolle este tipo de riesgos. Los Estados tienen que implementar sistemas altamente seguros que disipen la desconfianza de los operadores jurídicos, especialmente de los abogados, frente al uso de la vía digital para este tipo de juicios, aunque esto no asegure una tasa de cero incidencias (Medina, 2022).

Otra desventaja que acarrea el uso de la tecnología digital en la resolución de conflictos legales, es que, aunque su finalidad principal es el acceso a la justicia, aún se mantienen grupos sociales y profesionales de derecho que no comprenden su proceso, generando que haya desconfianza hacia estas herramientas lo que dificultará su implementación. Además, Botero

et al. (2024) manifestó que el juez digital, entendido como un sistema tecnológico que analiza casos legales, valora pruebas y toma decisiones, genera cuestionamientos sobre cómo garantizar que la interpretación y la argumentación jurídica de la ley sean justas y transparentes, especialmente en un contexto donde no todos los ciudadanos tienen el mismo acceso a la tecnología.

Por ello, para garantizar la equidad jurídica, es fundamental que la incorporación de tecnologías en la justicia se realice bajo una normativa clara, con una perspectiva inclusiva y criterios éticos, asegurando que sus beneficios no generen nuevas formas de discriminación ni vulneren derechos fundamentales. Los sistemas de inteligencia artificial tienen que diseñarse y utilizarse respetando principios básicos como los derechos humanos, la igualdad, la tolerancia y el humanismo, asimismo es importante que las personas tengan control sobre la aplicación, supervisión y decisión respecto al uso de estas tecnologías para evitar posibles abusos (Rustamzade et al., 2024).

Para finalizar, hay cinco objetivos propuestos para la investigación, el primero consiste en analizar cómo la implementación de la tecnología en los sistemas transforma el acceso a la justicia, el segundo busca establecer los elementos esenciales para la implementación efectiva de tecnologías judiciales en países subdesarrollados, el tercero se centra en investigar el cambio resultante en la participación de los ciudadanos implementando tribunales digitales, el cuarto se dedica a identificar los riesgos ético-legales que vienen con la digitalización tecnológica y como último objetivo, determinar el impacto de la automatización de los procedimientos legales en la eficacia del sistema judicial. Para lograr estos propósitos, el estudio aplica un análisis de casos con el fin de garantizar una mayor comprensión de la justicia digital.

METODOLOGÍA

La administración de justicia se ha visto profundamente transformada por la incorporación de tecnologías digitales generando un nuevo enfoque tanto en la gestión como en el acceso a la justicia, puesto que la llegada de estas herramientas ha abierto nuevas posibilidades para que las personas en general puedan acceder a los procesos judiciales de una manera más sencilla, eficaz y transparente. Sin embargo, no todo es positivo, debido a que también trae consigo riesgos importantes para los operadores jurídicos,

así como para el entorno social; es por ello que se tiene el propósito de evaluar si esta nueva era digital cumple con los estándares de justicia que se necesita.

Esta investigación se llevó a cabo con un enfoque cualitativo, con el propósito de profundizar el tema denominado el impacto de la tecnología en la administración de justicia, comprendiendo a fondo no sólo los aspectos positivos, sino también los diversos desafíos que se vienen desarrollando y comparar el uso de estos instrumentos tecnológicos en países desarrollados. Este enfoque se centra en la “dispersión o expansión” de datos e información, lo que nos permitió explorar diversas perspectivas y matices sobre el mismo.

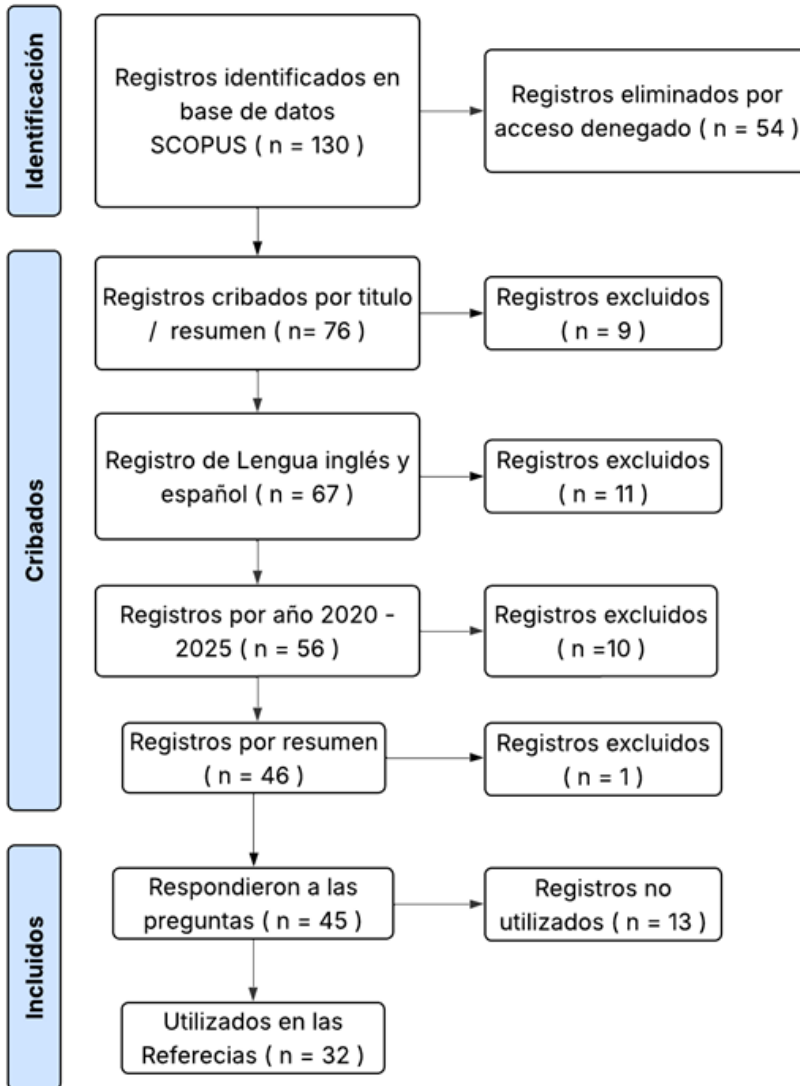
El tipo de investigación fue descriptiva y el diseño de investigación fue no experimental, la técnica empleada se limitó a una revisión bibliográfica de 32 artículos científicos y jurídicos seleccionados de las bases de datos reconocidas como Scopus y para la recolección de información se utilizaron fichas bibliográficas organizadas en una hoja de cálculo de Excel que contenía datos clave como el año de publicación, la revista, los autores, el país donde se realizó la investigación, así como los objetivos y las conclusiones de cada estudio; el análisis necesito de un enfoque deductivo con un tipo de argumentación orientado al orden de ideas de forma prevalente.

Por consiguiente, se estableció un esquema temático para guiar el análisis; en primer lugar, fue necesario analizar la transformación del acceso de justicia través la tecnología; en segundo lugar, establecer la tecnología en la modernización de los sistemas judiciales en países subdesarrollados; en tercer lugar, investigar los cambios que ha traído la implementación de la tecnología en la participación ciudadana; en cuarto lugar, identificar los riesgos éticos y legales de la tecnología digital en la administración de justicia, y finalmente, determinar el impacto de la automatización de los procesos judiciales en el sistema de justicia.

Pº	Pregunta de investigación	Referencias	#
1	¿De qué manera la digitalización de procesos judiciales transformó el acceso a la justicia?	(Bhatt et al., 2022), (Cerdá, 2020), (Castro et al., 2024), (Ferreira & Aquino, 2024), (Sacoto & Cordero, 2021), (Rustamzade et al., 2024), (Reiling, 2020), (Mohamad et al., 2020), (Medina, 2022), (Lillo, 2024), (Fabri, 2024), (Pérez, 2023), (Demertzis et al., 2023), (Terzidou, 2023), (Silva et al., 2023), (Kuhimbisa, 2024), (Naizir, 2023), (Botero et al., 2024), (Contini, 2020a), (Tamošiūnienė et al., 2024), (Cerdá, 2022), (Olugasa, 2020), (Fernández, 2024), (Lupo & Carnevali, 2022), (Sánchez, 2022), (Ajah et al., s. f.), (Fernández, 2025), (Villa, 2023), (Papagianneas & Junius, 2023), (Djamaludin et al., 2023), (Razmetaeva et al., 2022), (Chen et al., 2024), (Duong, 2024), (Chaves & Pires, 2024), (Fruet et al., 2024), (Borges, 2020), (Shabalin et al., 2024), (Lírio do Valle, 2023).	38
2	¿Cuál es el papel que juega la tecnología en la modernización de los sistemas judiciales de países en vías de desarrollo?	(Cárdenas, 2021), (Bhatt et al., 2022), (Ferreira & Aquino, 2024), (Sacoto & Cordero, 2021), (Pérez, 2023), (Terzidou, 2023), (Kuhimbisa, 2024), (Silva et al., 2023), (Contini, 2024), (Botero et al., 2024), (Olugasa, 2020), (Fernández, 2024), (Reiling, 2020), (Mohamad et al., 2020), (Medina, 2022), (Lillo, 2024), (Fabri, 2024), (Castellano, 2021), (Demertzis et al., 2023), (Vanderveen, 2023), (Naizir, 2023), (Díaz & Astudillo, 2021), (Méndez, 2024), (Contini, 2020a), (Tamošiūnienė et al., 2024), (Cerdá, 2022), (Papagianneas & Junius, 2023), (Lupo & Carnevali, 2022), (Sánchez, 2022), (Ajah et al., s. f.), (Fernández, 2025).	32
3	¿Qué cambios ha traído la implementación de tribunales digitales en la participación ciudadana y el acceso al proceso judicial?	(Cárdenas, 2021), (Sacoto & Cordero, 2021), (Reiling, 2020), (Mohamad et al., 2020), (Medina, 2022), (Lillo, 2024), (Fabri, 2024), (Castellano, 2021), (Pérez, 2023), (Demertzis et al., 2023), (Vanderveen, 2023), (Kuhimbisa, 2024), (Botero et al., 2024), (Contini, 2024), (Díaz & Astudillo, 2021), (Méndez, 2024), (Contini, 2020a), (Tamošiūnienė et al., 2024), (Cerdá, 2022), (Olugasa, 2020), (Papagianneas & Junius, 2023), (Fernández, 2024), (Lupo & Carnevali, 2022), (Sánchez, 2022), (Ajah et al., s. f.), (Fernández, 2025), (Fabri, 2024), (Villa, 2023), (Djamaludin et al., 2023), (Razmetaeva et al., 2022), (Chen et al., 2024), (Duong, 2024), (Chaves & Pires, 2024), (Fruet et al., 2024), (Borges, 2020), (Shabalin et al., 2024), (Lírio do Valle, 2023).	37

4	¿Cuáles son los riesgos éticos y legales del uso de tecnologías digitales en la administración de justicia?	(Bhatt et al., 2022), (Sacoto & Cordero, 2021), (Rustamzade et al., 2024), (Reiling, 2020), (Mohamad et al., 2020), (Lillo, 2024), (Fabri, 2024), (Castellano, 2021), (Pérez, 2023), (Demertzis et al., 2023), (Vanderveen, 2023), (Terzidou, 2023), (Naizir, 2023), (Silva et al., 2023), (Botero et al., 2024), (Contini, 2024), (Díaz & Astudillo, 2021), (Méndez, 2024), (Contini, 2020), (Tamošiūnienė et al., 2024), (Cerdá, 2022), (Olugasa, 2020), (Papagianneas & Junius, 2023), (Fernández, 2024), (Lupo & Carnevali, 2022), (Sánchez, 2022), (Ajah et al., s. f.), (Fernández, 2025), (Fabri, 2024), (Villa, 2023), (Razmetaeva et al., 2022), (Chen et al., 2024), (Duong, 2024), (Chaves & Pires, 2024), (Fruet et al., 2024), (Borges, 2020), (Shabalin et al., 2024), (Lírio do Valle, 2023).	39
5	¿Qué impacto tiene la automatización de procesos judiciales en la eficiencia del sistema de justicia?	(Bhatt et al., 2022), (Cerdá, 2020), (Castro et al., 2024), (Ferreira & Aquino, 2024), (Sacoto & Cordero, 2021), (Rustamzade et al., 2024), (Reiling, 2020), (Mohamad et al., 2020), (Medina, 2022), (Lillo, 2024), (Fabri, 2024), (Pérez, 2023), (Demertzis et al., 2023), (Vanderveen, 2023), (Terzidou, 2023), (Silva et al., 2023), (Kuhimbisa, 2024), (Naizir, 2023), (Botero et al., 2024), (Contini, 2024), (Díaz & Astudillo, 2021), (Méndez, 2024), (Contini, 2020), (Tamošiūnienė et al., 2024), (Cerdá, 2022), (Olugasa, 2020), (Papagianneas & Junius, 2023), (Lupo & Carnevali, 2022), (Sánchez, 2022), (Villa, 2023), (Djamaludin et al., 2023), (Razmetaeva et al., 2022), (Duong, 2024), (Chaves & Pires, 2024), (Fruet et al., 2024), (Borges, 2020), (Shabalin et al., 2024), (Lírio do Valle, 2023).	42

RESULTADOS Y DISCUSIÓN



1. La transformación del acceso a la justicia a través de la implementación de la tecnología en los procesos judiciales

Las tecnologías digitales han causado una transformación profunda en los procesos judiciales, fortaleciendo significativamente el acceso a la justicia, de modo que, permite que se convierta en un sistema más eficaz, ágil, transparente, así como accesible a los operadores jurídicos y a la población; reduciendo las barreras tradicionales, como la distancia geográfica, los costos y los retrasos en la tramitación de casos que limitaban la participación de la ciudadanía (Bhatt et al., 2022; Rustamzade et al., 2024). Esta transformación demuestra un progreso indispensable e inevitable, sobre todo cuando existe una ascendente necesidad de modernización, por lo que estas herramientas tecnológicas denotan una oportunidad provechosa para alcanzar una excelente eficiencia en el manejo del sistema judicial.

Asimismo, para que se haya logrado esta transformación se ha invertido un tiempo prudente en la detección de cuáles son esas verdaderas necesidades para alcanzar la optimización de los servicios judiciales, además se ha evaluado la contribución que tienen las TIC en el proceso de modernización, evidenciando que el terreno propicio de la tecnología es en los procedimientos repetitivos y de alto volumen, como las órdenes de pago, las demandas de menor cuantía y los requerimientos judiciales, demostrando mejores resultados cuando aplica a ellos (Fabri, 2024).

La idea que transmite el autor, es que la tecnología se ha aplicado en donde existe un fuerte impacto en el sistema judicial, por lo que por justa razón requieren mejoras como es el caso de la tramitología, debido a que la diversidad de carga hace que el proceso se vuelva lento e ineficiente, por ello es correcto que se haya planificado la incorporación de la modernización teniendo como base el análisis real de al menos algunas de estas necesidades, evitando utilizar la misma como una tendencia o moda, sino porque realmente así se requiere.

Por otro lado, las TIC han contribuido a una mejor comunicación con los órganos judiciales habilitando diversos canales o medios para el ofrecimiento de servicios electrónicos, lo que implica un avance más en el acceso a la justicia, reduciendo lo ya antes mencionado como son esas limitaciones o barreras físicas, facilitando la interacción más directa, rápida y accesible con el sistema judicial (Naizir, 2023).

La escasa comunicación entre los órganos de justicia, es otra necesidad que ha estado activa por mucho tiempo, por lo que como consecuencia ha

generado mayor desconfianza, así como la falta de transparencia, pues la rigidez de los canales tradicionales, la presentación física de los escritos, la poca atención presencial también ha dado como resultado desinformación, retrasos, violación de derechos, entre otros. Provocando una lejanía entre la población y la justicia, es por eso que el autor menciona que frente a la realidad presentada la incorporación de las TIC son un medio ideal para superar toda limitación comunicativa, obteniendo una comunicación oportuna y clara con las personas del sistema.

Ahora bien, en relación a lo expuesto al inicio, esta transformación tecnológica en el sistema judicial reforzará y promoverá aún más los principios básicos como son de igualdad y de oportunidad, contribuyendo justamente en la eliminación de cualquier tipo de barrera ya mencionadas, que anteriormente restringían el pleno ejercicio de los derechos (Botero et al., 2024). Es factible señalar que la participación de las personas es indispensable en un proceso, sin embargo, no todos poseen los recursos suficientes, pues algunos de ellos pueden encontrarse a distancia de los órganos jurisdiccionales como son las zonas rurales, no contar con el sustento económico para tramitar un proceso, falta de información sobre el proceso, entre otros, por lo que, con esto se garantizan dos derechos fundamentales.

De igual forma, sobre las demás figuras del sistema judicial, la tecnología permite que los jueces, magistrados y abogados cuenten con una adecuada formación para el uso de medios técnicos disponibles, trasladando un proceso convencional a uno electrónico, en el que tengan facilidad de información y comunicación de los casos pendientes, número de audiencias, análisis de datos, realizar audiencias virtuales, registrar decisiones electrónicamente, entre otros (Cerdá, 2020; Ferreira & Aquino, 2024).

Un claro ejemplo de esta transformación se materializa en el uso del Sistema de Audiencias Avanzadas (SAV), que permite que tanto las partes litigantes, así como el juez, aunque se encuentren en diferentes lugares, puedan reunirse simultáneamente en una sala virtual para llevar a cabo el proceso (Mohamad et al., 2020). De esta manera, las partes del proceso se ven beneficiadas por instrumentos que no solo ahorran tiempo, sino que eliminan las barreras que se originan en un proceso convencional.

Bajo esta perspectiva, gracias a la digitalización acompañada de la automatización visibles en lo que ahora se conoce como la inteligencia

artificial, expedientes electrónicos, asistentes virtuales como (Chatbots) que realizan consultas en línea o audiencias por videoconferencia resultan ser beneficiosas, pues superan las deficiencias problemáticas del sistema judicial, logrando sobre este un mayor control, transparencia, confianza y accesibilidad para todas las personas que atraviesan por un conflicto jurídico (Contini, 2020; Fernández, 2025). Este planteamiento muestra con acierto que la tecnología puede ser una aliada, pues deja de lado tanto un sistema obsoleto como limitado, permitiendo un mayor dinamismo, optimización del tiempo y los recursos de los procesos judiciales.

Finalmente, teniendo en cuenta todo lo mencionado, la transformación tecnológica fortalece la justicia con la finalidad de convertirla en inclusiva, funcional e innovadora, logrando que el servicio que se brinda se adapte a la realidad social y el acceso a sus mecanismos no sea visto como un privilegio, sino un derecho efectivo, además de eliminar la carga procesal, también elimina los errores administrativos como las decisiones mal ejecutadas e injustas que conlleven la violación de los derechos humanos. Igualmente, es importante mencionar, que la tecnología no debe reemplazar la labor de los operadores jurídicos, sino que debe servir como complemento, potenciando la capacidad que tienen para mejorar las funciones que les son atribuidas al sistema legal de manera oportuna y justa.

2. La tecnología en la modernización de los sistemas judiciales de países en desarrollo

El uso de la tecnología está impulsando una renovación profunda en el sistema jurídico, lo que resulta beneficioso, dado que disminuye la carga judicial y brinda optimización en la repartición de casos, incluso sobrepasando las restricciones de competencia territorial, facilitando la orientación de la gestión de casos entre distintos tribunales. Cárdenas (2021) expresó que cuando otros países utilizan la tecnología en su sistema judicial, ofrecen la idea de ir más allá de las limitaciones, traspasar el ámbito de las competencias territoriales, así como reducir la carga judicial y fomentar que los casos sean atendidos con una mayor especialización.

En este contexto, la tecnología se convierte en una herramienta vital en zonas con barreras geográficas, como zonas rurales, selváticas o insulares, donde la accesibilidad física a los tribunales es limitada. Este avance tecnológico presenta una creciente importancia, gracias a iniciativas como las del Poder Judicial de Brasil, que emplean plataformas como Codex (que

convierte documentos judiciales en datos) y Sinapses (infraestructura para alojar modelos compartidos de Inteligencia Artificial), que evidencian la capacidad de implementar algoritmos para respaldar a los jueces en la clasificación (Ferreira & Aquino, 2024).

Sin embargo, para que estos avances tengan un impacto real y positivo en los países en vías de desarrollo, es fundamental enfrentar una serie de limitaciones estructurales que requieren ser atendidas para eliminar la brecha digital. Terzidou (2023) señaló como algunas limitaciones a la carencia de infraestructura tecnológica apropiada, el analfabetismo digital en usuarios, la falta de marcos regulatorios claros, la ausencia de marcos normativos definidos para regular el uso de IA, la protección de datos y la interoperabilidad entre sistemas.

Atender estas limitaciones es un paso imprescindible para que la tecnología cumpla con su papel de transformación de los sistemas judiciales en países subdesarrollados, siendo así no sólo un conjunto de herramientas nuevas, sino un motor de transformación, haciendo que su uso sea posible para todos (Pérez, 2023). Esto permitirá aprovechar plenamente los beneficios que trae consigo la digitalización, además de que contribuirá en el fortalecimiento institucional y en el desarrollo de la población.

En este sentido, la incorporación de la tecnología en el sistema judicial se ha vuelto esencial en años recientes, tomando como experiencia el Poder Judicial de Europa donde se ha evidenciado que la inversión tecnológica no sólo es legítima, sino también imprescindible, permitiendo sistemas de justicia más ágiles, eficientes y cercanos a los ciudadanos, asimismo se debe comprender a la tecnología como un socio estratégico que facilita la transformación en los procesos judiciales haciendo la justicia más accesible y transparente (Kuhimbisa, 2024).

La implementación de instrumentos tecnológicos como plataformas digitales, expedientes electrónicos e inteligencia artificial ha reducido considerablemente los tiempos de tramitación, mejorado la rastreabilidad de los procesos y facilitado la asignación de recursos (Silva et al., 2023). Esto no solo potencia la habilidad institucional del Poder Judicial, sino que produce un efecto directo y beneficioso en la experiencia del ciudadano, quien percibe un servicio más factible.

La tecnología también empodera a los usuarios del sistema judicial, mediante plataformas digitales e información disponible en línea, así los ciudadanos tienen la posibilidad de conocer sus derechos, mantener un

seguimiento de sus procesos, así como efectuar gestiones sin la necesidad de desplazarse físicamente, lo que es particularmente ventajoso en situaciones geográficas difíciles o con escasez de servicios públicos; de esta manera, la tecnología no sólo acelera los procesos, sino que también robustece el principio de transparencia y el derecho a la información (Contini, 2024).

La digitalización en el sistema de justicia constituye una oportunidad crucial para modernizar y potenciar la justicia en países en vías de desarrollo, particularmente en áreas rurales o de difícil acceso, donde haya restricciones territoriales, carga procesal y ausencia de acceso a la justicia, asimismo, facilita la mejora de la distribución de los casos, disminuyendo considerablemente los períodos de gestión y potenciando la eficacia del servicio (Botero et al., 2024).

Además, la aplicación de expedientes electrónicos, plataformas virtuales y sistemas de IA contribuye a una organización, categorización y ordenación más eficiente de los casos, creando un sistema más optimizado y especializado que mejora la administración de justicia. En este contexto resulta imprescindible que los Estados promuevan políticas holísticas que aseguren la accesibilidad, interoperabilidad y seguridad de las herramientas tecnológicas, además de programas de formación constante que faciliten el uso correcto y responsable de estas innovaciones (Olugasa, 2020).

Solo de esta manera, la tecnología se podrá convertir en un auténtico aliado de la justicia, fomentando la transparencia, robusteciendo la institucionalidad y asegurando que todos los ciudadanos, sin excepción, sean capaces de ejercer sus derechos de manera completa y a tiempo (Fernández, 2024). De esta manera se construye un sistema judicial justo, así como accesible, donde todos se sientan protegidos.

No obstante, para que todas estas ventajas se hagan realidad plenamente, es esencial tener una normativa apropiada que defina marcos de ley claros, particularmente en lo que respecta al manejo de datos personales, la utilización de inteligencia artificial en resoluciones judiciales y la interoperabilidad de sistemas entre instituciones. Igualmente, es vital la formación continua de los operadores judiciales, igual que de los usuarios para asegurar un uso efectivo de las herramientas digitales, de lo contrario la brecha tecnológica y la ausencia de preparación podrían convertirse en nuevos obstáculos para un acceso justo a la justicia.

3. Cambios que ha traído la implementación de tribunales digitales en la participación ciudadana y el acceso al proceso judicial

El uso de los tribunales digitales ha cambiado de manera significativa como interactúa la sociedad y el sistema judicial, este cambio valioso como lo es la digitalización amplía el acceso para aquellos sectores que a lo largo de la historia fueron marginados, vulnerables, simplemente por las barreras físicas o territoriales, por lo que estas herramientas digitales fomentan una participación ciudadana más activa al eliminar obstáculos tanto geográficos como económicos, permitiendo realizar consultas, presentar recursos y dar seguimiento a los casos en tiempo real (Rustamzade et al., 2024).

Como se señaló, la implementación de tribunales digitales ha democratizado el acceso a la justicia, especialmente para grupos históricamente excluidos como personas en zonas rurales o con discapacidades, siendo estas herramientas como las audiencias virtuales y expedientes electrónicos fundamentales para una interacción remota sin necesidad de desplazamientos costosos (Duong, 2024). Además, Contini (2024) mencionó que plataformas como chatbots y notificaciones automatizadas reducen la realización de trámites para usuarios con limitaciones tecnológicas básicas.

La digitalización ha optimizado la gestión judicial al reducir tiempos de resolución y descongestionar la carga procesal. Sistemas como el E-court en Indonesia permiten presentar demandas y participar en juicios virtuales, agilizando procedimientos que antes requerían meses (Djamaludin et al., 2023). Este camino fue incorporado también en los países a raíz de la pandemia del COVID-19 haciendo que las audiencias se realicen de manera virtual o de manera remota, liberando de cierta manera la carga procesal que existía hasta ese momento.

Desde su uso en el ámbito jurídico, la tecnología ha brindado mayor eficiencia, Lillo (2024) indicó que la digitalización ha hecho más ágiles los procedimientos, ha reducido los plazos y ha incrementado la transparencia, por su parte, Chen et al. (2024) destacó que estos avances han contribuido a disminuir costos y a democratizar el acceso a la justicia. En esta misma línea, Lupo & Carnevali (2022) manifestaron que, para lograr el éxito en la justicia electrónica, se requiere de un enfoque incremental en el desarrollo de sistemas para ir mejorando poco a poco hasta consolidar un proyecto exitoso.

La aceptación de los tribunales digitales varía según el contexto cultural y jurídico de cada país, por ejemplo, mientras países como Uganda han

adoptado con éxito las videoconferencias para reducir retrasos (Kuhimbisa, 2024). Otros enfrentan resistencia de operadores judiciales acostumbrados a métodos presenciales (Fruet et al., 2024). La clave, según Demertzis et al. (2023) está en combinar innovación con diálogo social tales como consultas públicas así también capacitaciones que pueden mitigar resistencias y asegurar que las herramientas sean percibidas como legítimas.

Sin embargo, Razmetaeva et al. (2022) advirtió que la dependencia tecnológica también expone vulnerabilidades, como fallos en plataformas o ciberataques, que pueden paralizar procesos, asimismo, Fernández (2025) hizo mención que la automatización de tareas administrativas ha generado preocupaciones sobre la deshumanización del servicio y el impacto en empleos judiciales tradicionales. Ambos autores aportan dos puntos sumamente importantes y muy reales, por un lado, está la dependencia que genera el uso de la IA, el uso de estas también conlleva que la ciberdelincuencia incremente al intentar acceder a la información de estas plataformas, por otro lado, la IA puede generar desempleo o el reemplazo de alguno de ellos, llegando en algún momento al punto de que existan máquinas en vez de personas.

No cabe duda que los tribunales digitales tienen grandes ventajas, puesto que agilizan los procesos reduciendo la carga procesal, permitiendo una mayor celeridad en los procesos para impartir justicia, pero no solo es eso, con estas nuevas implementaciones se permite que se puedan evitar costos o la reducción de alguno de ellos, beneficiando así a las personas con menos recursos que acuden a la justicia. Sin embargo, aunque la mayor parte de estas nuevas implementaciones son buenas, también pueden generar dificultades, con respecto a que, puede afectar de manera negativa a aquellas personas que no cuentan con conocimiento avanzado en las tecnologías o no tienen la misma facilidad y habilidad para realizarlas.

Un punto clave es la percepción de legitimidad, en relación a ello, Botero et al. (2024) advierte que, si bien los tribunales digitales agilizan los procesos, es fundamental garantizar la transparencia para que las resoluciones automatizadas sean comprensibles. Aquello tiene mucha razón, pues es fundamental que las resoluciones automatizadas sean comprensibles para todas las personas y exista la transparencia que no solo facilita el acceso a la información, sino que también fortalece la confianza y la legitimidad del sistema judicial.

En fin, es indiscutible que la digitalización ha traído cambios positivos a la participación ciudadana, haciendo que el acceso a la justicia sea más

accesible igual que eficiente, esta implementación de tribunales digitales facilita el que todos los ciudadanos puedan tener un proceso con celeridad y un debido proceso, sin embargo, su fortalecimiento requiere de que estos tribunales digitales tengan un uso controlado también responsable, pero no solo ello, también debe existir una capacitación adecuada y marcos regulatorios bien sólidos para asegurar la confianza en el sistema.

4. Riesgos éticos y legales de la tecnología digital en la administración de justicia

La implementación de tecnologías digitales en la administración de justicia, presenta tanto riesgos éticos como legales, que deben ser cuidadosamente considerados con la finalidad de asegurar la equidad, transparencia y protección de los derechos fundamentales, en el desarrollo de un proceso judicial. El manejo de información sensible mediante sistemas digitales aumenta el riesgo de violaciones de datos personales, en particular, la utilización de IA implica, por consecuencia, el tratamiento de datos, lo que puede acarrear en accesos no autorizados o filtraciones en la base de datos judicial (Rustamzade et al., 2024).

En este contexto, el uso de algoritmos en la inteligencia artificial pueden producir sesgos históricos, perjudicando la imparcialidad de las decisiones judiciales originando injusticias sistemáticas, especialmente cuando los datos de entrenamiento contienen prejuicios (Rustamzade et al., 2024; Reiling, 2020). La opacidad de estos algoritmos, denominada “caja negra”, dificulta la identificación y corrección de dichos sesgos (Terzidou, 2023).

Estos sesgos informativos connotados en la toma de decisiones judiciales son un grave perjuicio a los principios inherentes a una persona en un proceso judicial, enajenando la función principal de una decisión judicial, la búsqueda de la verdad materializada en la justicia. La introducción de mecanismos artificiales para la resolución de conflictos, al valorar minuciosamente la sociología-jurídica e individualizar sus criterios al momento de emitir un fallo, carece de información sesgada, dificultando y entorpeciendo un sistema judicial garantista.

Además, los fallos automatizados carecen de transparencia, transgrediendo el derecho a una justicia comprensible y motivada. Los sujetos sobre los que recaen las decisiones judiciales, fundamentadas en IA, usualmente, no pueden conocer los criterios y fundamentos de estas, lo que compromete el debido proceso (Fabri, 2024). Por ello, la Unión Europea ha señalado la

indispensabilidad de instrucciones éticas para garantizar la compresibilidad de los sistemas inteligentes (Demertzis et al., 2023).

La justicia no puede sentirse como una respuesta automática, sin rostro, sin explicación. Si una persona no puede saber qué datos se usaron, cómo se interpretaron o por qué se eligió una opción y no otra, entonces no se habla de justicia, sino de incertidumbre de sistemas de inteligencia artificial pueden ayudar, claro, pero no deben decidir por sí solos. Se requiere que todo lo que se haga en nombre de la justicia pueda ser explicado con claridad, con razones que cualquier persona pueda comprender. Por qué, al final, lo justo no es solo lo correcto, sino también lo que se puede entender.

La digitalización de procesos judiciales, acarrea que, los sistemas a una posibilidad de riesgos de ciberataques, alteración de evidencias digitales y fallos técnicos, que pueden comprometer la seguridad de los procesos almacenados en una base de datos (Lillo, 2024). Estas posibilidades complican la fragilidad en la protección de datos y la evidencia digitalizada, un desafío que pone en una situación de riesgo tanto a las instituciones encargadas de custodiar la información como a los ciudadanos afectados (Chen et al., 2024).

Un factor preocupante, que se debe tener en cuenta, es el riesgo de digitalizar un proceso judicial, arriesgando a una vulneración del sistema y un manejo exterior de la información almacenada digitalmente, perjudicando la probidad de los procesos judiciales. La defensa de los datos registrados, al ser endeble, puede ser perjudicial tanto para la institución, así como para cualquier ciudadano, al sufrir algún tipo de violabilidad o fallos técnicos en el acopio digitalizado de información.

Frente a la creciente relación de dependencia con la tecnología, puede marginar a poblaciones que no tienen acceso o sin habilidades digitales, ocasionando una brecha social y nuevas formas de exclusión (Villa, 2023). Este escenario se agrava cuando la infraestructura tecnológica es insuficiente, limitando el acceso efectivo a la justicia para áreas vulnerables de la población (Olugasa, 2020).

De lo anterior, se entiende que, aunque la tecnología está cada vez más vigente, no todos tienen la oportunidad de hacer uso de ella, dado que, muchas personas no saben manejarla o no tienen acceso quedando, por lo tanto, excluidas, lo cual genera una brecha social. Este problema se vuelve más grave cuando en ciertas comunidades no hay la tecnología necesaria

haciendo difícil el acceso a la justicia digital, es por ello que se debe hacer de la tecnología una herramienta que sea de gran alcance para todos asegurando que nadie se quede atrás por falta de recursos o habilidades.

La ausencia de marcos normativos específicos para tecnologías emergentes, como IA o blockchain, genera incertidumbre jurídica (Razmetaeva et al., 2022). Por tal razón, es indispensable que las leyes se adapten rápido para que la integración de tecnologías en la justicia no acabe transformándose en una caja negra en cuanto a la forma en la que se toman las decisiones, es importante tener el control humano en todos los procesos para evitar errores y garantizar decisiones justas.

La incorporación de tecnologías ofrece grandes beneficios, pero también plantea riesgos éticos así también como legales que no pueden pasarse de largo, entre estos se encuentran los algoritmos que pueden evidenciar prejuicios históricos, de tal forma que llegue a haber decisiones injustas que afecten la imparcialidad que debe tener todo proceso judicial; asimismo, también están los sistemas que funcionan como “cajas negras”, lo cual encadena distintas complicaciones a la hora de entender cómo se toman las decisiones afectando negativamente la confianza en la justicia. En el plano legal, la protección de datos es vulnerable a ciberataques o filtraciones, la existente falta de normas para determinadas tecnologías emergentes genera incertidumbre y riesgos para el debido proceso, por ello, es necesario que la tecnología se use bajo la supervisión humana y con normas legales sólidas.

En conclusión, desde una mirada crítica y cercana, se percibe que llevar la justicia al mundo digital es un avance inevitable, pero no exento de sombras, si bien es cierto, la tecnología promete eficiencia, también puede acarrear desigualdad, así como opacidad, si no se maneja con cuidado. Que una máquina decida sobre la vida de alguien, sin que ni siquiera se entienda cómo llegó a esa conclusión, resulta preocupante, además, cuando se habla de datos personales, cualquier fallo técnico o acceso indebido no es solo un error, es una violación, por tanto, la justicia, no puede depender solo de códigos y algoritmos.

5. Impacto de la automatización de procesos judiciales en el sistema de justicia

El impacto en el sistema de justicia se ha modernizado y esto ha introducido nuevos modelos para practicar la actividad judicial, utilizando las tecnologías para avanzar con firmeza hacia la e-justicia. Este concepto moderno implica

el empleo de una amplia variedad de herramientas tecnológicas en todos los procedimientos fundamentales, así como conexos al impartir justicia (Sacoto & Cordero, 2021). Estas tecnologías no solo implican transformar la manera en que se imparten las actuaciones judiciales, sino que también permiten una gestión más dinámica, eficiente y acorde a las peticiones de una colectividad cada vez más moderna.

La automatización en el ámbito judicial ha permitido avanzar hacia un sistema más eficiente, logrando mayor reducción en los plazos procesales o una mejora en la organización interna, este cambio atiende a la necesidad de renovar instituciones públicas, logrando una ciudadanía cada vez más conectada igual que demandante de servicios ágiles y eficaces (Cerdá, 2020). Este avance tecnológico no es solo una mejoría técnica, sino que es, además, necesaria ante una ciudadanía con un futuro mecanizado y riguroso, donde exista un requerimiento de servicios públicos modernos operativos.

En este contexto, el tribunal deja de ser un lugar para convertirse en un servicio, llamado online court; es decir, ejecución de un método jurisdiccional específico seguido en todos sus períodos de forma digital, integrando el acceso a un expediente electrónico, interposición de primeros escritos, promociones, recursos, notificaciones, audiencias virtuales, entre otros (Medina, 2022). Se entiende que, los juzgados dejan de verse únicamente como un espacio físico, para verse como un servicio digitalizado de manera que los juicios y todas las etapas que se desarrollan se abordarán con esta nueva formalidad, lo que implica que el acceso a la justicia se está ejecutando con todas las facilidades que antes no existían, garantizando la eficacia e incluso la descentralización

Este avance fomentado por la creciente automatización permite un escenario de e-justicia más dinámico, reduciendo los plazos procesales, regenerando la organización interna, descongestionando la carga judicial, entre otros. Asimismo, se hace un llamado a la participación de las instituciones públicas y la ciudadanía para lograr de manera armoniosa cumplir con estos objetivos, pues en un sistema que es cada vez más digitalizado resulta necesario que todos colaboren.

Sin embargo, es fundamental que el uso de nuevas tecnologías no se vea como una barrera de entrada a los tribunales para quienes no cuentan con los recursos necesarios, es por eso que se ha llevado a cabo un intenso proceso de discusión y un cambio regulatorio para que los procesos de

implementación de estándares y los cambios culturales se unifiquen y creen estándares avanzados (Lillo, 2024).

Si bien es un avance necesario, es importante recordar que no debe ser desligada de las desigualdades sociales y económicas que aún persisten especialmente en lugares donde los ciudadanos carecen de conectividad regular, por lo mismo se debe tener en cuenta también los cambios culturales de igual forma que todas las personas tengan la posibilidad de poder utilizar este servicio.

El sistema judicial representado por un nuevo concepto de e-justicia le da un nuevo nacimiento al tribunal como un servicio de alto alcance y accesible de manera electrónica, donde se permite la agilización, eficacia y descentralización en los procesos judiciales tradicionales. Asimismo, esta realidad social no puede estar completamente alejada de las brechas económicas o sociales aún existentes, puesto que esto afectaría a grandes sectores donde el avance judicial no va a la par de los avances tecnológicos.

En definitiva, la justicia electrónica representa un nuevo modelo para el sistema judicial, concebido como un servicio de alto alcance así como accesible, que agiliza, descentraliza y hace más eficaz la administración de justicia, respondiendo a las necesidades legales de la población, asimismo creando un entorno para la prevención de problemas legales antes de que ocurran causas profundas de injusticia, siendo así de mucha ayuda para fortalecer la confianza en el sistema de justicia (Kuhimbisa, 2024).

Las ciencias aplicadas de la información han permitido la continuidad de la función jurisdiccional incluso en situaciones adversas como las limitaciones físicas. Gracias a las audiencias virtuales, corporaciones de Asistencia Judicial, clínicas jurídicas y abogados en general, se ha podido mantener una labor con la misma eficacia y seriedad que en las audiencias que se llevaban a cabo de manera presencial (Díaz & Astudillo, 2021). Esto demuestra que la tecnología puede asegurar un sistema judicial resiliente.

Por esta razón, la justicia modernizada garantiza un acceso más equitativo, eficaz al sistema judicial, colocando a las personas y comunidades como el centro de atención del proceso, asimismo este enfoque moderno no solo permite resolver conflictos, sino que también contribuye a prevenir la aparición de nuevas injusticias, por ello, la tecnología es clave para asegurar la efectividad de los procesos judiciales y que esta se dé sin interrupciones.

Respecto a lo mencionado anteriormente, se puede concluir que la

transformación del sistema judicial a través de la tecnología digital es una realidad que ha dado lugar al concepto de “e-justicia”, que abarca desde la digitalización de expedientes hasta la realización de audiencias virtuales, cambiando el modo de impartir justicia haciendo merecedor de procesos más ágiles, eficientes y accesibles. No obstante, esta transformación no puede desligarse de las desigualdades sociales, así como económicas, de modo que el impacto de la tecnología puede verse limitado por la brecha digital igual que la falta de recursos o habilidades de ciertos sectores. Sin embargo, lo más favorable de este gran cambio es que centra su atención en la población en general, permitiéndoles mayor acceso y previniendo nuevas injusticias.

CONCLUSIONES

- Se analizó que la transformación del acceso a la justicia a través de la implementación de la tecnología en los procesos judiciales ha favorecido enormemente al sistema judicial poniendo en evidencia la existencia de herramientas digitales como: Los sistemas de gestión electrónica de expedientes, audiencias virtuales, chatbots y la inteligencia artificial. Todas estas herramientas ayudan a que los procesos sean mucho más eficientes, ágiles, transparentes e incluso accesibles a la población en general, puesto que reducen las distancias geográficas, así como los costos elevados que requieren los procesos tradicionales.
- Se estableció que la tecnología en la modernización de los sistemas judiciales de países en desarrollo se ha convertido en una herramienta esencial, ayudando a superar obstáculos que durante mucho tiempo han dificultado que las personas accedan a la justicia, y entre sus beneficios destacan: La reducción de la carga judicial, el fácil acceso a la justicia en zonas alejadas, expedientes digitales, especialización de casos entre otros. Estos avances demuestran que la digitalización hace que los procesos sean más rápidos, organizados y que la justicia llegue a quienes más la necesitan sin importar la zona geográfica, para ello es fundamental el uso de normas claras que regulen el uso de la tecnología.
- Se investigó que los cambios que ha traído la implementación de tribunales digitales en la participación ciudadana y el acceso al proceso judicial han mejorado significativamente el acceso a la justicia, teniendo como cambios más notorios los siguientes: Eliminar las barreras de distancia y costos, acelerar los trámites judiciales, ofrecer herramientas como las audiencias virtuales, así como también los chatbots, reducir tiempos, por

último, capacitar tanto a los usuarios como a los operadores jurídicos. Estos cambios permiten que la justicia se siente más cerca, más ágil y, en muchos casos, más transparente, sin embargo, aún hay comunidades que se quedan atrás por falta de internet o desconocimiento tecnológico, por ello es necesario que esta transformación sea acompañada con educación.

- Se identificó ciertos riesgos éticos y legales de la tecnología digital en la administración de justicia, los cuales son: El blockchain, los algoritmos de análisis automatizado, los sesgos en los sistemas de inteligencia artificial, falta de transparencia en las decisiones, vulnerabilidades en la protección de datos personales, filtraciones de información y ausencia de marcos normativos. Esto demuestra que, aunque la tecnología ofrece grandes beneficios, no se puede dejar que todo dependa de máquinas, por eso es fundamental que haya un control humano constante con marcos normativos que supervisen el funcionamiento de este nuevo sistema digital.
- Se determinó que el impacto de la automatización de procesos judiciales en el sistema de justicia ha sido positivo para la eficiencia del sistema de justicia; entre los principales impactos están: La reducción de los tiempos de resolución, mejora en la gestión interna de los tribunales, posibilidad de hacer tanto audiencias como trámites en línea y ampliación del acceso a la justicia. Este avance responde a las exigencias de una sociedad cada vez más digitalizada posicionando a las personas en el centro del sistema judicial facilitando la solución de conflictos y garantizando la continuidad del servicio incluso frente a situaciones adversas, así se demuestra lo eficiente que es la justicia digital.

REFERENCIAS

- Bhatt, H., Bahuguna, R., Singh, R., Gehlot, A., Akram, S. V., Priyadarshi, N., & Twala, B. (2022). Artificial Intelligence and Robotics Led Technological Tremors: A Seismic Shift towards Digitizing the Legal Ecosystem. *Applied Sciences*, 12(22), Article 22. <https://doi.org/10.3390/app122211687>
- Botero, L. Al., Guevara, L. J., & Moreno, V. J. (2024). El impacto de las tecnologías en el proceso judicial: Una mirada a partir de los conceptos de juez digital y debido proceso. *Novum Jus*, 18(3), Article 3. <https://doi.org/10.14718/NovumJus.2024.18.3.7>

- Cárdenas, R. (2021). ¿Jueces robots? Inteligencia artificial y derecho. *Revista Justicia & Derecho*, 4(2), Article 2. <https://doi.org/10.32457/rjyd.v4i2.1345>
- Cerdá, J. I. (2020). La modernización y transformación digital de la Administración de Justicia: El papel del Consejo General del Poder Judicial. *IDP. Revista de Internet, Derecho y Política*, 31, Article 31. <https://doi.org/10.7238/idp.v0i31.3239>
- Chen, Z., Geng, R., Jia, Z., Wang, H., Hu, F., & Cai, Q. (2024). Securing privacy in the digital age: The quest for judicial protection of personal information. *Journal of Infrastructure, Policy and Development*, 8(12), Article 12. <https://doi.org/10.24294/jipd.v8i12.9253>
- Contini, F. (2020). Artificial Intelligence and the Transformation of Humans, Law and Technology Interactions in Judicial Proceedings. *Law, Technology and Humans*, 2(1), Article 1. <https://doi.org/10.5204/lthj.v2i1.1478>
- Contini, F. (2024). Unboxing Generative AI for the Legal Professions: Functions, Impacts and Governance. *International Journal for Court Administration*, 15(2). <https://doi.org/10.36745/ijca.604>
- Demertzis, K., Rantos, K., Magafas, L., Skianis, C., & Iliadis, L. (2023). A Secure and Privacy-Preserving Blockchain-Based XAI-Justice System. *Information*, 14(9), Article 9. <https://doi.org/10.3390/inf14090477>
- Díaz, E., & Astudillo, C. (2021). La enseñanza clínica del derecho y la telepresencialidad: Análisis de caso aplicado en la pandemia Covid-19. *Revista Pedagogía Universitaria y Didáctica del Derecho*, 8(1), Article 1. <https://doi.org/10.5354/0719-5885.2021.58358>
- Djamaludin, D., Muhammad, aziz, Ar-Rasyid, Y., & As-Sayyis, I. A. (2023). Assessing the Impact of Electronic Court Systems on the Efficiency of Judicial Processes in the Era of Digital Transformation. *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, 1-18. <https://doi.org/10.24090/volksgeist.v6i1.8082>
- Duong, Q. H. (2024). Digital transformation and building e-courts to meet the requirements of judicial reform in Vietnam. *Journal of Infrastructure, Policy and Development*, 8(11), Article 11. <https://doi.org/10.24294/jipd.v8i11.8225>

- Fabri, M. (2024). From Court Automation to e-Justice and Beyond in Europe. *International Journal for Court Administration*, 15(3). <https://doi.org/10.36745/ijca.640>
- Fernández, F. J. (2024). The future of court's procurators with the advent of artificial intelligence technologies. *Oñati Socio-Legal Series*, 14(6), Article 6. <https://doi.org/10.35295/osls.iisl.1907>
- Fernández, F. J. (2025). The Impact of Artificial Intelligence Technologies on the Justice Administration and on the Judicial Office Personnel. *Zeitschrift Für Rechtssoziologie*. <https://doi.org/10.1515/zfrs-2025-2008>
- Ferreira, L. F., & Aquino, T. (2024). Factors Associated with Innovation Capacity in Courts. *BAR - Brazilian Administration Review*, 21, e230061. <https://doi.org/10.1590/1807-7692bar2024230061>
- Fruet, B., Castagna, F., & Ribeiro, P. (2024). Digital Access to Judicial Services in the Brazilian Amazon: Barriers and Potential. *Social Sciences*, 13(2). Scopus. <https://doi.org/10.3390/socsci13020113>
- Kuhimbisa, E. (2024). Experience and Impact of Digital Transformation in the Administration of Justice in Uganda: A Critical Analysis. *International Journal for Court Administration*, 15(1). <https://doi.org/10.36745/ijca.580>
- Lillo, R. (2024). *ICT's in the Chilean and Latin-American civil justice. Analysis from the right of access to justice*. <https://doi.org/10.1556/2052.2023.00471>
- Lupo, G., & Carnevali, D. (2022). Smart Justice in Italy: Cases of Apps Created by Lawyers for Lawyers and Beyond. *Laws*, 11(3), Article 3. <https://doi.org/10.3390/laws11030051>
- Medina, E. (2022). Hacia una teoría sobre la e-justice o justicia digital: Instrucciones para armar. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, 177-212. <https://doi.org/10.22201/ijj.24484881e.2022.46.17052>
- Mohamad, A. M., Hamin, Z., Nor, M. Z. M., Kamaruddin, S., & Nizam, M. S. (2020). The Implications of Audio/Video Conference Systems on the Administration of Justice at the Malaysian Courts. *Webology*, 17(2), 904-921. <https://doi.org/10.14704/WEB/V17I2/WEB17076>

- Naizir, J. C. (2023). Impacto tecnológico en el derecho procesal: Subsanación de la demanda, prueba testimonial y sentencia C-134 de 2023. *Vniversitas*, 72. <https://doi.org/10.11144/Javeriana.vj72.itdp>
- Olugasa, O. (2020). Utilising Technology in Making the Nigerian Administration of Criminal Justice Act Effective for Criminal Trials. *International Journal for Court Administration*, 11(2). <https://doi.org/10.36745/ijca.332>
- Pérez, J. (2023). Soluciones digitales en el Poder Judicial de Uruguay: Retos, soluciones, avances y perspectivas. *Revista Oficial del Poder Judicial*, 15(20), Article 20. <https://doi.org/10.35292/ropj.v15i20.866>
- Razmetaeva, Y., Barabash, Y., & Lukianov, D. (2022). THE CONCEPT OF HUMAN RIGHTS IN THE DIGITAL ERA/ CHANGES AND CONSEQUENCES FOR JUDICIAL PRACTICE. *Access to Justice in Eastern Europe*, 5(3), 41-56. <https://doi.org/10.33327/AJEE-18-5.3-a000327>
- Reiling, A. D. (Dory). (2020). Courts and Artificial Intelligence. *International Journal for Court Administration*, 11(2), 8. <https://doi.org/10.36745/ijca.343>
- Rustamzade, A., Bagirov, A. R., & Huseynov, S. Z. (2024). Justice and Artificial Intelligence. *Revista Jurídica Portucalense*, 163-184. [https://doi.org/10.34625/issn.2183-2705\(36\)2024.ic-7](https://doi.org/10.34625/issn.2183-2705(36)2024.ic-7)
- Sacoto, M., & Cordero, J. (2021). E-justicia en Ecuador: Inclusión de las TIC en la administración de justicia. *Foro: Revista de Derecho*, 36, Article 36. <https://doi.org/10.32719/26312484.2021.36.5>
- Silva, G. J., Piray, P. O., Vicuña, V. E., & Silva, D. A. (2023). Vision of disruptive technologies and administration of justice: Their impact and future in contemporary law of Ecuador. *Salud, Ciencia y Tecnología - Serie de Conferencias*, 2, 1047-1047. <https://doi.org/10.56294/sctconf20231047>
- Tamošiūnienė, E., Terebeiza, Ž., & Doržinkevič, A. (2024). The Possibility of Applying Artificial Intelligence in the Delivery of Justice by Courts. *Baltic Journal of Law & Politics*, 17(1), 223-237. <https://doi.org/10.2478/bjlp-2024-0010>

- Terzidou, K. (2023). *The Evolution of the Perception of Artificial Intelligence in the EU: The Case of Judicial Administration* (SSRN Scholarly Paper No. 4633945). Social Science Research Network. <https://doi.org/10.2139/ssrn.4633945>
- Villa, P. (2023). Legal Process Automation as a Tool for Access to Justice: A Proposal to Restructure First Contact Interviews in the Federal Institute of Public Defenders. *Mexican Law Review*, 41-80. <https://doi.org/10.22201/ijj.24485306e.2023.2.17617>

EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO: DESAFÍOS E IMPLICACIONES ÉTICAS

Víctor J. Flores-Ríos¹

RESUMEN:

Esta investigación tuvo por objetivo describir el vínculo entre la inteligencia artificial y el ámbito legal, para esto se utilizó un enfoque cualitativo, una investigación de tipo básica, con un diseño no experimental – descriptivo, recolectando la información de las bases de datos: DIALNET, DOAJ, REDALYC y EBSCOhost, obteniendo un total de 30 artículos que se analizaron. Los principales resultados arrojaron lo siguiente: La IA impacta el sistema judicial en dos niveles: como herramienta que mejora procesos administrativos, y como sustituto de funciones humanas. Esto plantea cuestiones como la protección de datos y la ética en el uso de algoritmos, puesto que la IA depende de grandes volúmenes sobre información personal, lo que genera desafíos para la privacidad y el establecimiento de normativas que resguarden los derechos esenciales; asimismo, los algoritmos, al ser creados por humanos, pueden reflejar prejuicios y llevar a decisiones injustas, lo que genera interrogantes sobre la responsabilidad cuando un sistema de IA cause daño; este artículo explora cómo la IA afecta al derecho, desde su impacto en la enseñanza universitaria hasta su influencia en los principios y garantías fundamentales en los procesos judiciales. También aborda la preocupación por la privacidad y la toma de decisiones autónomas, y cómo establecer la culpabilidad ante perjuicios ocasionados por inteligencias artificiales.

Palabras Clave: Inteligencia artificial, derecho, protección de datos, decisiones, judicial.

¹ vfloresr2@upao.edu.pe

Programa de estudio de Derecho, Universidad Privada Antenor Orrego

ABSTRACT

This research aimed to describe the relationship between artificial intelligence and law, for this a qualitative approach was used, a basic research type, with a non-experimental - descriptive design, collecting information from the databases: DIALNET, DOAJ, REDALYC and EBSCOhost, obtaining a total of 30 articles that were analyzed. The main results showed the following: AI impacts the judicial system on two levels: as a tool that improves administrative processes, and as a substitute for human functions. This raises issues such as data protection and ethics in the use of algorithms, as AI depends on large volumes of personal data, which poses challenges for privacy and the creation of laws that protect fundamental rights; Furthermore, algorithms, being created by humans, can reflect biases and lead to unfair decisions, raising questions about liability when an AI system causes harm; This article explores how AI affects law, from its impact on university teaching to its influence on fundamental principles and guarantees in judicial processes. It also addresses concerns about privacy and autonomous decision-making, and how to determine liability in the event of harm caused by AI systems.

Keywords: artificial intelligence, right, data protection, decisions, judicial.

INTRODUCCIÓN

Con el pasar de los años se ha visto cómo la inteligencia artificial (IA), se integra cada instante más a los diferentes aspectos de la vida cotidiana, como en la atención médica, el comercio, el entretenimiento, la educación y por supuesto en el derecho; estos son algunos aspectos en los que se está presentando mayor integridad.

Este avance tecnológico ha desencadenado una revolución tecnológica y como se expresa en el párrafo anterior, va reformando varios aspectos de la vida cotidiana; desde la forma en cómo se interactúa con los dispositivos, hasta en cómo gestionan sus operaciones las empresas. En el contexto de los nuevos escenarios sociales del siglo XXI, las tecnologías de la información se han integrado en la vida cotidiana y en las transformaciones socioculturales, formando parte de la cuarta generación de derechos humanos (Galindo, 2019).

La IA es la capacidad que poseen las máquinas para la realización de tareas o labores que requieren normalmente de inteligencia humana; como tomar decisiones, aprender o resolver problemas; es así que la inteligencia artificial está transformando el panorama legal de maneras multifacéticas y profundas. La IA se ha transformado en una herramienta valiosa en el

campo del derecho al plantear desafíos y dilemas significativos para su regulación; con su capacidad gran capacidad en analizar datos, aprender patrones y tomar decisiones autónomas; es por ello que el derecho al ser un sistema normativo diseñado para regular la conducta humana y resolver conflictos, aún enfrenta el reto de adaptarse a la veloz evolución tecnológica.

Al aplicarlo en el ámbito legal, no solo se redefinirá la administración en los procesos judiciales y en los asesoramientos legales, sino que se debe desafiar las nociones tradicionales de equidad y responsabilidad en el derecho. Es por ello que el adaptarse no solo implica la creación de nuevas normativas, sino también el ajuste de principios legales y la reinterpretación.

El proceso de irrupción y la expansión de la IA en el sistema de justicia se lleva a cabo en dos niveles, en el primero se muestra a la tecnología instrumental a través de una herramienta, como por ejemplo los expedientes y las notificaciones; mientras que el segundo se refiere a la tecnología funcional, que vendría a ser un complemento o sustitución a la función humana (De Luis, 2023).

Teniendo en cuenta lo antes citado, es decir los dos niveles expuestos, se podrá conectar con temas relacionados; el primer nivel sería la protección de datos y privacidad, y el segundo relacionado a la ética y a la responsabilidad. Y eso es lo que se plantea en este trabajo, la relación entre la Inteligencia Artificial y el Derecho.

La privacidad y la protección de datos son particularmente campos sensibles, pues en los sistemas de IA dependen de grandes datos que requieren accesos a la información personal; planteando significativos desafíos para recopilar, utilizar y almacenar información. Esto propone que las leyes de privacidad evolucionen a fin de enfrentar estos desafíos, para garantizar de manera ética el manejo de los datos y a respetar el derecho a la privacidad de los individuos.

Países que conforman la UE, abordan algunos de estos problemas, requiriendo así ajustes continuos en la tecnología de la IA que tiene una rápida evolución; donde marcos legales como el **Reglamento General de Protección de Datos**, son necesarios para la creación de leyes que puedan adaptarse a los avances tecnológicos sin vulnerar la garantía de los derechos esenciales (Sánchez, 2016).

También la ética juega un papel crucial en la regulación de la IA, pues la creación y el uso de algoritmos pueden influir en decisiones judiciales o de contratación, que deben ser gestionadas con cuidado para evitar discriminación. Los algoritmos son diseñados por las personas, reflejando y ampliando prejuicios existentes; lo que podría llevar a decisiones injustas y desiguales; entonces los sistemas de IA que operan de manera autónomas, como los algoritmos o vehículos autónomos, pueden tomar decisiones que afecten a las personas; esto conlleva a plantear preguntas sobre la responsabilidad de una persona, cuando la IA actúa de manera perjudicial o causa algún daño.

Es por ello que en este artículo se analizó la influencia de la inteligencia artificial o también llamada IA en el ámbito legal, lo cual da los alcances de su desarrollo y adecuación en este campo de estudio desarrollando su papel en las enseñanzas universitarias, así mismo su influencia en la mentalidad de los juristas al momento de aplicar las normas. De igual manera se señala la afectación de los principios y garantías fundamentales en el proceso judicial por parte de la IA.

Su influencia en términos de resguardo de información y privacidad, pues la inteligencia artificial dentro del derecho implica que se procese y recopile datos, provocando preocupación en el acceso personal de la información. Todo esto abordado a raíz de los escándalos mediáticos de las redes y plataformas digitales que conlleva a plantear la creación de leyes para regular los sistemas IA.

Como otro punto se trató su influencia en las tomas de decisiones que abarca en que la inteligencia artificial es capaz de generar predicciones con mayor precisión, y también pueden realizar razonamientos con el fin de tomar decisiones autónomas, de manera que esto interviene en el pensamiento y en el modo de vida de las personas. Y, por último, la culpabilidad de la IA en situaciones de perjuicio, es decir buscar al responsable de los delitos cometidos por estos sistemas, llevando a formular interrogantes de quién puede responder por los daños causados, y si existiría una reparación.

METODOLOGÍA

Esta investigación tuvo como fin lograr un acercamiento a la relación de la Inteligencia Artificial con el Derecho, su impacto en la administración de justicia y en la toma de decisiones judiciales, protección de datos y

privacidad; así mismo se desarrolló un enfoque cualitativo con un tipo de investigación básica con un enfoque jurídico, tanto explicativo como descriptivo, dado que se trata de un estudio puramente dogmático (Sánchez & Zegarra, 2022).

La técnica que se usó en este trabajo fue la revisión bibliográfica y como instrumento la ficha bibliográfica, lo cual implica que tomó como base la recopilación de datos, incluyendo la indagación de 31 artículos de investigación que tengan relación con el tema antes mencionado en las plataformas digitales de bases de datos; como: DOAJ, Redalyc, Scopus, Dialnet, EBSCO y Scielo. Lo que arrojó un campo de estudio en países como: México, Venezuela, Chile, Argentina, Colombia, Ecuador, Perú y España; sobre la relación del derecho con la inteligencia artificial, su regulación en algunos países, su uso en las tomas de decisiones de jueces, así como sus análisis en los derechos de protección de datos y protección a la privacidad.

Se hizo un análisis descriptivo basado en un diseño de investigación no experimental; según Villareal (2023), es un enfoque metodológico en investigación, especialmente popular en las ciencias sociales, en el que el investigador observa y analiza sin intervenir o alterar las variables de interés; este tipo de investigación es fundamental para entender fenómenos tal y como ocurren en su contexto natural. Pues la finalidad de este trabajo es la relación de la Inteligencia Artificial IA con el Derecho; como este ha incursionado en los procesos judiciales y si existe o debe existir su regulación en un futuro próximo, se observa en la Unión Europea y ciertos países del área. El inicio de la investigación se centró a mediados de agosto del año 2024 teniendo como primer punto recabar la información necesaria para la formulación de introducción y realización de los objetivos, concluyendo a finales del año 2024.

El trabajo se desarrolló de la siguiente manera: En primer lugar fue describir los desafíos que plantea la inteligencia artificial en términos de protección de datos y privacidad; en segundo lugar, examinar las repercusiones éticas de la inteligencia artificial en decisiones autónomas; posteriormente, evaluar su impacto en la justicia y los procesos judiciales; y, por último, determinar la responsabilidad en perjuicios ocasionados por estas mismas.

RESULTADOS

1. La IA en términos de protección de datos y privacidad

Antes de hablar de los desafíos que involucra a la IA en los derechos de protección de datos y privacidad, se tiene que tener un conocimiento de estos derechos y cuáles son sus alcances en la vida de las personas y como son vulneradas con los sistemas IA. Según Sánchez (2023) la protección jurídica de los datos tiene su origen en lo establecido por el Tribunal Constitucional de Alemania en el año 1983 en él se señalaba que el desarrollo libre de la personalidad implica, en el contexto actual del procesamiento de datos, la protección de las personas ante la recolección restringida de su información; y se afirma de que esto se encuentra protegido en la Ley Fundamental, en relación con los derechos fundamentales.

La protección de la privacidad o la vida privada como se conoce a las otras legislaciones como México, es la intimidad que tienen las personas. Farfán *et al.* (2023) afirmaron que la implementación de la IA en el sector jurídico supone recopilación y procesamiento de datos, lo que plantea preocupaciones en términos de privacidad, especialmente cuando el IA accede a información personal confidencial.

Las publicaciones sobre privacidad tienen como objetivo que la información funcione como un medio para empoderar a las personas y abordar la cuestión de cómo resguardar los datos personales. Estas publicaciones explican cómo opera la privacidad, destacan su importancia, alertan sobre el uso de ciertas aplicaciones y buscan educar sobre la protección de datos, ofreciendo recomendaciones y acciones para enseñar a proteger la información en diversas aplicaciones y navegadores (Galindo, 2019).

Galindo destaca la importancia de educar a las personas sobre cómo proteger sus datos personales en un ecosistema digital en constante expansión cada vez más complejo. Las publicaciones sobre privacidad buscan empoderar a los usuarios al proporcionarles herramientas y conocimientos necesarios para resguardar su información, ayudándoles a tomar decisiones informadas sobre el uso de aplicaciones y navegadores.

La protección de datos no solo es uno de los aspectos más desarrollados en las constituciones en cuanto a la informática, sino también el primero en el que se pensó debido al riesgo que representaba para la privacidad de las personas. Este riesgo abarcaba tanto la recopilación de datos sobre los individuos, como su interrelación y la creación de perfiles. Este enfoque

ya estaba presente en la Constitución Portuguesa de 1976 (art. 35) y en el artículo 18.4 de la Constitución Española. A raíz de ello, se comenzaron a buscar respuestas y mecanismos para resguardar a los individuos ante los poderes públicos y privados; por lo que, la recopilación y utilización de datos no es exclusiva de las entidades estatales. De hecho, los actores privados pueden tener incluso mayor capacidad tecnológica que los propios gobiernos. Estas garantías pueden organizarse en tres grandes áreas fundamentales (Sánchez, 2016).

Lo mencionado destaca la relevancia de la seguridad de la información como uno de los primeros derechos abordados por las constituciones, dado el riesgo que la informática representa para la privacidad personal; este énfasis en la privacidad, especialmente en relación con la acumulación y el cruce de datos, subraya la necesidad de contar con mecanismos legales que salvaguarden la intimidad de las personas.

Así mismo se señala la expansión del alcance de la protección de datos, no solo frente al poder público, sino también frente a los actores privados; este es un aspecto crucial, pues muchas veces las empresas privadas cuentan con recursos y capacidades tecnológicas superiores a los del propio estado, lo que agrava los riesgos de vulneración de la privacidad, aquí se abre un debate sobre la necesidad de una regulación robusta que contemple a todos los actores involucrados en el tratamiento de datos personales, más allá de los poderes públicos.

Es necesario replantear los marcos conceptuales que sustentan el razonamiento jurídico, debido a que las nuevas tecnologías alteran las estructuras sociales y los derechos fundamentales; por tanto, el reto no solo es técnico o normativo, sino también conceptual: transformar la mentalidad del jurista frente a un mundo digitalizado.

Morales (2021) expresa que hay otras cuestiones que han sido analizadas en el campo jurídico aquellas cuestiones vinculadas a la privacidad y los datos personales. En los últimos años, a partir de controversias mediáticas, este problema ha comenzado a tratarse parcialmente, impulsando la elaboración de normativas sobre la protección de datos. No obstante, en este escenario, la IA suele ser vista sólo como un medio para obtener estos datos, y no como una herramienta que depende de la información para funcionar, lo cual plantea una serie de interrogantes que se discutirán más adelante.

El fragmento antes citado resalta cómo el derecho ha comenzado a abordar la protección de datos personales, especialmente a raíz de escándalos mediáticos, mediante leyes y regulaciones. Sin embargo, el texto señala que la IA se ha considerado principalmente como un medio para recolectar datos, sin reflexionar sobre cómo esta depende de la información para operar, lo que genera cuestionamientos clave sobre su regulación, porque no solo se trata de proteger los datos, sino también de entender cómo su contexto y uso afectan la operatividad de la tecnología y sus implicaciones éticas y legales.

Dicho de otro modo, la inteligencia artificial debe ser creada con el propósito de beneficiar a las personas y no explotarlas, especialmente en el manejo de datos personales, donde podrían vulnerarse derechos esenciales como la igualdad, la privacidad, la seguridad de la información e incluso el derecho a la vida (Mendoza, 2021).

El autor antes citado resalta una preocupación fundamental sobre el uso de la inteligencia artificial como su potencial para vulnerar derechos humanos esenciales. La IA, cuando no se regula adecuadamente, puede ser utilizada de manera que perjudique a las personas, como en el caso del tratamiento irresponsable o abusivo de los datos personales.

Mientras que el diseño y la implementación de la IA deben garantizar una mejor calidad de vida para las personas, respetando su dignidad y derechos fundamentales, en lugar de explotar o poner en riesgo su privacidad, seguridad o igualdad. Alborno (2021) Mencionó que el manejo de la información personal de un individuo identificable o físico debe estar amparado por el derecho a su protección.

En este sentido, la salvaguarda de los datos personales constituye un derecho humano autónomo, reconocido en diferentes marcos normativos, como la Carta de los Derechos Fundamentales de la Unión Europea, donde su artículo establece que toda persona tiene derecho a la protección de sus datos.

Así mismo Alborno afirma que los datos personales que solicitan consentimiento para ser utilizados por los sistemas IA, tienden a vulnerar el derecho a la privacidad y a la protección de datos personales, además de afectar garantías como la no discriminación y la autonomía en la toma de decisiones, estas son situaciones diarias que ilustran los efectos negativos de este tratamiento sin que el autor sea consciente.

La automatización del tratamiento de datos, a menudo opaca y fuera del control directo de los titulares, puede resultar en consecuencias invisibles, como la discriminación algorítmica o la limitación de las opciones disponibles para una persona en función de datos que no han sido adecuadamente gestionados, esta realidad plantea un desafío importante para el derecho y la ética, dado que los individuos deben tener no solo el derecho a la protección de sus datos, sino también el derecho a comprender cómo se usan y cómo impactan en su vida cotidiana. Martínez reflexiona que la orientación de los estudios jurídicos sobre informática y robótica van hacia una problemática instrumental o técnica, creyendo una herramienta útil a la máquina. O estos estudios también se centran en un tratamiento jurídico o problemática ética que pueden ser: comercio electrónico, protección de datos, amenazas a la libertad, ciberseguridad, acceso y control de usuarios; pero lo que interesa aquí es el impacto a la forma mental del jurista (Valero, 2021).

Valero señala que los estudios jurídicos sobre informática y robótica suelen centrarse en aspectos técnicos o legales específicos, como la protección de datos o la ciberseguridad. Sin embargo, el verdadero desafío para los juristas radica en cómo estas tecnologías impactan su forma de pensar y abordar el derecho; más allá de adaptar las leyes a los avances tecnológicos.

En lo que respecta a las repercusiones del uso de sistemas de inteligencia artificial para salvaguardar los datos personales, los límites para evitar un efecto negativo de estos mecanismos abarcan el derecho al consentimiento explícito de los individuos para el procesamiento de sus datos, el principio de minimización de estos datos y el conjunto de derechos relacionados con la autorización para la toma de decisiones automatizadas (Juri, 2021).

La autora citada anteriormente resalta la necesidad de proteger la privacidad en el uso de inteligencia artificial, asegurando que el consentimiento explícito, la minimización de datos y la regulación de decisiones automatizadas sean principios clave. Esto garantiza que se respeten los derechos de los individuos y se eviten impactos negativos, promoviendo un uso ético y responsable de la tecnología.

Y por último Toache & Rosales (2023) indican que, en esencia, para que estas tecnologías sean aceptadas y generen un efecto positivo en la sociedad, no solo deben poseer capacidades técnicas avanzadas, sino también garantizar el respeto a los derechos de información, transparencia y rendición de cuentas. Asimismo, es crucial asegurar la protección de

datos y la privacidad, definir límites precisos en su uso, distribución y almacenamiento, y disponer de mecanismos de ciberseguridad que prevengan el robo de información.

Es decir que ellos subrayan que, más allá de la innovación, es crucial garantizar la transparencia, la rendición de cuentas y el respeto por los derechos de los usuarios. La protección de datos y la privacidad no solo dependen de la calidad técnica de las herramientas, sino también de las políticas claras y las medidas de ciberseguridad para evitar vulnerabilidades.

2. La IA en la toma de decisiones

Cabrera (2024) indica que los sistemas de aprendizaje automático son procesos computacionales creados para extraer conocimientos de los datos y mejorar la precisión de sus decisiones y predicciones. Estos sistemas inician con un conjunto de características definidas para identificar patrones (como distinguir entre la imagen de un gato y la de un perro) y se entrenan con grandes volúmenes de datos etiquetados que les permiten reconocer cada categoría. De este modo, el algoritmo de aprendizaje automático es capaz de identificar esas características en nuevos datos (como una imagen sin etiquetar de un animal doméstico) y hacer inferencias sobre si se trata de un gato o un perro, incluso si la imagen no fue parte del conjunto de entrenamiento.

El enfoque de Cabrera resalta la capacidad de los sistemas de aprendizaje automático para generalizar y hacer predicciones con alta precisión, incluso en situaciones no previamente previstas; no obstante, también se podría profundizar más en cómo factores como la calidad de los datos, la selección de características relevantes y la complejidad de los algoritmos influyen en la efectividad y la precisión de estos sistemas. Asimismo, sería interesante explorar los retos asociados, como el sesgo en los datos de entrenamiento o la necesidad de grandes volúmenes de datos etiquetados, que pueden limitar la aplicabilidad de estos sistemas en algunos contextos.

Según Valero (2021) la inteligencia artificial es un campo de la informática que emplea procesos diseñados para que las máquinas puedan razonar y tomar decisiones de forma similar a un ser humano; en el ámbito jurídico, La inteligencia artificial se emplea en diversos ámbitos, como: i) modelos para el razonamiento y la toma de decisiones; ii) categorización de documentos jurídicos; iii) recopilación de información; y iv) diseño y estructuración de sistemas normativos (Fernández & Boulat, 2015).

De este modo, la planificación de un sistema legislativo busca organizar la información y facilitar la interacción entre el usuario y la máquina, permitiendo que las personas realicen sus actividades con el apoyo de un sistema, lo que contribuye a tomar decisiones más informadas.

Lo señalado anteriormente subraya el potencial transformador de la inteligencia artificial en el ámbito del Derecho, destacando cómo esta tecnología puede replicar el razonamiento humano para tomar decisiones, lo que abre nuevas posibilidades para la automatización y la mejora de procesos legales. La aplicación de la IA en áreas como la argumentación jurídica, la clasificación de textos legales y la extracción de información permite una mayor eficiencia y precisión en el manejo de grandes volúmenes de datos legales; además, la planificación de sistemas legislativos apoyados por IA, como se menciona, tiene el objetivo de optimizar la interacción entre el usuario y la máquina, lo que no solo facilita la labor de los profesionales del derecho, sino que también podría mejorar el acceso a la justicia y ayudar a las personas a tomar decisiones más informadas.

La inteligencia artificial posibilita que tareas o decisiones que usualmente realizan los humanos sean llevadas a cabo por algoritmos, los cuales se alimentan de datos obtenidos de su entorno para generar resultados que, en teoría, son más racionales (Ortega, 2023). En esto se destaca cómo la inteligencia artificial puede automatizar decisiones humanas utilizando algoritmos que procesan datos para obtener resultados más racionales. Sin embargo, esto plantea desafíos sobre la calidad de los datos, los posibles sesgos y la necesidad de mantener el control humano en decisiones importantes.

No obstante, hoy en día, ninguno de estos sistemas puede justificar sus acciones ni tomar decisiones con la misma complejidad que los seres humanos. El principal temor o conflicto que los humanos sienten hacia la inteligencia artificial se origina en la influencia del cine de ciencia ficción, donde las máquinas son representadas tomando decisiones en contra de los humanos. No obstante, esto es incorrecto, debido a que el aprendizaje automático no es una capacidad central de la inteligencia artificial (Farfán *et al.*, 2023).

Como ha indicado Susskind, los ordenadores no deben reemplazar a los jueces en su labor. La toma de decisiones en casos complejos, especialmente cuando se trata de cuestiones de principios, políticas y moralidad, está muy por encima de las capacidades técnicas recientes de

los sistemas informáticos, que se limitan a tareas como la automatización de documentos, notificaciones e investigación de casos (Krenz, 2021).

La diferencia fundamental entre la capacidad de los humanos para tomar decisiones complejas y la funcionalidad de los sistemas de la IA, resalta en la afirmación de Susskind de que la importancia de la intervención humana en la toma de decisiones judiciales, especialmente en contextos que involucran principios éticos, morales y políticos; es esencial, pues los juicios no solo requieren análisis de datos, sino también juicio, empatía y una comprensión profunda de la justicia.

Existe un temor hacia la IA, este miedo puede desvirtuar la realidad de lo que la tecnología es capaz de hacer hoy en día; es necesario entender que, aunque la IA puede realizar tareas específicas de manera eficiente, no puede sustituir la complejidad del pensamiento humano ni la capacidad de juicio en situaciones que requieren sensibilidad y ética.

En el ámbito de la inteligencia artificial aplicada al derecho, existen programas avanzados que no solo automatizan tareas burocráticas en el ámbito legal, sino que también intervienen directamente en el proceso judicial como decisores. Un ejemplo de esto son los programas basados en el conocimiento jurídico, que realizan representaciones y análisis de casos utilizando su conocimiento legal y, mediante la actualización de datos, pueden emitir un juicio legal sustancial sobre qué leyes han sido violadas, a partir de un análisis lógico-deductivo de las obligaciones, prohibiciones o permisos infringidos (Nieva, 2018 citado por Villasmil et al., 2024).

Lo antes citado señala cómo la inteligencia artificial en el ámbito legal va más allá de la automatización de tareas administrativas, participando activamente en el proceso judicial. Al basarse en el conocimiento jurídico y el análisis de datos, estos programas pueden emitir juicios legales, lo que plantea tanto oportunidades como desafíos en cuanto a la precisión, la transparencia y la supervisión humana en las decisiones legales.

Otra cuestión es la adecuación o no de las respuestas proporcionadas por otras tecnologías en relación con la informática y la inteligencia artificial, estas pueden influir o mediar en las decisiones que se tomen sobre ellas mismas, dado que se trata de inteligencia externa y no humana. No es casual que la informática, y potencialmente la inteligencia artificial, ya se utilicen como herramientas en la toma de decisiones importantes, como ocurrió recientemente con el reparto de refugiados en Europa, donde se buscó, precisamente, despolitizar dicha decisión (Sánchez, 2016).

El citado autor destaca una cuestión clave: la influencia de la informática y la inteligencia artificial en la toma de decisiones, especialmente cuando estas tecnologías, como sistemas de inteligencia externa, pueden mediar en decisiones que afectan a la sociedad. La idea de que las respuestas generadas por estas tecnologías puedan ser adecuadas o no plantea una reflexión crítica sobre su papel en contextos complejos, como el reparto de refugiados en Europa; el ejemplo de la despolitización de esa decisión a través de herramientas informáticas e inteligencia artificial sugiere que, al eliminar factores subjetivos o ideológicos, estas tecnologías pueden contribuir a una toma de decisiones más objetiva y eficiente.

Ahora se puede realizar un análisis desde otro medio, como lo es el Big Data; Sánchez (2023) manifiesta que el análisis a través de Big Data ha transformado la manera en que se gestionan diversos aspectos del mundo, desde la toma de decisiones en políticas públicas hasta áreas como marketing, salud pública, economía, elecciones y negociaciones internacionales. El manejo de grandes volúmenes de datos permite obtener información más precisa; sin embargo, en temas de derechos humanos, y especialmente en lo relacionado con la protección de datos personales, el uso de Big Data ocupa un papel crucial y si se utiliza de forma indebida, puede dar lugar a actos discriminatorios y aumentar la desigualdad de oportunidades.

Entonces Sánchez resalta el impacto transformador de Big Data en la gestión de múltiples áreas, desde políticas públicas hasta economía y marketing, destacando su capacidad para proporcionar información más precisa y tomar decisiones más informadas, también pone en evidencia un aspecto crucial: el uso adecuado de estos datos es fundamental, especialmente en lo que respecta a los derechos humanos y la protección de datos personales. La advertencia sobre los riesgos de un uso indebido es relevante, dado que el análisis incorrecto de grandes volúmenes de datos puede no solo invadir la privacidad, sino también reforzar desigualdades y generar discriminación, haciendo que este equilibrio entre el aprovechamiento de las ventajas de Big Data y la necesidad de un manejo ético y responsable sea esencial para evitar consecuencias negativas en la sociedad.

Existe un debate donde surge la pregunta de ¿por qué es relevante la ética en el desarrollo de la inteligencia artificial? La ética abarca a todos los seres con capacidad de actuar con autonomía e inteligencia, es decir, aquellos que pueden tomar decisiones y razonar de manera lógica. La autonomía, en este contexto, hace referencia a la facultad de los seres racionales para

escoger libremente su curso de acción, lo que la convierte en un rasgo característico y exclusivo de los seres humanos (Zabala, 2021).

En lo anterior se resalta la relevancia de la ética en el desarrollo de la inteligencia artificial, especialmente al considerar la autonomía como una característica clave de los seres humanos. La pregunta plantea la necesidad de reflexionar sobre si las máquinas, al carecer de verdadera autonomía y racionalidad, pueden o deben tomar decisiones por sí mismas. Esto abre un debate fundamental sobre el control humano, la responsabilidad y las implicaciones éticas de delegar decisiones importantes a sistemas artificiales.

En Argentina existe un proyecto donde se establece una prohibición sobre el uso de la inteligencia artificial para manipular o influir en decisiones clave, como los procesos electorales o la formación de opiniones públicas (Vercelli, 2024). Este proyecto subraya la importancia de regular el uso de la inteligencia artificial para proteger la integridad de procesos democráticos, como las elecciones y la formación de opiniones públicas. La medida busca prevenir posibles manipulaciones y asegurar que la tecnología se utilice de manera ética y transparente.

Galvis & Esquivel (2022) señalaron que la robótica explora cómo la inteligencia artificial puede evolucionar para desarrollar actividades propias de los seres humanos, no sólo en términos de acciones, sino también en la capacidad de tomar decisiones. Es decir que ellos destacan el potencial de la robótica e inteligencia artificial para replicar no solo las acciones humanas, sino también la capacidad de tomar decisiones, lo que plantea importantes cuestiones éticas y prácticas sobre el grado de autonomía que pueden alcanzar las máquinas en el futuro.

Farfán et al., (2023) mencionan que, no obstante, hoy en día, ninguna de estas tecnologías tiene la capacidad de justificar sus propios actos ni de tomar decisiones con la misma complejidad o criterio con el que lo hacen los seres humanos. El principal temor o conflicto de los seres humanos con la inteligencia artificial proviene, en gran parte, de las películas de ciencia ficción, que representan a las máquinas como entidades capaces de tomar decisiones en contra de los seres humanos.

Los autores destacan una preocupación clave en el debate sobre la inteligencia artificial: la incapacidad de las máquinas para justificar sus decisiones con la misma complejidad que los seres humanos. Esta

limitación resalta la diferencia fundamental entre el razonamiento humano y la lógica de los sistemas automatizados; además, se menciona cómo el temor hacia la IA está alimentado por la representación distorsionada en la ciencia ficción, donde las máquinas toman decisiones perjudiciales para la humanidad; y este miedo, aunque comprensible, no refleja la realidad tecnológica, que sigue siendo mucho más controlada y limitada.

3. La inteligencia artificial en la administración de justicia y en los procesos judiciales

La inteligencia artificial está transformando progresivamente el ámbito jurídico, mejorando la rapidez y exactitud en actividades como el examen de contratos, la investigación normativa y el estudio de casos. No obstante, su integración presenta retos legales, como la determinación de responsabilidades en el uso de estos sistemas, la salvaguarda de la privacidad y los datos personales, así como el peligro de sesgos en los algoritmos (Farfán *et al.*, 2023).

La integración de la inteligencia artificial en el ámbito jurídico optimiza la rapidez y exactitud en procesos como la evaluación de contratos y el estudio de casos, sin embargo, también genera retos significativos, como la atribución de responsabilidades en estos sistemas, la seguridad de la información y la privacidad, además del posible sesgo en los algoritmos. Para garantizar un uso equitativo y ético de esta tecnología, es fundamental contar con una regulación adecuada.

La implementación de sistemas de IA en la Justicia no es reciente, los sistemas expertos jurídicos, fundamentados en el conocimiento, ya representan la aplicación más destacada de la inteligencia artificial en el ámbito legal y en la toma de decisiones judiciales. Su valor radica en la capacidad de abordar conflictos concretos, proponer soluciones basadas en conocimiento especializado y justificar sus razonamientos (Ordelin, 2021).

La aplicación de la inteligencia artificial en la Justicia, en particular a través de sistemas expertos jurídicos, ha sido un avance importante en la aplicación de la tecnología al Derecho. Estos sistemas optimizan la toma de decisiones judiciales y permiten una mayor precisión en la resolución de conflictos al aplicar el conocimiento experto, lo que también contribuye a la transparencia y confianza al explicar los razonamientos detrás de las decisiones, con lo cual es fundamental que su implementación

sea responsable y regulada para evitar riesgos como la opacidad en el razonamiento o la dependencia excesiva de la tecnología.

En este contexto, el cambio de mentalidad en los juristas no se logrará únicamente a través de una regulación normativa y la aplicación de esas normas por parte de los operadores del Derecho. Un verdadero cambio mental requiere reflexionar sobre cómo la inteligencia artificial impacta al Derecho y sobre cómo dirigir la profesión hacia una auténtica ciencia multidisciplinaria (Valero, 2021).

Lo antes mencionado señala que el cambio de mentalidad en los juristas frente a la inteligencia artificial no se logrará solo con nuevas normativas, sino que requiere una reflexión profunda sobre cómo la IA está transformando el Derecho. Además, destaca la necesidad de orientar la profesión hacia una ciencia multidisciplinaria, integrando conocimientos de diversas áreas para afrontar los desafíos tecnológicos en el ámbito legal, este enfoque demanda un cambio en la formación y la mentalidad de los profesionales del Derecho.

La irrupción de la robótica y la inteligencia artificial (IA) ha sido equiparada al impacto de la invención de la imprenta de Gutenberg en el siglo XV. Este avance facilitó la transición del conocimiento basado en la doctrina religiosa hacia un enfoque empírico, marcando el inicio del cambio de la Era de la Religión a la Era de la Razón. Como consecuencia, se impulsaron transformaciones significativas, entre ellas el surgimiento de la Ilustración, un proceso que perduró por siglos (Navas, 2021).

El párrafo anterior destaca el gran impacto de la inteligencia artificial y la robótica, comparándolas con la invención de la imprenta por Gutenberg, así como la imprenta permitió el acceso al conocimiento empírico y transformó la sociedad, la IA tiene el potencial de generar un cambio similar en el mundo. Este paralelismo sugiere que, como la Ilustración marcó una nueva era, la inteligencia artificial podría dar paso a una transformación profunda en diversas áreas de nuestra vida.

Por ejemplo en Colombia recientemente se ha puesto en marcha la aplicación TYBA, la cual ha contribuido a mejorar el sistema informático en el ámbito judicial, dando inicio a un proceso clave para modernizar la administración de justicia y digitalizar los expedientes judiciales en el área de las acciones de tutela (Suárez et al., 2023).

Entonces la implementación de la aplicación TYBA marca un avance significativo en la modernización del sistema judicial, facilitando la

digitalización de expedientes y optimizando la gestión de las acciones de tutela; este paso hacia la innovación tecnológica promete mejorar la eficiencia y accesibilidad del proceso judicial.

La vigencia, efectividad y salvaguarda de los derechos humanos se ha visto alterada por la era digital. Las nuevas tecnologías han transformado la manera en que los derechos humanos se ejercen en el entorno virtual, lo que inevitablemente afectará al mundo real, por lo que es necesario que la legislación y la actuación de los encargados de impartir justicia se adapten a estos cambios (Mendoza, 2021).

Se resalta cómo la era digital ha transformado la forma en que se gestionan y protegen los derechos humanos, tanto en el ámbito virtual como en el real y las nuevas tecnologías han introducido desafíos que requieren una actualización de las leyes y de la forma en que los jueces y autoridades interpretan y hacen valer los derechos fundamentales, por lo que es esencial que las normativas y procedimientos judiciales evolucionen para asegurar el respeto a los derechos humanos en todos los ámbitos, especialmente en una sociedad cada vez más digitalizada.

Es fácil prever los riesgos que conlleva el uso de herramientas de IA en el proceso judicial y cómo esto podría afectar los principios y garantías fundamentales del procedimiento cuando el órgano judicial tome una decisión basándose en el resultado proporcionado por la máquina (De Luis, 2023). El autor señala los riesgos de utilizar inteligencia artificial en el ámbito judicial, como la posible afectación de principios y garantías procesales; aunque la IA puede mejorar la eficiencia, depender de sus resultados podría comprometer la transparencia y la justicia en las decisiones judiciales, lo que requiere una regulación adecuada para evitar consecuencias negativas.

Según la Organización Mundial de la Propiedad Intelectual (OMPI), la implementación de la inteligencia artificial se ha extendido a casi todos los sectores de la economía y la sociedad, impactando de manera significativa el proceso de creación, producción y distribución de bienes intangibles, tanto económicos como culturales. Esta expansión plantea un desafío para la propiedad intelectual, las aplicaciones de IA pueden generar, de manera autónoma o asistida, obras literarias y artísticas, lo que plantea la necesidad de considerar cómo proteger dichas creaciones (Osorio, 2022).

Lo anterior señala cómo la expansión de la inteligencia artificial en diversos sectores plantea nuevos desafíos para la propiedad intelectual. A

medida que la IA crea obras literarias y artísticas, surge la necesidad de adaptar las leyes de propiedad intelectual para proteger estas creaciones, asegurando que los derechos sobre obras generadas por máquinas sean claramente definidos y gestionados.

Según Casanovas, la inteligencia artificial no busca replicar las capacidades cognitivas del cerebro humano, sino analizar y comprender su organización y operatividad en aspectos como el procesamiento de información, la memoria, el lenguaje, la interpretación, la expresión y el razonamiento. A partir de este conocimiento, se pretende optimizar dichos procesos a través de herramientas computacionales y adaptarlos a sistemas automatizados para su aplicación en contextos prácticos (Parra & Concha, 2021).

Los autores resaltan una visión clave sobre la inteligencia artificial, que según Casanovas, señala que su objetivo no es replicar el cerebro humano, sino entender y optimizar sus funciones cognitivas fundamentales. Al centrarse en mejorar procesos como la memoria, el razonamiento y el lenguaje mediante la computación, la IA busca aplicaciones prácticas en contextos reales, lo que abre nuevas posibilidades para resolver problemas complejos de manera más eficiente y precisa.

No obstante, para entender la relevancia de la tecnología en el aprendizaje del derecho, es necesario comprender cómo se lleva a cabo la toma de decisiones, debido a que esto proporciona seguridad y confianza en la administración de justicia (Rincón y Martínez, 2020). Esta tarea, además, puede ser realizada a través de la inteligencia artificial (Quezada et al., 2022).

Los autores antes citados destacan la importancia de comprender el proceso de toma de decisiones en el derecho para asegurar confianza y seguridad en la justicia. La inteligencia artificial, al poder replicar y mejorar estos procesos, ofrece una herramienta valiosa para optimizar la administración de justicia, asegurando que las decisiones sean más precisas y objetivas, subrayando cómo la tecnología puede jugar un papel fundamental en el aprendizaje y la práctica del derecho, facilitando una gestión más eficiente y confiable.

4. Daños causados por los sistemas IA

La tecnología ha sido y continúa siendo un pilar esencial en ámbitos como el sector económico, el ámbito educativo, el sistema de salud y la gestión de políticas públicas y la vida diaria a nivel global. En este sentido, su

aplicación responsable puede aportar beneficios significativos tanto en el sector público como en el privado. No obstante, un uso inadecuado puede afectar gravemente la protección de los derechos humanos, en particular la dignidad y el derecho al libre desarrollo de la personalidad, estrechamente vinculado con el resto de los derechos fundamentales (Sánchez, 2023).

El párrafo anterior destaca correctamente cómo la tecnología es crucial en sectores como la economía y la salud, y cómo su uso adecuado puede beneficiar a la sociedad. Sin embargo, también subraya los riesgos de su mal uso, que puede poner en peligro derechos humanos esenciales, como la integridad y la autonomía en el desarrollo personal. Esto resalta la necesidad de una gestión ética y responsable de la tecnología para proteger los derechos fundamentales.

Dado el rápido avance de la robótica y los sistemas inteligentes, es fundamental comenzar una discusión sobre la creación de una legislación específica para la inteligencia artificial. En el Perú, aún no existe una regulación al respecto, posiblemente porque estos sistemas no han generado cambios significativos en la vida cotidiana, ni en el marco legal peruano y considerando los casos internacionales mencionados anteriormente, es imprescindible plantear situaciones en las que el ser humano y un robot estén involucrados (Valero, 2021).

El autor resalta la necesidad urgente de desarrollar una legislación específica sobre inteligencia artificial, dada la velocidad con la que avanzan la robótica y los sistemas inteligentes. A pesar de que en Perú aún no se han generado cambios significativos, es fundamental anticiparse a los posibles desafíos legales que puedan surgir, como se ha evidenciado en otros países; y también una reflexión sobre la interacción entre seres humanos y robots es esencial para garantizar que el marco legal sea adecuado y proteja los derechos de las personas frente a nuevas tecnologías.

Los contratos inteligentes o ejecutables, pueden servir de ejemplo como una forma de coacción para las partes involucradas, o la responsabilidad de objetos autónomos que conlleva una responsabilidad no humana en caso de causar daños a terceros, siendo estos algunos de los paradigmas nuevos de la tecnología con IA. Por lo tanto, es esencial tratar este nuevo paradigma en el contexto del trabajo del abogado (Sánchez, 2021).

El autor señala la necesidad de que los abogados aborden los nuevos desafíos legales que surgen con la inteligencia artificial, como los contratos

inteligentes y la responsabilidad de objetos autónomos. Estos avances tecnológicos plantean cuestiones importantes sobre coacción y asignación de responsabilidades por daños, lo que requiere una adaptación del marco legal.

Los vehículos autónomos son un ejemplo de robots capaces de tomar decisiones sin la intervención de una persona. Están desarrollados para gestionar de manera independiente el control y la operación durante la conducción, lo que permite que la persona sea pasajera mientras el sistema del vehículo maneja. En este caso, es el robot el encargado de operar las funciones del automóvil. Esta autonomía plantea un debate sobre la responsabilidad y los problemas que surgirían si el sistema informático llegara a fallar (Valero, 2021).

Sánchez (2021) señala un ejemplo claro basándose en las siguientes premisas: Primero, un robot no debe causar daño a un ser humano ni permitir que, por su inacción, un ser humano sea dañado. Segundo, un robot debe seguir las órdenes dadas por los seres humanos, a menos que estas entren en conflicto con la primera ley; y tercero, un robot debe cuidar de su propia existencia, siempre que dicha protección no interfiera con la primera o segunda ley.

Los párrafos antes mencionados destacan la creciente autonomía de los robots, ejemplificada por los automóviles autónomos, que operan sin intervención humana, planteando un debate sobre la responsabilidad en caso de fallos del sistema, un aspecto crucial para el desarrollo de una regulación adecuada. Además, las leyes propuestas por Sánchez, proporcionan un marco interesante para abordar la ética de la inteligencia artificial, sugiriendo que los robots deben priorizar la seguridad humana, seguir órdenes y proteger su existencia sin poner en riesgo a las personas; estas premisas ayudan a estructurar un enfoque legal que podría ser fundamental para tratar los desafíos futuros en la interacción entre humanos y robots.

Dado que una IA no está influenciada por la subjetividad humana, es lógico y probable que pueda recibir y ser programada con información negativa, abusiva, inapropiada, indeseable e incluso ilegal, lo que podría llevarla a cometer delitos; este hecho plantea la necesidad de debatir sobre la posible responsabilidad penal de una IA (Morán, 2021). El autor resalta un desafío clave en el uso de la inteligencia artificial: su capacidad para ser programada con información perjudicial o ilegal, lo que podría llevar

a la IA a cometer delitos y manifestando la importancia de discutir la responsabilidad penal de las IA, su falta de subjetividad humana puede complicar la asignación de culpa en caso de mal uso.

A medida que la innovación tecnológica avanza, lo que es evidente es que será cada vez más difícil identificar al responsable de los daños causados en la realidad, lo que deja a la víctima en una situación de indefensión, especialmente en un sistema basado en el concepto de “culpa”. Los escenarios futuros que se plantean, como un robot cometiendo mala praxis médica, un dron matando a un niño, sistemas de IA atacando redes sociales o un “robot juez” tomando decisiones erróneas en un juicio, son solo algunos ejemplos de las complejas cuestiones de responsabilidad que podrían surgir (Morales, 2021).

Morales destaca los desafíos que plantea la rápida evolución tecnológica en cuanto a la responsabilidad por daños. Con el avance de la inteligencia artificial y la autonomía de los robots, identificar al responsable de un daño será cada vez más complicado, lo que podría dejar a las víctimas desprotegidas y con sus ejemplos mencionados subraya la necesidad urgente de establecer marcos legales claros sobre la responsabilidad de las IA y sus posibles consecuencias.

Actualmente, se discute quién debe responder cuando un sistema de inteligencia artificial genera errores o perjuicios. La dificultad para determinar responsabilidades radica en la autonomía y falta de transparencia de algunos sistemas de IA. Se han propuesto marcos normativos que distribuyen la responsabilidad entre desarrolladores y usuarios finales, con el objetivo de garantizar mayor claridad y rendición de cuentas en su aplicación dentro del ámbito jurídico (Farfán et al., 2023).

Los autores citados anteriormente resaltan un tema crucial en el contexto de la inteligencia artificial: la dificultad de asignar responsabilidad cuando los sistemas autónomos causan daños. La naturaleza opaca y autónoma de la IA complica la identificación de los responsables y la propuesta de un marco normativo que involucra tanto a los creadores como a los usuarios finales busca garantizar una mayor transparencia y rendición de cuentas, un paso importante para asegurar que la IA se utilice de manera ética y legal.

Por otro lado, la implementación efectiva del derecho puede crear desventajas que afectan principalmente a las iniciativas públicas relacionadas con

los recursos lingüísticos. En este sentido, no se puede ignorar que, en la práctica, resulta sumamente complicado para el propietario de las bases de datos y recursos demostrar que se ha violado una prohibición de minería de datos y que dicho incumplimiento le ha causado perjuicios (Cotino, 2023).

Cotino resalta una problemática importante en la aplicación del derecho en el ámbito de los recursos lingüísticos, especialmente en lo relacionado con la minería de datos. La dificultad para probar el incumplimiento de las normativas y los daños causados refleja una de las limitaciones que enfrentan tanto los propietarios de bases de datos como las autoridades encargadas de velar por el cumplimiento de las leyes.

Y para culminar Castro et al. (2021) manifiestan que la incorporación de la inteligencia artificial en el derecho penal ofrece importantes ventajas, tales como: (I) una mayor agilidad y eficiencia en la administración de justicia, (II) una mayor seguridad jurídica para la víctima en cada caso, al eliminar las influencias subjetivas humanas en la clasificación del delito, y (III) un análisis más preciso y riguroso, fundamentado en los principios legales, para tomar decisiones durante el proceso.

En otras palabras, se resaltan las ventajas fundamentales de la inteligencia artificial en el campo del derecho penal pues la IA promete transformar la administración de justicia al hacerla más ágil y eficiente, reduciendo la influencia de sesgos humanos en la tipificación de delitos y garantizando un análisis más riguroso basado en principios legales. Además, es importante reflexionar también sobre los desafíos éticos y prácticos que pueden surgir en la implementación de esta tecnología, especialmente en términos de transparencia y responsabilidad.

CONCLUSIONES

- Se alcanzó a identificar cuáles son los desafíos que plantea la IA en los términos de protección de datos y protección de la privacidad; estos desafíos vinculados a la vulneración de los datos personales, es decir que en algunos aspectos la IA no cumple con el objetivo de garantizar la protección personal de los usuarios, inclusive se puede decir que la inteligencia artificial al no ser regulada puede ser usada para cometer delitos cibernéticos y la violación de la privacidad.
- Se analizó cómo la inteligencia artificial (IA) influye en la toma de

decisiones de personas, especialmente en el ámbito legal, involucrando a abogados, jueces y magistrados; los resultados muestran que las decisiones humanas difieren de las tomadas por sistemas o plataformas automatizadas; algunos jueces ya recurren a la IA para consultar o respaldar sus veredictos, lo que sugiere que también los abogados y juristas podrían usarla en tareas como preparar alegatos, redactar escritos, artículos o incluso demandas.

- Se identificó el impacto que tiene la inteligencia artificial en la administración de justicia y en los procesos judiciales, específicamente en la toma de decisiones judiciales como por ejemplo la IA tiene impacto en algunos jueces al tomar sus veredictos al dictar una sentencia, es decir consulta con la inteligencia artificial su decisión final. Así mismo impacto o influye en el campo del derecho, no sólo en el ámbito de la realización de audiencias o procesos, sino también en la enseñanza, en la redacción de textos legales.
- Se determinó quién sería el responsable de los daños causados por los sistemas de IA, con el objetivo de determinar quién responde por infracciones como la violación de privacidad o la vulneración de datos personales. Esto no solo se aplica a plataformas digitales, sino también a casos como los automóviles con piloto automático o robots; se llegó a la conclusión de que es necesario regular la IA mediante una normativa especial que no solo establezca límites en su uso, sino que también defina las responsabilidades por los daños causados, evitando así el mal manejo y los delitos asociados a la IA.

REFERENCIAS

- Albornoz, M. M. (2021). *El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición?* <https://www.redalyc.org/articulo.oa?id=293270311010>
- Cabrera, C. T. (2024). El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial. *InDret, 1*, Article 1. <https://doi.org/10.31009/InDret.2024.i1.02>
- Castro, M. F., Sánchez, N. E., & Ortégón, L. M. (2021). Valoración de la inserción de la inteligencia artificial en el ámbito jurídico: Un análisis frente al proceso del ente acusador en etapa de indagación. *Via Inveniendi Et Iudicandi, 16*(2), Article 2. <https://doi.org/10.15332/19090528.6787>

- Cotino, L. (2023). Inteligencia artificial, tecnologías y recursos del lenguaje: Políticas y derecho para la explotación de corpus y bases de datos. *Revista de Llengua i Dret*, 61-77. <https://doi.org/10.58992/rld.i79.2023.3860>
- De Luis, E. (2023). Justicia, inteligencia artificial y derecho de defensa. *IDP. Revista de Internet, Derecho y Política*, 39, Article 39. <https://doi.org/10.7238/idp.v0i39.417164>
- Farfán, J. L., Farfán, J. A., Farfán, B., & Núñez, J. P. (2023). Inteligencia artificial y Derecho: ¿La justicia en manos de la IA? *Frónesis*, 30(2), 173-197.
- Galindo, A. C. (2019). Derechos digitales: Una aproximación a las prácticas discursivas en internet desde la etnografía virtual. *PAAKAT: revista de tecnología y sociedad*, 16, 1-18.
- Galvis, J. C., & Esquivel, L. M. (2022). Derechos y deberes en la inteligencia artificial: Dos debates inconclusos entorno a su regulación. *Nuevo Derecho*, 18(31), 1-17. <https://doi.org/10.25057/2500672X.1479>
- Juri, Y. E. (2021). Inteligencia artificial y dignidad humana: Los desafíos para el derecho. *Revista Justicia & Derecho*, 4(2), Article 2. <https://doi.org/10.32457/rjyd.v4i2.1350>
- Krenz, R. C. (2021). ¿Jueces robots? Inteligencia artificial y derecho. *Revista Justicia & Derecho*, 4(2), Article 2. <https://doi.org/10.32457/rjyd.v4i2.1345>
- Mendoza, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *REVISTA IUS*, 15(48). <https://doi.org/10.35487/rius.v15i48.2021.743>
- Morales, A. (2021). El impacto de la inteligencia artificial en el Derecho. *Advocatus*, 039, Article 039. <https://doi.org/10.26439/advocatus2021.n39.5117>
- Morán, A. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *REVISTA IUS*, 15(48), Article 48. <https://doi.org/10.35487/rius.v15i48.2021.706>
- Navas, O. (2021). En el umbral de una nueva era: El derecho privado ante la robótica y la inteligencia artificial. *Revista Facultad de Jurisprudencia*, 9, 178-219.

- Ordellin, J. L. F. (2021). *El uso de la inteligencia artificial en la mediación: ¿quimera o realidad?* <https://www.redalyc.org/articulo.oa?id=293270311016>
- Ortega, C. (2023). Sobre los diferentes ritmos del derecho y la Inteligencia Artificial. La desincronización como patología social: *Daimon Revista Internacional de Filosofía*, 90, Article 90. <https://doi.org/10.6018/daimon.551741>
- Osorio, F. (2022). Inteligencia artificial y derecho de autor: Un estudio sobre la regulación británica. *Revista Justicia & Derecho*, 5(1), Article 1. <https://doi.org/10.32457/rjyd.v5i1.1833>
- Parra, D., & Concha, R. (2021). Inteligencia artificial y derecho. Problemas, desafíos y oportunidades. *Vniversitas*, 70, 1-25. <https://doi.org/10.11144/Javeriana.vj70.iadp>
- Quezada, G. A., Castro, M. del P., & Quezada, M. del P. (2022). Inteligencia artificial y enseñanza del derecho: Su incorporación durante la pandemia de la Covid-19. *Revista Venezolana de Gerencia*, 27(8), Article 8. <https://doi.org/10.52080/rvgluz.27.8.2>
- Sánchez, J. F. (2016). El Derecho constitucional ante la era de Ultrón: La informática y la inteligencia artificial como objeto constitucional. *Estudios de Deusto*, 64(2), Article 2. [https://doi.org/10.18543/ed-64\(2\)-2016pp225-258](https://doi.org/10.18543/ed-64(2)-2016pp225-258)
- Sánchez, M. F. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, 10(1), Article 1. <https://doi.org/10.14409/redoeda.v10i1.12626>
- Sánchez, P. J., & Zegarra, L. J. (2022). Necesidad de regulación de la inteligencia artificial en la responsabilidad civil extracontractual en el Perú, 2021. *Repositorio Institucional - UTP*. <http://repositorio.utp.edu.pe/handle/20.500.12867/6643>
- Sánchez, S. (2021). Ciencia Ficción como Fuente de Principios Jurídicos para regular la Inteligencia Artificial. *REVISTA IUS*, 15(48), Article 48. <https://doi.org/10.35487/rius.v15i48.2021.690>
- Suárez, W. Y., De León, G. I., & Monsalve, J. J. (2023). Un análisis sobre la aplicabilidad de la inteligencia artificial en el derecho colombiano. *Prolegómenos. Derechos y Valores*, XXVI(52), 11-23.

- Toache, E. A., & Rosales, M. A. (2023). Preocupaciones éticas en el uso de inteligencia artificial, transparencia y derecho de acceso a la información. El caso de los chatbots en el gobierno de México, en el contexto de la COVID-19. *Estudios en Derecho a la Información*, 85-111. <https://doi.org/10.22201/ijj.25940082e.2023.15.17472>
- Valero, C. D. Q. (2021). Derecho e Inteligencia Artificial en el mundo de hoy: Escenarios internacionales y los desafíos que representan para el Perú. *THEMIS Revista de Derecho*, 79, 311-322. <https://doi.org/10.18800/themis.202101.017>
- Vercelli, A. (2024). Regulaciones e inteligencias artificiales en Argentina: *InMediaciones de la Comunicación*, 19(1), Article 1. <https://doi.org/10.18861/ic.2024.19.1.3549>
- Villareal, C. P. (2023). La Justicia en Tiempos de Inteligencia Artificial. *Ciencia Latina Revista Científica Multidisciplinar*, 7(5), Article 5. https://doi.org/10.37811/cl_rcm.v7i5.8517
- Villasmil, J. J., Berrocal, J. C., & Rodelo, M. R. (2024). Inteligencia artificial y nuevas formas de derecho en el siglo XXI. *Revista de Ciencias Sociales*, 30, 447-458. <https://doi.org/10.31876/rcs.v30i.42324>
- Zabala, T. D. (2021). La ética en inteligencia artificial desde la perspectiva del derecho. *Via Inveniendi Et Iudicandi*, 16(2). <https://doi.org/10.15332/19090528.6785>

TELETRABAJO POST PANDEMIA Y SUS IMPLICANCIAS EN EL SECTOR LABORAL INTERNACIONAL

Hubert J. Fernández-Arroyo¹

RESUMEN

Esta investigación tuvo por objetivo describir el impacto del teletrabajo impuesto por la pandemia COVID-19 en la salud mental y emocional de los trabajadores, para ello se utilizó una metodología de investigación de tipo básica y el diseño de investigación, no experimental y descriptivo, asimismo se realizó una revisión bibliográfica de 30 artículos científicos extraídos de bases de datos como Scopus, Dialnet, Redalyc y SciELO, que permitió analizar la problemática de manera integral. Los resultados desarrollados fueron: el surgimiento del teletrabajo a raíz de la pandemia Covid-19, los beneficios del teletrabajo tanto en la vida familiar como laboral, las principales barreras que limitan el acceso al teletrabajo y la adaptación de los trabajadores con respecto al teletrabajo. Concluyendo que, el teletrabajo, acelerado por la pandemia de COVID-19, se ha consolidado como una herramienta clave para transformar las relaciones laborales hacia un modelo más flexible, inclusivo y sostenible, asimismo, entre sus principales beneficios destacan la flexibilidad de horarios, la reducción de costos y la inclusión laboral, aunque su implementación ha enfrentado barreras como la falta de conectividad, la resistencia al cambio y la preparación insuficiente de las organizaciones, no obstante, a pesar de los desafíos, su capacidad para equilibrar las necesidades tanto personales como laborales lo posiciona como una práctica esencial para el futuro, siempre que se acompañe de inversión en recursos tecnológicos, capacitación y liderazgo adaptativo.

Palabras clave: Teletrabajo, tecnología, beneficios, trabajadores

¹ hfernandez1@upao.edu.pe

Programa de Estudio de Derecho, Universidad Privada Antenor Orrego

ABSTRACT

This research aimed to describe the impact of telework imposed by the COVID-19 pandemic on workers' mental and emotional health. To achieve this, a basic research methodology and a non-experimental, descriptive research design were used. Additionally, a bibliographic review of 30 scientific articles extracted from databases such as Scopus, Dialnet, Redalyc, and SciELO was conducted, allowing for a comprehensive analysis of the issue. The results included the emergence of telework due to the COVID-19 pandemic, the benefits of telework in both family and professional life, the main barriers limiting access to telework, and workers' adaptation to telework. In conclusion, telework, accelerated by the COVID-19 pandemic, has established itself as a key tool for transforming labor relations into a more flexible, inclusive, and sustainable model. Among its main benefits are flexible schedules, cost reduction, and labor inclusion. However, its implementation has faced challenges such as limited connectivity, resistance to change, and insufficient organizational preparedness. Nonetheless, despite these challenges, its ability to balance both personal and professional needs positions telework as an essential practice for the future, provided it is supported by investments in technological resources, training, and adaptive leadership.

Keywords: Teleworking, technology, benefits, workers

INTRODUCCIÓN

Durante la pandemia Covid-19, se tuvo cierta incertidumbre entre las personas que prestaban sus servicios tanto intelectuales como físicos dentro de una empresa; esto conllevó a que la preocupación se hiciera más extensiva dentro del hogar familiar, debido a que no solamente no podían solventar sus lugares de residencia como en el día a día lo hacían, sino que también generaba una preocupación por el incremento de la tasa de decesos que existían en aquel momento.

En este contexto, es relevante destacar las cifras de fallecimientos recopiladas por la Universidad Johns Hopkins, que evidenciaron el impacto global de la pandemia; entre los países más afectados se encontraron Estados Unidos, con 20,614 muertes; Italia, con 19,468; España, con 163,027; Francia, con 13,832; el Reino Unido, con 9,875; y China, con 3,343 víctimas mortales (Maguiña *et al.*, 2020).

Correlacionado con la tasa de decesos presentada en el párrafo precedente, tampoco se pudo dejar de tener en cuenta que la estabilidad emocional jugaría un papel fundamental, puesto que ésta iba decreciendo en la vida cotidiana de las personas, resultante de las implicancias que se suscitaban por no tener trabajo durante la pandemia Covid-19.

En ese marco, Bonilla *et al.* (2014) señalaron una nueva forma que los estados implementaron a raíz de la pandemia a causa del SARS-Cov-2, la cual fue el teletrabajo y se planteó como una forma de realizar actividades, que posteriormente se caracterizaría por la separación física entre el empleado y el lugar de trabajo principal.

En ese sentido, Kniffin *et al.* (2021, citados por Yeves *et al.*, 2023) refirieron que se habría observado un deterioro en las condiciones laborales a causa de la pandemia Covid-19, lo cual trajo como consecuencia mayor riesgo de experimentar un estado de agotamiento físico, emocional y mental, debido al estrés laboral que generaba no encontrar un empleo; esto mostró que dicho fenómeno mundial no solo trajo consigo muerte de la manera en la que se conoce, sino también una especie de muerte mental subjetiva.

Según Camacho (2021) consideró que el teletrabajo se transformó en la principal alternativa para reducir los efectos del coronavirus, tanto en la sociedad como en el ámbito empresarial esto era considerado un beneficio; sin embargo, se volvió una necesidad a causa de la problemática mencionada. Además el autor destaca que, debido a las circunstancias derivadas de la pandemia y con el fin de proteger tanto la economía como la salud mental de quienes trabajaban presencialmente, se consiguió implementar una solución efectiva a este problema social: la modalidad virtual de trabajo.

De esta manera, Osio (2010) hace mención que una tecnología como la que se presentó '*virtualidad de teletrabajar*' permitiría mayor comunicación, movilidad, aumento de productividad, así como de libertad a la hora de trabajar y relacionarse, es decir, que donde muchos veían desconocimiento y vaguedad, otros lo usaron como recurso para solucionar un problema en grave ascenso.

Más allá de la adaptación social en general a esta nueva idea de trabajo, la cual no convencía a muchos, existen datos en los que se puede dar a conocer que no existía una práctica longitudinal por parte de las personas, es decir, que la gran mayoría se encontraba adaptada a un medio de trabajo que perduró a lo largo de los años, y este fue el que se daba de manera presencial en un centro de labores.

En ese sentido, la Comisión Económica para América Latina y el Caribe (2020, como se citó por Benavides & Silva-Peñaherrera, 2022) señaló que solo el 21,3% de las personas empleadas tenían la posibilidad de realizar el teletrabajo cuando comenzó la pandemia de COVID-19. Este porcentaje

variaría entre las diversas actividades practicadas por los trabajadores habituales; de esta manera se indicaría que la mayoría de la población no estaba preparada para enfrentar un cambio de tal magnitud, lo que resultó en la pérdida de empleo para muchas personas.

Para reforzar la idea anterior, Andrade (2022) refirió que el teletrabajo con su avanzada tecnología y sistemas inteligentes, transformó radicalmente el mundo laboral convirtiéndose en una herramienta clave del poder; sin embargo, según los datos analizados precedentemente, se observó que si bien la tecnología avanzó grandes pasos; por otro lado, dejó sin empleo a diversas masas de trabajadores los cuales eran el sustento de sus hogares.

Por otro lado, se pudieron observar ciertos beneficios, hasta inclusive comodidades que los trabajadores no tenían cuando laboraban de manera presencial en sus entidades a las cuales les prestaban sus servicios, sin embargo, no se puede dejar de mencionar ciertas implicancias que se suscitaron en el transcurso de la nueva adaptación por parte de los empleados.

Entre las ventajas identificadas destacan la flexibilidad en los horarios y la eliminación de los desplazamientos diarios, lo que permitió a los trabajadores gestionar mejor su tiempo y experimentar un aumento en su satisfacción general. En este contexto, Pérez & Gálvez (2009) señalaron que el teletrabajo llegó a ser una opción eficaz para armonizar las esferas laboral, familiar y personal, lo que resultó factible para mantener un equilibrio entre el trabajo y la vida familiar sin que ninguno de estos aspectos se vea comprometido.

Para poder equilibrar dichos problemas, tanto las empresas como los trabajadores deberían aplicar estrategias que logren optimizar el teletrabajo; además, sería fundamental que las organizaciones desarrollen políticas claras que establezcan límites para evitar la sobrecarga laboral. Asimismo, se debe invertir en herramientas, así como recursos que faciliten la comunicación y la colaboración a distancia, de este modo se podrá obtener una mayor productividad al momento de desarrollar ciertas actividades en las jornadas laborales.

En ese sentido, la investigación persigue cuatro objetivos; en primer lugar, definir el surgimiento del teletrabajo a raíz de la pandemia Covid-19, identificando su origen y sus características; en segundo lugar, detallar los beneficios de este, tanto en la vida familiar como laboral; en tercer

lugar, estudiar las principales barreras de acceso que limitan el teletrabajo; y finalmente, examinar la adaptación de los trabajadores a este nuevo sistema.

El artículo ofrece un enfoque integral sobre el teletrabajo, presentándose como una herramienta transformadora surgida a raíz de la pandemia de COVID-19, un fenómeno social que marcó un hito en el ámbito laboral. En esa línea, este avance, si bien representa una innovación significativa, también conlleva implicancias importantes, como la necesidad de adaptación por parte de los trabajadores a un sistema laboral completamente nuevo.

METODOLOGÍA

Esta investigación tuvo relevancia en base a un enfoque cualitativo con el fin de lograr un acercamiento al tema del Teletrabajo post pandemia Covid-19 y sus implicancias que tuvo respecto a la adaptación de los trabajadores a un nuevo sistema laboral, quienes se encontraban en un sistema de labores aparentemente estable relacionado a la presencialidad.

El estudio realizado fue de naturaleza básica, lo que significa que su objetivo principal fue recopilar información o desarrollar una teoría; este tipo de investigación no busca resolver problemas urgentes, sino ampliar el cuerpo de conocimientos de una disciplina. En ese sentido, se puede entender que se emplea el conocimiento ya existente, sin generar uno nuevo (Rodríguez & Pérez, 2007).

Por otro lado, el diseño de investigación fue no experimental – descriptivo, en donde no se manipulan variables, sin embargo, los fenómenos se observan de manera natural para posteriormente analizarlos, esto quiere decir, que este diseño permitirá estudiar situaciones en su estado natural, o que ya ocurrieron (Hernández-Sampieri y Mendoza, 2018).

La técnica se limitó a una revisión bibliográfica de 30 artículos científicos de las bases de datos: Redalyc, Scopus, SciELO y Dialnet, las cuales permitieron realizar tanto una búsqueda, como recopilación informativa del Teletrabajo post pandemia de manera general, asimismo, la investigación se desarrolló entre abril y noviembre de 2024, y a su vez, se emplearon fichas bibliográficas seleccionadas en un Excel, en la cual se registraron datos clave como el año de publicación, revista, autores, país de origen, objetivos y conclusiones, de manera que la revisión bibliográfica sirvió

para resumir el conocimiento plasmado por otros autores (Fernández, 2009, citado en Fernández & Peral, 2011).

Por último, se analizó la información relacionada con el teletrabajo desde la perspectiva de la adaptación de los trabajadores, donde muchos de ellos no lograron ajustarse a este nuevo ritmo laboral debido a diversas barreras que dificultan su integración en este sistema, como el acceso limitado a una conexión de internet (Domínguez, 2020, citado en Ramírez *et al.*, 2021).

En tal sentido, el esquema temático de la investigación abordó el teletrabajo desde cuatro aspectos clave: Primero, se definió el surgimiento del teletrabajo a raíz de la pandemia Covid-19, identificando su origen y sus características; segundo, se detalló los beneficios del teletrabajo, tanto en la vida familiar como laboral; tercero, se estudió sobre las principales barreras de acceso que limitan el teletrabajo; y finalmente, se examinó la adaptación de los trabajadores a este nuevo sistema.

RESULTADOS

1. Surgimiento del teletrabajo a raíz de la pandemia Covid-19

Al aunar en el tema del teletrabajo, se tiene que tener en cuenta un punto de partida, el cual fue la Revolución Industrial, en donde se creó un nuevo tipo de trabajadores especializados que dependían de forma directa o indirecta de su centro de labores (fábrica) en el cual tenían que mantenerse al cuidado del funcionamiento de la maquinaria (Tunal, 2012).

En ese sentido, se puede afirmar que el teletrabajo antiguamente era una opción prácticamente nula en la vida de los trabajadores; sin embargo, con el pasar de los años se convirtió en una forma flexible de organización laboral que le permitió al trabajador realizar sus funciones profesionales sin la necesidad de encontrarse físicamente en las instalaciones de la empresa (Civit y March, 2000, como se citó en Rodríguez, 2007).

Ahora bien, según lo manifestado por Dorrance (2020, como se citó en Araujo-Robles *et al.*, 2021) durante la Covid-19, que se presentó a gran escala, topándose con todos y cada uno de los países, produjo efectos económicos y sociales, entre ellos, la pérdida de trabajos o recientes emprendimientos realizados por las personas que anhelaban un puesto laboral.

Para enfatizar la idea anterior, los problemas sociales generados durante la pandemia trajeron consigo consecuencias emocionales significativas debido al confinamiento, en donde las familias experimentaron molestia, frustración y diversas preocupaciones, como la incertidumbre sobre su subsistencia. Además, la transición del trabajo presencial al teletrabajo, a raíz del COVID-19, fue otro factor que impactó a muchas personas emocionalmente (Broche-Pérez *et al.*, 2020).

En el momento que surge el teletrabajo, este se presenta como una herramienta favorable para los trabajadores, surgiendo más como una alternativa de flexibilización, lo cual permitió ejercer la producción de las actividades desde el hogar del empleado sin dejar de faltar al trabajo en el cual fue contratado (Nilles, 2012, citado en García-Rubio *et al.*, 2021).

Al hablar de “herramienta favorable” el autor lo toma como una solución flexible que permitió a los empleados continuar con sus labores desde casa sin incumplir con sus obligaciones, de esta manera se resalta que el teletrabajo emergió como una manera de flexibilizar las relaciones laborales, brindando a los trabajadores la posibilidad de desempeñar sus tareas sin la necesidad de estar presente en la empresa por circunstancias adversas como la pandemia.

Por otro lado, al hacerse la gran pregunta de ¿Se otorgaron los mismos beneficios a los empleados? García-Rubio *et al.* (2021) refirieron que si bien es cierto, sí se le otorgaron los mismos beneficios y las mismas garantías a los trabajadores, éstos también tuvieron las mismas obligaciones a las que se suscribieron al trabajar de manera presencial.

Haciendo énfasis al párrafo precedente, el autor manifestó que sin importar cuán nueva fuera la nueva modalidad de trabajo, la cual surgió como consecuencia del Covid-19, esta, no afectó en los beneficios (seguro social, recepción de cursos de capacitación, etc) que pudieran tener los empleados de la empresa, sin embargo, y lógicamente tendrían que cumplir con sus actividades laborales asignadas en el trabajo regular demostrando así su competitividad.

Cuando se refiere la competitividad y producción dentro del teletrabajo, se ha demostrado mediante un estudio en México que éste presenta una gran viabilidad por las ventajas que le ofrecen a la empresa (Graizbord, 2015, citado por Guzmán & Abreo, 2017). De esta manera quedó demostrado que la nueva modalidad de trabajo significó un gran avance a nivel empresarial, siendo factor clave la flexibilidad del teletrabajador.

Los autores señalaron que el teletrabajo demostró ser beneficioso para las empresas; puesto que, a través de un estudio, se habría evidenciado que esta modalidad de laborar llegó a ofrecer ventajas significativas, como la mejora en la competitividad y la producción. Un aspecto importante que se mencionó también fue la flexibilidad, la cual permitió a los teletrabajadores consolidar su vida personal junto con la laboral.

Continuando con la idea, se vio reflejado que el teletrabajo resultó ser ventajoso tanto para los empleados como para las empresas al generar un entorno más eficiente y rentable, puesto que cuando se ve bien empleada una nueva tecnología se logra satisfacer las necesidades del empleado y del empleador referentes a prestar un servicio, siendo esta una herramienta útil en el futuro.

Según Álvarez (2020) afirmó que además de los beneficios y el surgimiento mencionado, parece ser que el teletrabajo, ya sea bajo la normativa que se encuentre presente o con una regulación más avanzada a futuro está destinado a crecer significativamente, implementándose como una mejor herramienta laboral.

En ese sentido, y de acuerdo a las ideas planteadas en el capítulo, el teletrabajo logró surgir como respuesta a la pandemia Covid-19, en donde muchos trabajadores no podían asistir a su centro de labores, de esta manera se tiene que tomar en cuenta que ésta fue una herramienta favorable tanto para las empresas como para sus empleados, solucionando así la problemática de no trabajar debido a causas subyacentes como la referida pandemia.

2. Beneficios del teletrabajo tanto en la vida familiar como laboral

A raíz del Covid-19, el teletrabajo demostró ser una alternativa efectiva que benefició tanto a los empleados como a las empresas; en el ámbito familiar, una de las principales ventajas fue la flexibilidad de horarios, lo que permitió a las personas disfrutar más tiempo con sus seres queridos.

En ese sentido, Pérez & Gálvez (2009) señalaron que el teletrabajo es una herramienta útil para promover la conciliación, puesto que ayuda a resolver dos grandes obstáculos: la gestión del tiempo y la distancia; al permitir que el trabajo se realice desde cualquier lugar y de forma más ágil, reducen el tiempo dedicado a las tareas laborales, lo que liberó el dedicar más tiempo a otras áreas de la vida, como la familia y el autocuidado.

Los autores dan a conocer que el teletrabajo logró ser un recurso clave para mejorar la estabilidad entre la vida laboral y personal, esto se debe a que permitió superar dos problemas importantes: el tiempo y la distancia, de esta manera se pudo posibilitar que las personas puedan trabajar desde cualquier lugar y de manera más eficiente sin descuidar el ámbito familiar.

Desde que el teletrabajo se implementó a nivel global, logró ganar una creciente aceptación, y cada vez más empresas adoptan esta modalidad; esto se debe, en parte, a los beneficios que ofrece a las organizaciones, como la reducción de costos en infraestructura, tecnología y otros servicios (Sánchez *et al.*, 2019 como se citó en Arce & Rojas, 2020)

Los autores refieren que, desde que el teletrabajo comenzó a implementarse en todo el mundo a raíz de la pandemia Covid-19, éste, habría sido cada vez más aceptado por las empresas, esto se debe a que ofrece importantes beneficios para las mismas, como la reducción de costos asociados a mantener oficinas físicas, equipos tecnológicos y servicios necesarios para el trabajo presencial.

Entre los numerosos beneficios del teletrabajo, Vargas & Osma (2013) consideraron entre ellos, la posibilidad de implementar diversas maneras de organizar y gestionar las empresas, lo que conduciría la disminución de los costos, la mejora en el uso de los recursos y la difusión de información, generando un intercambio de conocimiento.

En ese sentido, lo que se quiere dar a conocer es cómo estas nuevas formas de gestión permitieron un uso más eficiente de los recursos, es decir, las empresas lograron aprovechar mejor lo que tenían a su disposición, como el tiempo, el dinero y el personal, los cuales terminaron siendo teletrabajadores, logrando así un aumento en la productividad y una menor inversión en locales para las empresas.

Otro beneficio que surgió a raíz del teletrabajo fue la inserción al mercado laboral de personas con habilidades diferentes, mal llamados “*discapacitados*”, en donde se les pudo brindar la oportunidad de acceder a empleos que, de otro modo, pudieron ser difíciles de conseguir por sus propias condiciones (Fantini, 2013).

Haciendo alusión a la idea precedente que señaló el autor; la inclusión de personas con habilidades diferentes en el mercado laboral, facilitada por el teletrabajo, representó un avance significativo hacia la igualdad de oportunidades, puesto que estas personas eran consideradas incapaces de desempeñarse en un puesto de trabajo.

Un beneficio que trajo consigo la implementación del teletrabajo, también fue el acceso y la creación de nuevas oportunidades laborales, las cuales lograron abrir un espacio a nuevos puestos de trabajo; esto es, para personas que probablemente se encontraban desempleadas en tiempos de pandemia (Arévalo, 2024).

De esta manera, al permitir que las empresas adaptaran sus operaciones a un modelo remoto, se lograron generar nuevas oportunidades laborales que anteriormente eran escasas, especialmente para aquellos que se encontraban desempleados debido a la pandemia.

Según lo manifiesta Carrasco-Mullins (2021, citado en De Mello, 2024) los únicos que obtendrían beneficios respecto al teletrabajo no solo serían los empleados, sino también la institución que los acogió, puesto que si ésta les brinda a los trabajadores una mejor calidad de vida, tendrían como resultado una mejor productividad, compromiso, así como fidelidad hacia la empresa.

Lo resaltante de esta idea es que el teletrabajo genera un círculo virtuoso entre trabajador y contratante; dado que al contribuir con una mejor calidad de vida para los empleados, la empresa no solo fomenta un ambiente laboral más saludable, sino que también obtiene beneficios directos en términos de rendimiento.

Un beneficio muy resaltante del teletrabajo es permitirle al trabajador desempeñarse a su propio ritmo, claro está, sin disminuir la productividad que le ofrece a la empresa; de esta manera se resalta la flexibilidad que tiene el empleado para poder equilibrar su vida laboral con la familiar; cosa que no sucedía en un puesto presencial (Pérez 2010, citado en Tapasco-Alzate & Giraldo-García, 2020).

En ese orden de ideas, esta flexibilidad permite al trabajador organizar mejor su tiempo, adaptando su jornada laboral a sus necesidades personales, lo cual es especialmente beneficioso para quienes tienen responsabilidades familiares, empero, esto no significa que estos descuiden sus labores como teletrabajadores.

De esta manera, el teletrabajo probó ser una modalidad beneficiosa tanto para los empleados como para las empresas al ofrecer mayor flexibilidad para equilibrar la vida personal y laboral, promoviendo así un entorno en el que los trabajadores pudieran gestionar su tiempo de manera más eficiente aumentando su productividad.

Además, el teletrabajo ha impulsado la inclusión laboral al abrir oportunidades para personas con habilidades diferentes y para quienes se encontraban desempleados durante la pandemia; este modelo también fomentó la innovación en la gestión empresarial, permitiendo a las organizaciones adaptarse a nuevas formas de operar, mejorando su competitividad y fortaleciendo la relación con sus trabajadores. En esencia, el teletrabajo no sólo redefinió el concepto de empleo, sino que logró establecer un paradigma más equitativo y eficiente, alineado con las necesidades de la sociedad y el mercado laboral.

3. Principales barreras que limitan el acceso al teletrabajo

Un aspecto clave que marcó el desarrollo del teletrabajo, fue la existencia de diversas barreras que dificultan su implementación, entre estas se encontraron las limitaciones tecnológicas, especialmente en regiones con infraestructuras digitales deficientes, impidiendo el acceso a una conectividad adecuada por parte de los trabajadores.

Enfatizando el párrafo que precede, Ramírez *et al.* (2021) mencionaron que a pesar de existir cierta evolución en algunos estados respecto al teletrabajo, aún se encuentran barreras en la implementación de este mismo, tales como el efectivo acceso a la conectividad o internet especialmente en regiones rurales o en desarrollo, donde la infraestructura tecnológica sigue siendo deficiente.

Por su parte, Steimberg & Mañas (2008, citado por Agudo, 2014) refirieron que otra de las barreras que afectó el desarrollo del teletrabajo, fue la falta de confianza por parte de los directivos al momento de invertir en la formación e implementación de nuevas herramientas telemáticas para los trabajadores, puesto que no se sabía a ciencia cierta si estos podrían conciliar tanto su vida profesional como familiar.

El autor señaló que una de las barreras más significativas para el progreso del teletrabajo fue la falta de confianza de los directivos, puesto que al invertir en nuevas herramientas y una plena capacitación, éstos, temían que dicha inversión no se vea compensada con su productividad debido a las implicancias familiares que existieran.

Por otro lado, y es de verse que no es un problema ajeno a alguna sociedad que la falta de economía y educación fueron parte de las barreras que tuvo el teletrabajo, puesto que constituyó en causa para que las personas que no contaban con estos beneficios no pudieran acceder a un trabajo de esta modalidad (Aristizábal *et al.*, 2022).

En ese sentido, la falta de recursos económicos y educación fueron una de las barreras que impidieron el desarrollo del teletrabajo; esta situación afectó especialmente a las personas que no contaban con los mencionados beneficios, limitando de esta manera su acceso a la nueva modalidad de trabajo y por lo tanto generando desempleo.

Por otro lado, se evidenció la falta de oportunidades laborales para las mujeres, posiblemente debido a una discriminación de género por parte de los empleadores, esto generó una barrera ideológica basada en la creencia de que las mujeres no eran capaces de equilibrar su vida laboral y familiar.

Según Rodríguez (2009, citado por Osio & Delgado, 2010) señaló que las mujeres han enfrentado múltiples obstáculos, como barreras económicas, culturales, formativas y sociales, que han dificultado su acceso al uso de tecnologías como el teletrabajo, impidiéndoles aprovechar completamente las oportunidades que estas herramientas brindan.

Según lo manifestado por Valle (2018) consideró que otra de las barreras que limitó el avance del teletrabajo fue particularmente la resistencia al cambio de esta modalidad, puesto que los empleados tenían un conocimiento insuficiente respecto a aquellas posibilidades que se ofrecían.

De la idea plasmada en el párrafo anterior, el autor destacó que una barrera limitativa para el avance del teletrabajo fue la negativa de algunos empleados a aceptar cambios; esta resistencia surgió, en parte, por el conocimiento limitado que los trabajadores tenían sobre una nueva modalidad laboral, además, muchos de ellos habían sido formados en una cultura tradicional de trabajo, ajena a la era digital, lo que agravó el problema y dificulta la adaptación al entorno telemático.

Dentro de las implicancias que presenta el teletrabajo, se encuentran también las denominadas barreras estructurales, las cuales dificultan el acceso y la participación equitativa de personas con habilidades diferentes a puestos laborales, debido a las normas sociales o políticas, que se encuentran profundamente arraigadas en la estructura de una sociedad.

Según un estudio realizado por el Banco Interamericano de Desarrollo (2020, citado por Roncal, 2021) el teletrabajo presentó múltiples ventajas, pero también generó que se creara una barrera estructural respecto a las personas que presentaban habilidades diferentes, las cuales no fueron tomadas en cuenta por la sociedad empresarial.

De las ideas planteadas anteriormente, se pudo considerar que las principales barreras que limitaron el acceso al teletrabajo abarcaron desde problemas tecnológicos, como la falta de conectividad en regiones rurales, hasta obstáculos culturales y económicos. Asimismo, la resistencia al cambio por parte de trabajadores y directivos, junto con la falta de inversión en formación y herramientas digitales, también contribuyó a dificultar la implementación efectiva del teletrabajo.

Por otro lado, las barreras estructurales han afectado de manera significativa a ciertos grupos, como las personas con habilidades diferentes y las mujeres, estas limitaciones profundamente arraigadas en la cultura y políticas laborales, restringieron su participación equitativa en la nueva modalidad laboral.

En ese contexto y a pesar de los avances que surgieron en el ámbito laboral, persisten dificultades que evidencian la necesidad de un enfoque más inclusivo, que contemple las necesidades específicas de estos grupos y rompa con las barreras ideológicas y estructurales que aún impiden un acceso pleno y justo al trabajo remoto.

4. Adaptación de los trabajadores al teletrabajo

Este punto significó uno de los desafíos más importantes en la transición hacia esta modalidad laboral; con la rápida implementación del trabajo en casa, especialmente tras la pandemia de Covid-19, muchos empleados tuvieron que ajustar sus rutinas y aprender nuevas habilidades para desempeñar sus tareas de manera eficiente fuera de las oficinas tradicionales.

Entendido ya el punto de partida, Benavides & Silva-Peñaherrera (2022) refirieron que la adaptación de los trabajadores es asemejada a la Revolución Industrial que data desde hace más de 300 años y que el teletrabajo tan solo sería una nueva forma que llegó para organizar el mundo laboral frente a profundos cambios sociales como el Covid-19.

De esta manera, el autor compara la adaptación de los trabajadores al teletrabajo con los grandes cambios que trajo la Revolución Industrial, sugiriendo que el teletrabajo es simplemente una nueva modalidad que surgió para reorganizar el mundo laboral frente a transformaciones sociales significativas, lo que implicaría una evolución en la manera en que se entiende y se realiza el trabajo en respuesta a estos cambios.

En otro ámbito de la adaptación laboral, Aragüez-Valenzuela (2019, citado por Romero-Padilla *et al.*, 2022) mencionó que el referido término, trajo

como consecuencia un nuevo fenómeno denominado “*tecnoestrés*” el cual tiene como significado al estrés específico derivado de la introducción y uso de las nuevas tecnologías en el trabajo.

Continuando con la idea de la autora, esta manifestó que una de las causas generadoras del tecnoestrés, sería la incertidumbre tecnológica, la cual generaría sentimientos de obsolescencia, frustración y ansiedad ante la insuficiente adaptación a los avances tecnológicos constantes, presentándose así una adaptabilidad insuficiente por parte de los trabajadores.

Por su parte, Contreras & Rozo (2015) refirieron que el teletrabajo no sirvió ni sirve para todas las compañías, puesto que algunos de sus trabajadores no se encontraron aptos para el cambio, siendo que el estilo de liderazgo dentro de un ambiente laboral remoto, no sería el mismo que uno que se practique de manera presencial.

Dentro de lo más destacado de manera antecedente se encontraría que el estilo de liderazgo es y fue diferente, lo que generó dificultades en la gestión y supervisión del equipo, esto implicó que en algunos casos, las dinámicas laborales y la adaptación de los empleados no fue suficiente para hacer que el teletrabajo funcione de manera efectiva en todas las organizaciones.

Según lo refiere Pulakos (2000, citado por Ortiz *et al.*, 2024) refirió que la capacidad de emprender acciones efectivas en el momento adecuado, responder de manera ágil a eventos imprevistos y ajustar los planes de acción según sea necesario está relacionada con la adaptabilidad; quedando esto demostrado con la pandemia Covid-19.

Partiendo de esa idea, el fenómeno mundial generó un proceso de adaptación en el que tanto empleados como empleadores experimentaron nuevas emociones, lo cual afectó su desempeño en el trabajo, es decir, que ante nuevas situaciones es complicado, más no imposible reaccionar frente a ellas, sin embargo si trae como consecuencia un desempeño normal de funciones laborales.

Como lo manifestó Silva (2017, citado en Chávez & Mendoza, 2024) las organizaciones, al implementar el teletrabajo, buscaron proporcionar un valor adicional a sus empleados, puesto que esta modalidad facilitó el equilibrio entre la vida laboral y personal; no obstante, a pesar de sus ventajas, las investigaciones sobre la adaptación al teletrabajo continúan

siendo limitadas, puesto que aún los trabajadores se encuentran en un cambio.

Este enfoque se ha visto como una manera de mejorar la calidad de vida de los trabajadores, permitiéndoles flexibilidad en su jornada laboral, sin embargo, a pesar de estas ventajas, la investigación sobre cómo los empleados logran adaptarse al teletrabajo sigue siendo escasa, esto implica que aunque la práctica del teletrabajo se expandió, aún se carece de un entendimiento profundo sobre cómo se lleva a cabo con éxito y los factores clave que facilitan o dificultan esa adaptación.

En un estudio realizado por Fernández (2023) se evidenció que, al investigar sobre la adaptación al teletrabajo, algunos empresarios no estuvieron preparados para hacer frente a la transición de la modalidad presencial a la virtual. En ese sentido, si el empleador no se encontraba preparado para adaptarse a algo nuevo, el empleado, quien sería su subordinado tampoco lo estaría.

De esta manera, se da a conocer que la capacidad de los empleados para adaptarse al teletrabajo está estrechamente ligada a la preparación de sus empleadores, si las empresas no invierten con las herramientas, la capacitación y los procesos necesarios para el teletrabajo, sus empleados tendrán más dificultades para ser más productivos dentro la empresa.

De acuerdo a las ideas planteadas, el teletrabajo ha revelado una compleja interacción de factores tecnológicos, organizacionales y personales, si bien esta modalidad laboral ofrece beneficios como la flexibilidad y la conciliación en la vida familiar, su implementación ha puesto de manifiesto la necesidad de un enfoque que considere tanto las necesidades de los empleados como las de las organizaciones.

Los estudios consultados evidenciaron que la adaptación al teletrabajo no fue un proceso lineal ni sencillo; factores como el tecnoestrés, la incertidumbre tecnológica y las diferencias en los estilos de liderazgo han sido obstáculos significativos. Asimismo, la preparación de las organizaciones resultó crucial, puesto que la falta de herramientas, capacitación y procesos adecuados dificultó la adaptación de los empleados a un nuevo sistema laboral.

CONCLUSIONES

- Se definió el surgimiento del teletrabajo a raíz de la pandemia Covid-19, partiendo desde la Revolución Industrial, hasta la presente época, de igual manera, este nuevo medio demostró ser una herramienta versátil con proyección a futuro, puesto que permitió un equilibrio entre las necesidades personales y laborales de los empleados, consolidando su implementación como una práctica clave para el desarrollo empresarial, al integrar avances tecnológicos y estrategias adaptativas, representando un paso importante hacia una nueva era de relaciones laborales más dinámicas, inclusivas y sostenibles.
- Se detalló los beneficios del teletrabajo, dentro de los cuales, los principales serían: la flexibilidad de horarios, que permitió a los empleados equilibrar su vida laboral y familiar al gestionar mejor su tiempo; la reducción de costos empresariales, que optimizó el uso de recursos y eliminó la necesidad de grandes infraestructuras físicas; y la inclusión laboral, que facilitó el acceso al empleo para personas con habilidades diferentes y para aquellos afectados por el desempleo durante la pandemia.
- Se estudió las principales barreras de acceso que limitan el teletrabajo, teniendo como principales: la falta de conectividad y recursos tecnológicos, especialmente en regiones rurales o con infraestructura digital deficiente; la resistencia al cambio y la desconfianza de los directivos, quienes dudaron en invertir en capacitación y herramientas digitales por temor a una baja productividad; y las barreras estructurales y culturales, las cuales excluyeron a ciertos grupos, como mujeres y personas con habilidades diferentes, debido a prejuicios ideológicos así como políticas laborales poco inclusivas.
- Se examinó la adaptación de los trabajadores a este nuevo sistema, obteniendo como resultado que ésta fue un proceso desigual y desafiante, condicionado por factores como el *tecnoestrés*, la falta de habilidades digitales y la resistencia al cambio, muchos empleados enfrentaron frustración y ansiedad ante la incertidumbre tecnológica, mientras que otros lograron beneficiarse de la flexibilidad para equilibrar su vida personal y laboral; sin embargo, la preparación insuficiente de las organizaciones, reflejada en la falta de herramientas, capacitación y estilos de liderazgo adaptativos, limitó el éxito de la transición de un sistema de trabajo antiguo a uno nuevo.

REFERENCIAS BIBLIOGRÁFICAS

- Agudo, J. (2014). *El teletrabajo en las organizaciones: Análisis de sus beneficios y barreras en las empresas españolas*. <https://digitum.um.es/digitum/handle/10201/51060>
- Álvarez, H. (2020). Del recurso al teletrabajo como medida de emergencia al futuro del trabajo a distancia. *Lan harremanak: Revista de relaciones laborales*, 43, 7. <https://dialnet.unirioja.es/servlet/articulo?codigo=7572660>
- Andrade, E. (2022). El teletrabajo como mecanismo paradigmático del poder en las sociedades de control modernas. *Foro: Revista de Derecho*, 38, 207-228. <https://doi.org/10.32719/26312484.2022.38.10>
- Araujo-Robles, E., Díaz, M., & Díaz, J. (2021). Dinámica familiar en tiempos de pandemia (COVID -19): Comunicación entre padres e hijos adolescentes universitarios. *Revista Venezolana de Gerencia*, 26(95), 610-628. <https://www.redalyc.org/journal/290/29069613009/>
- Arce, L., & Rojas, K. (2020). Satisfacción laboral y estrés en teletrabajadores y trabajadores presenciales de una universidad estatal de Costa Rica. *UNED Research Journal*, 12(2), e3141. <https://doi.org/10.22458/urj.v12i2.3141>
- Arévalo, J. (2024). El teletrabajo en el Perú. *Revista de Derecho Procesal del Trabajo*, 7(9), Article 9. <https://doi.org/10.47308/rdpt.v7i9.958>
- Aristizábal, K., Escandon, J., Ruiz, E., Alvarado, V., Castillo, P., Gonzales, J., & Blanquicet, V. (2022). El teletrabajo: Un antes, un durante y un después de la pandemia. *Relaciones humanas, comunicación y normativa durante la pandemia, 2022*, ISBN 978-958-5158-46-7, págs. 181-206. <https://dialnet.unirioja.es/servlet/articulo?codigo=9024030>
- Benavides, F., & Silva-Peñaherrera, M. (2022). Datos y evidencias del teletrabajo, antes y durante la pandemia por COVID-19. *Archivos de Prevención de Riesgos Laborales*, 25(2), 133-146. <https://doi.org/10.12961/aprl.2022.25.02.06>
- Bonilla, L., Plaza, D., De Cerquera, G., & Riaño-Casallas, M. (2014). Teletrabajo y su Relación con la Seguridad y Salud en el Trabajo. *Ciencia & trabajo*, 16(49), 38-42. <https://doi.org/10.4067/S0718-24492014000100007>

- Broche-Pérez, Y., Ferández, E., & Reyes, D. (2020). *Consecuencias psicológicas de la cuarentena y el aislamiento social durante la pandemia de COVID-19*. <https://www.scielo.org/article/rcsp/2020.v46suppl1/e2488>
- Camacho, J. (2021). El teletrabajo, la utilidad digital por la pandemia del COVID-19. *Revista Latinoamericana de Derecho Social*, 32, 125-155. <https://www.redalyc.org/articulo.oa?id=429671777006>
- Chávez, M., & Mendoza, J. (2024). *Factores del comportamiento en el capital humano que impactan en la adaptación al teletrabajo: Una revisión de literatura.(Behavioral factors in human capital that impact on adaptation to teleworking: a literature review.)*. <https://vinculategica.uanl.mx/index.php/v/article/download/491/974>
- Contreras, O., & Roza, I. (2015). Teletrabajo y sostenibilidad empresarial. Una reflexión desde la gerencia del talento humano en Colombia. *Suma de Negocios*, 6(13), 74-83. <https://doi.org/10.1016/j.sumneg.2015.08.006>
- De Mello, P. (2024). Impactos del teletrabajo en la satisfacción laboral y el salario emocional. Caso empresa de telecomunicaciones de Uruguay. *Project Design and Management*, 6(1), Article 1. <https://doi.org/10.35992/pdm.6v1.2140>
- Fantini, A. (2013). Teletrabajo, una beneficiosa realidad. *Relaciones Laborales y Derecho del Empleo*. https://ejcls.adapt.it/index.php/rldc_adapt/article/view/80
- Fernández, B. (2023). *El recurso humano en la pandemia y el teletrabajo*. <https://portal.amelica.org/ameli/journal/223/2234308006/html/>
- Fernández, F., & Peral, D. (2011). Análisis De Redes Como Método Para La Definición De Conceptos: Bibliografía. *Anales de Documentación*, 14(1), 1-14. <https://www.redalyc.org/articulo.oa?id=63517100004>
- García-Rubio, M., Silva-Ordoñez, C., & Salazar-Mera, J. (2021). Modalidad teletrabajo en tiempos de pandemia COVID- 19 en Ecuador. *Revista de Ciencias Sociales*, 27.
- Guzmán, A., & Abreo, C. (2017). Las habilidades del teletrabajador para la competitividad. *Forum Empresarial*, 22(2), 5-30. <https://www.redalyc.org/journal/631/63154910002/>

- Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las ritas cuantitativa, cualitativa y mixta*.
- Maguiña, C., Gastelo, R., & Tequen, A. (2020). El nuevo Coronavirus y la pandemia del Covid-19. *Revista Médica Herediana*, 31(2), 125-131. <https://doi.org/10.20453/rmh.v31i2.3776>
- Ortiz, M., Larregui, G., & Rivera, J. (2024). Factores que impactan el desempeño laboral: Estudio sobre la adaptabilidad al teletrabajo inducido por el evento del COVID-19. *Revista Academia & Negocios*, 10(1), 121-144. <https://www.redalyc.org/articulo.oa?id=560876830006>
- Osio, L. (2010). El Teletrabajo: Una opción en la era digital. *Observatorio Laboral Revista Venezolana*, 3(5), 93-109. <https://www.redalyc.org/articulo.oa?id=219014912006>
- Pérez, C., & Gálvez, A. (2009). Teletrabajo y vida cotidiana: Ventajas y dificultades para la conciliación de la vida laboral, personal y familiar. *Athena Digital. Revista de Pensamiento e Investigación Social*, 15, 57-79. <https://www.redalyc.org/articulo.oa?id=53712929004>
- Ramírez, J., Tapia, H., & Vega, C. (2021). Teletrabajo en Sudamérica: Un desafío jurídico frente al covid-19. *Revista Venezolana de Gerencia*, 26(94), 622-677. <https://www.redalyc.org/articulo.oa?id=29069612011>
- Rodríguez, M. (2007). El teletrabajo en el mundo y Colombia. *Gaceta Laboral*, 13(1), 29-42. <https://www.redalyc.org/articulo.oa?id=33613102>
- Rodríguez, M., & Pérez, I. (2007). Tipos de estudio en el enfoque de investigación cuantitativa. *Enfermería Universitaria*, 4(1). <https://doi.org/10.22201/eneo.23958421e.2007.1.469>
- Romero-Padilla, Y., Susaeta-Erburu, L., & Martín-Duque, C. (2022). El impacto de la pandemia en las trabajadoras del sector hotelero: El reto de la conciliación y la adaptación al teletrabajo. *Algoritmos, teletrabajo y otros grandes temas del feminismo digital, 2022, ISBN 978-84-1122-494-9, págs. 439-454*, 439-454. <https://dialnet.unirioja.es/servlet/articulo?codigo=8768318>
- Roncal, X. (2021). Teletrabajo y capitalismo de vigilancia. *Telos*, 23(1), 177-188. <https://www.redalyc.org/articulo.oa?id=99365404014>

- Tapasco-Alzate, O., & Giraldo-García, J. (2020). Asociación entre posturas administrativas de directivos y su disposición hacia la adopción del teletrabajo. *Información tecnológica*, 31(1), 149-160. <https://doi.org/10.4067/S0718-07642020000100149>
- Tunal, S. (2012). Reflexiones en torno a los análisis sobre el teletrabajo. *Trabajo y Sociedad*, 19, 31-54. <https://www.redalyc.org/articulo.oa?id=387334691002>
- Valle, G. (2018). Teletrabajo, necesidad y solución en Méjico. Un estudio exploratorio de sus barreras culturales y obstáculos. *Teuken Bidikay: Revista Latinoamericana de Investigación en Organizaciones, Ambiente y Sociedad*, 9(12), 153-176. <https://dialnet.unirioja.es/servlet/articulo?codigo=8761020>
- Vargas, A., & Osma, J. (2013). Propuesta de Implementación de un Modelo de Teletrabajo. *Iberian Journal of Information Systems and Technologies*, 0(12), 17-31. <https://doi.org/10.4304/risti.12.17-31>
- Yeves, J., Bargsted, M., Orlandini, E., & Ureta, S. (2023). Flexibilidad Laboral en Pandemia y sus Efectos en Estrés, Inseguridad y Satisfacción Laboral. *Psykhē (Santiago), Online First*. <https://doi.org/10.7764/psykhe.2021.41401>

EL DESTINO DE LOS BIENES DIGITALES POST MORTEM

Angie F. Fernández-Silva¹

RESUMEN

Esta investigación tuvo por objetivo describir la regulación de la transmisión de bienes digitales post mortem en Latinoamérica, para ello se utilizó un enfoque cualitativo, en una investigación de tipo básica, con un diseño no experimental – descriptivo, recolectando la información de las bases de datos: SCOPUS, REDALY Y DIALNET obteniendo un total de 30 artículos que se analizaron. Los principales resultados arrojaron lo siguiente: la herencia digital está conformada por activos virtuales, desde cuentas bancarias hasta perfiles en redes sociales; la naturaleza jurídica de los bienes digitales es multifacética y cambiante, su naturaleza híbrida combina elementos patrimoniales y personales; la regulación de la herencia digital en Latinoamérica a pesar de algunos avances en áreas como la protección de datos personales, aún no existe un marco legal unificado; la sucesión de bienes digitales está en constante transformación jurídica, pero aún con muchas lagunas, a medida que los activos digitales cobra relevancia la necesidad de una regulación clara sobre su transmisión hereditaria se vuelve cada vez más apremiante. Concluyendo que, la transmisión de los bienes digitales en Latinoamérica avanza lentamente, pero que si se tiene conocimiento de la existencia de los bienes digitales y se usan las normas vigentes para su transmisión.

Palabras clave: Transmisión, bienes digitales, herencia digital, herederos.

¹ afernandezsl@upao.edu.pe

Programa de Estudio de Derecho, Universidad Privada Antenor Orrego

ABSTRACT

This research aimed to describe the regulation of the transmission of digital assets post-mortem in Latin America. A qualitative approach was used in a basic type of research with a non-experimental descriptive design. Information was collected from the databases SCOPUS, REDALY, and DIALNET, obtaining a total of 30 articles that were analyzed. The main results revealed the following: digital inheritance consists of virtual assets, ranging from bank accounts to social media profiles; the legal nature of digital assets is multifaceted and dynamic, with a hybrid nature that combines patrimonial and personal elements; despite some progress in areas such as personal data protection, there is still no unified legal framework for digital inheritance regulation in Latin America; the succession of digital assets is undergoing constant legal transformation but still faces many gaps. As digital assets gain relevance, the need for clear regulation on their hereditary transmission becomes increasingly pressing. The study concludes that the transmission of digital assets in Latin America is progressing slowly, but if awareness of digital assets exists and current regulations are applied, their transmission can be managed.

Keywords: Transmission, digital assets, digital inheritance, heirs.

INTRODUCCIÓN

Todo va evolucionando, antes los bienes solo eran considerados como tangibles e intangibles; al 2024, también se mencionan los denominados bienes digitales, demostrando que las personas han encontrado otras formas de constituir actos jurídicos que por su naturaleza estos son susceptibles de derechos sucesorios: como el bitcoin, criptomonedas, realidades virtuales e incluso las redes sociales.

Santos (2018) definió a los bienes digitales como cualquier información o archivo de naturaleza digital reservado localmente u online, se entiende que incluye una amplia gama de contenidos, desde documentos de texto y presentaciones hasta imágenes, videos y software. Al 2024, las nuevas generaciones son más cercanas a la tecnología y a la practicidad; los jóvenes ya no llevan dinero en las billeteras, sino que prefieren invertir su dinero en acciones o comprar criptomonedas, desencadenando así un patrimonio digital.

Castillo y Palancares (2010) establecieron que una característica preponderante de los bienes digitales es que implica una inversión inicial significativa, con costos fijos considerables, pero una vez realizada la adquisición, los costos adicionales por unidad producida son bajos; este

modelo de costos impulsa una competencia intensa, lo que redundará en ventajas para el acreedor.

Al significar un costo alto el adquirir un bien digital, llegando a considerarse como inversión a largo plazo, es prudente pensar en su preservación, protección y futura transmisión hacia los herederos, es por ello que resulta importante hablar de este tema y que lleva a una pregunta poco frecuente: ¿Qué pasará con mis bienes digitales después de mi muerte? ¿Hay alguna forma de dejarlos a mis herederos?

Países como EE. UU. cuenta con una legislación al respecto denominada “*Revised Uniform Fiduciary Access to Digital Assets Act*” (RUFADAA) para dar a los representantes legales (como albaceas y fiduciarios), la autoridad necesaria para gestionar los bienes digitales de personas que han fallecido o que ya no pueden hacerlo por sí mismas, para su conservación y posterior entrega (Cárdenas, 2024).

Por otro lado, en América Latina, no se sigue un modelo como el del país antes mencionado; al año 2024 las normativas son diversas y no rige un criterio uniforme, incluso en algunos países latinoamericanos aún es inexistente la normativa acerca de la transmisión del patrimonio digital post mortem, debido a que los legisladores no han visto esta situación como una de carácter urgente, como si se ha priorizado en EE.UU.

Un claro ejemplo es el país de Perú donde la normativa que regula las sucesiones es el Código Civil Peruano (2015) que menciona únicamente que desde la muerte de una persona todos sus bienes, derechos y obligaciones se transmiten a sus herederos, no existiendo alguna restricción en cuanto a los bienes digitales, porque el código no hace distinción de ellos, lo que resulta importante es regular esta práctica con alguna norma que permita una seguridad jurídica de que estos bienes serán entregados a los herederos.

En esa misma línea si bien no existe alguna restricción, el Código Civil Peruano desde su entrada en vigencia en el año 1984, al año 2024 tiene más de 40 años y al momento de su creación el legislador no imaginó que los bienes digitales formarían parte de la vida diaria, con el desarrollo de nuevas tecnologías que permiten poder adquirir estos bienes de forma más rápida; sin lugar a duda, estos son susceptibles de derechos sucesorios como cualquier otro bien que forma parte del patrimonio del causante y siendo los herederos (familia consanguínea) quienes tienen el privilegio de suceder al causante, estos también toman un papel protagónico.

Pérez (2010) mencionó que, al fallecer una persona, sus herederos tienen derecho a todo lo que ésta poseía, formando un patrimonio común hasta que se divida. Entonces se entiende que los herederos tomarán el papel del causante, pasarán a ser los nuevos titulares de los bienes que éste dejó, por ende, también se entiende que de los bienes digitales que pueda tener al momento de fallecer.

De lo que menciona el autor se puede entender que los herederos adquieren todos los derechos y obligaciones del fallecido, incluyendo los bienes digitales, esta perspectiva; sin embargo, choca con la naturaleza intangible y dinámica de los bienes digitales, que están sujetos a términos de servicio específicos de cada plataforma y a una regulación legal en desarrollo lo que dificulta la situación.

Este es un tema muy importante porque detrás de esos bienes digitales, se encuentra el dinero y tiempo que empleó esa persona para hacerse acreedor de ellos, bienes que como ya se ha mencionado enriquecen el patrimonio de una persona y estando Latinoamérica en su mayoría de países acogido a una tesis proteccionista de la legítima (bienes que heredan los parientes consanguíneos), esto quiere decir que se considera que la familia aportó de cualquier manera a enriquecer el patrimonio del causante (Fernández, 2017).

Por lo tanto, ante una situación compleja y de suma importancia en donde debe crearse un marco normativo que vaya acorde con las nuevas exigencias y las demandas crecientes de todos los peruanos respecto de los derechos sucesorios de bienes digitales. Tomando en cuenta que este tema engloba a temas no solo del derecho sucesorio sino del derecho contractual, comercial, tributario y notarial.

En este artículo, en primer lugar, se va a definir lo que se entiende por herencia digital; en segundo lugar, se va a identificar la naturaleza de los bienes digitales; en tercer lugar, se va a explicar la normativa existente sobre transmisión de bienes digitales post mortem en Latinoamérica y, finalmente, estudiar la posibilidad de la disposición del patrimonio digital mediante un testamento digital.

METODOLOGÍA

La falta de regulación de la transmisión de los bienes digitales post mortem en América Latina ha sido muy poco abordada, por lo que esta investigación

asume un enfoque cualitativo con el fin de lograr un acercamiento al tema de los bienes digitales post mortem; además, el tipo de investigación fue básica y el diseño de investigación fue no experimental – descriptivo. En un estudio descriptivo se miden las variables de forma individual, sin profundizar en sus interrelaciones, su propósito es ofrecer un retrato detallado del fenómeno estudiado, pero no siempre establecen conexiones causales entre las variables medidas (Hernandez et al., 1997).

La técnica se limitó a una revisión bibliográfica de 30 artículos científicos obtenidos de las bases de datos de Scopus, Redalyc, Dialnet, y la recolección de la información se realizó a través de fichas bibliográficas; que para su análisis se necesitó de un enfoque deductivo con un tipo de discurso orientado al orden de ideas de forma prevaleciente. Se llevó adelante el análisis documental de normativa internacional como: Constitución Política de Chile, Fiduciary Access to Digital Assets Act, Lei N°12.965, Lei N°13.709, Ley 1581, Ley de Protección de los Datos Personales, Ley Estatutaria 1266 y la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados, respecto a la delimitación temporal, inició el 19 de agosto del 2024, y se prolongó hasta el 2 de diciembre del 2024.

Se desarrolló el siguiente esquema temático: en primer lugar, fue necesario definir lo que se entiende por herencia digital; en segundo lugar, identificar la naturaleza de los bienes digitales; en tercer lugar, explicar la normativa existente sobre transmisión de bienes digitales post mortem en Latinoamérica y, finalmente, estudiar la posibilidad de la disposición del patrimonio digital mediante un testamento digital.

RESULTADOS

1. HERENCIA DIGITAL

Adriano y Hernández (2021) señalaron que el auge de las plataformas digitales ha dado origen a conceptos como herencia digital, también que esta figura exige una regulación clara para proteger los derechos de los usuarios y garantizar el cumplimiento de su última voluntad respecto a sus bienes digitales, tal como lo están haciendo países como Francia y España.

Entendiéndose que la herencia digital engloba el patrimonio digital Cucurull (2024) mencionaba que, en esencia, el patrimonio digital son los activos y elementos acumulados en un determinado entorno durante la vida de una persona, digital y valioso para la sociedad, estos activos reflejan la existencia y actividad de todos en el mundo digital.

Argelich (2023) definió que el término “herencia digital” engloba una amplia gama de activos digitales, entre los que destacan los criptoactivos. Estos son activos virtuales basados en la criptografía y la tecnología blockchain, como las criptomonedas y los NFTs, su valor es determinado por las fuerzas del mercado y puede fluctuar considerablemente.

La herencia digital no es ajena a la herencia convencional de bienes tangibles, esta herencia se transmite hacia los herederos igual que cualquier otra y la diferencia es que la herencia digital está compuesta de bienes digitales, estos bienes han sido adquiridos de forma digital o virtual por el causante antes de su fallecimiento y en algunos casos, tienen un importante valor económico que no puede ser desaprovechado por los sucesores.

La Carta de la UNESCO para la Preservación del Patrimonio Digital (2003) detalló que el patrimonio digital incluye documentos, arte, archivos, bases de datos, y otros materiales creados y almacenados electrónicamente, la carta destaca varias consideraciones clave para garantizar que este patrimonio no se pierda debido a obsolescencia tecnológica, degradación de soportes o falta de acceso.

Asimismo, que debe ser accesible para todos no solo a corto plazo, sino también para las generaciones futuras, también promueve la utilización de estándares abiertos y técnicas de preservación digital adecuadas, la carta enfatiza que la preservación del patrimonio digital es una responsabilidad colectiva que involucra a gobiernos, organizaciones internacionales, instituciones académicas, bibliotecas, archivos y demás actores clave, insta a la cooperación para la preservación digital.

Ordelin y Oro (2019) no dejaron de lado la importancia de una regulación de la sucesión digital, no solo se trata de asegurar la certeza legal, sino también de garantizar la efectividad de los derechos, debido a la creciente relevancia de los bienes digitales en la sociedad, especialmente considerando las implicaciones que surgen al momento de disponer de ellos tras el fallecimiento de su propietario.

Como se ha dejado en claro la herencia digital está compuesta por bienes digitales para lo que Santos (2018) definió que los “bienes digitales” son una amplia gama de elementos, desde cuentas bancarias online hasta contenidos creados por el usuario en redes sociales, en esencia, cualquier información almacenada digitalmente, ya sea de carácter personal o económico, puede considerarse un bien digital.

El autor logra capturar la complejidad y diversidad de lo que se entiende por “bienes digitales”, al incluir tanto aspectos patrimoniales (cuentas bancarias) como extrapatrimoniales (contenidos en redes sociales), reconoce la naturaleza multifacética de estos activos digitales, lo cual la hace de fácil adquisición y una posible transmisión después de la muerte.

Siguiendo con el concepto de herencia digital García (2021) mencionó que la herencia digital abarca dos elementos principales: el valor económico de las cuentas digitales y la identidad digital. El primero incluye cuentas que generan ingresos, mientras que el segundo se refiere a perfiles personales sin valor monetario directo, sin embargo, muchas cuentas en redes sociales combinan ambos elementos, aunque algunos países ofrecen herramientas para gestionar esta herencia, su eficacia es limitada y varía según el caso.

El autor señala la importancia de contar con herramientas y marcos legales para gestionar la herencia digital, sin embargo, también advierte sobre la limitada eficacia y variabilidad de estas herramientas según el contexto, también se marca una línea divisoria entre el valor económico y la identidad digital no siempre es clara, especialmente en el caso de las redes sociales, donde ambos elementos pueden coexistir.

Por otro lado Otero (2019) sostiene que la herencia digital abarca un espectro amplio, desde contenidos personales en redes sociales hasta activos digitales con valor económico, aunque la palabra “herencia” suele asociarse con bienes patrimoniales, en este contexto se extiende para incluir también aspectos más intangibles de la identidad digital.

Es propio mencionar que muchos autores consideran que los términos “patrimonio” y “herencia” son prácticamente iguales, diferenciándose únicamente por el momento en la vida de una persona: antes o después de su fallecimiento, sin embargo, algunos argumentan que la herencia trasciende lo meramente patrimonial, incluyendo aspectos más personales, en este sentido, el término «herencia digital» podría englobar tanto el contenido digital con valor económico como aquel que tiene un valor personal o sentimental (Cucurull, 2022).

Para Ginebra (2020) el “patrimonio digital” agrupa de manera amplia una heterogeneidad de elementos digitales, que van desde simples archivos hasta complejos activos virtuales, y que a menudo se denominan indistintamente bienes, contenidos o servicios digitales. Entonces puede entender que existe una amplia selección de bienes digitales que componen el patrimonio digital.

Por otro lado, se debe precisar que la expansión del concepto de herencia digital plantea nuevos desafíos legales en la regulación, diseñada principalmente para bienes materiales, no siempre es adecuada para gestionar la transmisión de bienes digitales, es necesario desarrollar marcos legales específicos que aborden cuestiones como la identificación de los herederos digitales, la gestión de las contraseñas, la protección de la privacidad y la validez de los testamentos digitales.

Respecto a los bienes digitales que forman parte de la personalidad del causante Farooqui et al. (2022) detallaron que redes sociales albergan una gran cantidad de activos digitales como imágenes, videos y mensajes que, más allá de su valor monetario, tienen un gran significado personal y social para los usuarios, a pesar de su importancia, la legislación en países como India y Estados Unidos aún no ha establecido un marco legal claro para determinar qué ocurre con estos activos digitales después de la muerte de una persona y quién tiene derecho sobre ellos.

Los activos no patrimoniales como las redes sociales se han convertido en una extensión de nuestra identidad digital, almacenando una gran cantidad de información personal y sentimental, sin embargo, como bien señala el estudio del autor antes mencionado la legislación en muchos países aún no ha logrado adaptarse a esta nueva realidad.

Estos activos están relacionados con la identidad digital para García (2017, citado por Ordelin & Oro, 2019) detallaron que dentro de los bienes digitales de carácter personal, se incluyen todos aquellos vinculados a la identidad digital, entendida como la identidad personal en el ámbito virtual, que puede o no coincidir con la identidad física, y que está asociada al perfil del usuario en plataformas de redes sociales.

Asimismo Ruda (2017, citado por Rodríguez & Martínez, 2018) mencionaron que, al abordar la herencia de los bienes digitales, su acceso y gestión no se trata únicamente con una cuestión regulada por el derecho sucesorio, existen aspectos relacionados con la privacidad, el derecho internacional privado y las prácticas sociales y culturales que, si se abordan desde un solo enfoque, pueden llevar a soluciones excesivamente limitadas.

Estos autores subrayan la complejidad de la herencia digital, al ir más allá del derecho sucesorio, reconocen la necesidad de un enfoque multidisciplinario que considere aspectos como la privacidad y el derecho internacional privado, esta perspectiva es crucial para evitar soluciones

simplistas y garantizar una gestión adecuada de los bienes digitales tras el fallecimiento de un individuo.

Para Farooqui et al. (2022) se debe implementar la herencia digital mediante un plan de patrimonio digital es una estrategia para organizar y proteger tus activos digitales, implica crear un inventario de tus cuentas en línea, contraseñas y otros datos importantes, y designar a un contacto de confianza para que gestione esta información en caso de fallecimiento o incapacidad.

2. Naturaleza de los bienes digitales

Con el paso de nuevas tecnologías el mundo ha evolucionado y esto ha traído consigo nuevas formas de adquirir bienes, a las formas tradicionales ya conocidas como la transacción directa de dinero o bancaria, al 2024 con dinero en el banco, una computadora e internet puedes hacerte acreedor a muchos bienes de forma rápida y directa, solo entrando a una página web o una aplicación. Es esto lo que facilita poder adquirir bienes digitales que muchas veces llegan al valor de un monto muy considerable, lo que lleva a una pregunta ¿Cuál es la naturaleza de los bienes digitales?

Haworth (2014, citado por Rodríguez & Martínez, 2018) propusieron que los bienes digitales se distinguen tanto por el tipo de servicio o por la naturaleza de su información a la que se desea tener acceso, para un mayor interés explicativo la segunda opción antes mencionada es la ideal, esta se centra en diferentes ámbitos como las redes sociales, criptomonedas, entre otros que se pasaran a explicar.

Al clasificar los bienes digitales por la naturaleza de su información, se evita una categorización demasiado general basada únicamente en el tipo de servicio, esto permite una comprensión más profunda de las características y particularidades de cada tipo de bien digital, al centrarse en diferentes ámbitos, la propuesta facilita una explicación más detallada y comprensible de las características y desafíos asociados a cada tipo de bien digital.

Por otro lado, la normativa Estadounidense denominada Ley Fiduciary to Digital Assets Act (2016) estableció que existen cuatro tipos de bienes: a) bienes que incluyen el acceso a información como dígitos de cuenta, que ayudarán a acceder a cuentas de connotación patrimonial. b) bienes tangibles no se refieren a la existencia física, sino a archivos informáticos (como fotografías hasta documentos de texto) que pueden ser transferidos a terceros, tienen valor económico, cultural o sentimental.

c) Bienes digitales intangibles, esta categoría se diferencia de las categorías anteriores porque se refiere a la información publicada en el perfil del usuario o en comentarios de sus publicaciones de una red social en línea, publicaciones de Instagram, Facebook, X (anteriormente Twitter) o “me gusta” de Facebook que marcan la presencia en línea.

d) Metadatos se refiere a datos almacenados electrónicamente en archivos o sitios web, incluida información sobre el historial de acceso, ubicación, datos eliminados, código de programa, etc. Los dos tipos son realmente difíciles de acceder y aún más difíciles de eliminar, los metadatos, aunque a menudo invisibles para el usuario promedio, contienen información valiosa sobre la creación, modificación y uso de archivos digitales.

Con todo lo mencionado se evidencia que la ley antes mencionada reconoce que los activos digitales abarcan un espectro amplio, desde aquellos que otorgan acceso a cuentas bancarias hasta información intangible como los metadatos, también demarca la diferenciación entre bienes tangibles digitales (archivos) e intangibles (información en redes sociales) es un paso importante para comprender la naturaleza diversa de estos activos, a su vez respecto a los metadatos refiere que la ley reconoce el valor intrínseco de esta información y la necesidad de protegerla. Todo ello por la tecnología digital que evoluciona rápidamente.

Por otro lado, Díaz (2017) mencionaba que de forma tradicional la clasificación de los bienes es tangible e intangible, pero esto ha quedado obsoleto ante el auge de lo digital. Al 2024, los intangibles se dividen en dos: los nativos digitales, creados y existentes únicamente en el ciberespacio, y los digitalizados, que han migrado al mundo digital desde un formato físico, estos, aunque tengan un original físico, pierden relevancia jurídica ante su versión digital.

La división propuesta entre bienes nativos digitales y digitalizados resulta especialmente acertada para comprender la complejidad de los activos en la era digital, al señalar que los bienes digitalizados, a pesar de tener un original físico, pierden relevancia jurídica ante su versión digital, se subraya la importancia creciente de los formatos digitales en el ámbito legal. Un ejemplo claro de bienes nativos digitales son los tokens.

Es propio mencionar que Brayans (2014, citado por Anatolyevna et al., 2020) determinaron que un token representa una porción de propiedad o acceso a un proyecto blockchain, proporcionando a sus titulares derechos

y privilegios exclusivos, como descuentos en productos o servicios, participación en decisiones de gobernanza, o acceso a funcionalidades especiales. Es importante mencionar ello porque como se ha mencionado que un token tiene naturaleza propia del ciberespacio.

Así mismo para Gámez y Corredor (2023) los NFTs, tokens no fungibles basados en blockchain, permiten la representación digital única de activos, con implicaciones significativas para la propiedad intelectual y la gestión de activos digitales, estos como nuevos actores en el ecosistema cripto, están demostrando un enorme potencial para revolucionar industrias creativas y coleccionables.

Por otro lado, Ordellin y Oro (2019) determinaron que los bienes digitales poseen una naturaleza personal porque está relacionada con la identidad digital del sujeto lo que fue en vida en el ámbito del mundo digital que contiene derechos personales como el derecho al honor que como bien se sabe no se extingue este derecho después de la muerte, también el derecho a la imagen a que se respete el nombre y apellido.

Como bien señalan, los bienes digitales están estrechamente vinculados a la identidad digital, lo que plantea cuestiones importantes sobre la privacidad, la seguridad y la protección de datos personales que opino que son privados, pero todo dependerá de la voluntad del causante, si este decide dejar en herencia sus redes sociales o cuentas de contenido patrimonial.

De la misma manera López y Araya (2022, citado por Goic & Martínez, 2023) concluyeron que el patrimonio digital goza de una identidad digital de naturaleza jurídica y sostienen que la identidad digital puede ser conceptualizada como un derecho de la personalidad, es decir, una facultad inherente a la persona que tiene como finalidad proteger su dignidad y garantizar su libre desarrollo de la personalidad.

Al considerar la identidad digital como un derecho de la personalidad, se reconoce su valor intrínseco y su importancia para el desarrollo personal y social. Asimismo, con los derechos de la personalidad, se establece un marco legal sólido para protegerla contra posibles abusos, sin embargo, la protección de la identidad digital puede entrar en conflicto con otros derechos, como el derecho a la libertad de expresión o el derecho a la información.

Para Castillo y Palancares (2010) los bienes digitales tiene un naturaleza económica, debido a que los costos de producción de bienes digitales se

concentran al inicio del proceso, la fijación de precios se convierte en un factor crucial para el éxito comercial de estos productos, es necesario establecer precios que permitan recuperar la inversión inicial y generar ganancias sostenibles.

Al destacar que los costos de producción de bienes digitales se concentran al inicio del proceso, los autores ponen de manifiesto una característica distintiva de estos bienes: una vez creado un producto digital, los costos de producción de unidades adicionales son prácticamente nulos. Esta particularidad implica que la recuperación de la inversión inicial resulta fundamental para la viabilidad económica de estos productos.

Por otro lado, Cucurull (2022) mencionó que algunos bienes digitales son de naturaleza puramente personal, tanto los datos personales como los contenidos digitales son susceptibles de ser utilizados para infringir derechos fundamentales como el honor, la intimidad y la propia imagen que pueden afectar a la persona tanto en vida como fallecida y sus herederos pueden tomar las acciones legales pertinentes.

En la misma línea Santos (2018) señaló que hay bienes digitales de carácter no patrimonial como que se refieren a los derechos morales y a las creaciones intelectuales, entendiéndose que son los producidos por el causante en una red social, que pueden formar parte de la masa hereditaria; y por consiguiente heredada por los sucesores, cabe señalar que este contenido suele ser fotográfico, informativo y auditivo.

El autor abre un interesante debate sobre la sucesión hereditaria en el ámbito digital, sin embargo, es necesario profundizar en el análisis jurídico y técnico de estos bienes digitales no patrimoniales para establecer un marco normativo adecuado que garantice tanto la protección de los derechos de los herederos como el respeto a la privacidad y a los derechos de autor.

Por otro lado Barroilhet (2019) destacó que a naturaleza jurídica de las criptomonedas, entendiéndose esta como parte de los bienes digitales, tiene ramificaciones legales de gran alcance, desde la determinación de quién debe regularlas y cómo se gravan, hasta la definición de las obligaciones de las partes involucradas en una transacción, la clasificación de las criptomonedas es un tema central en el debate jurídico. Ningún país desarrollado ha logrado establecer un marco regulatorio exhaustivo y específico para este fenómeno.

3. Normativa existente sobre transmisión de bienes digitales post mortem en latinoamérica

Si bien es cierto en América Latina el tema de la sucesión de los bienes digitales post mortem no se encuentra tan desarrollada como en países del continente europeo, quienes, sí dan salidas más factibles ante estas situaciones, sin embargo, se tienen ciertos alcances en torno a esta materia que buscan llegar a una solución que si bien es cierto no es del todo eficiente como una Ley *Siu Generis*, aportan algunos vestigios para controlar estas cuestiones.

Para fines del año 2023, Chile carecía de una normativa específica para los bienes digitales. Es así como Goic y Martínez (2023) consideraron que, esta se debe remitir a la Constitución Política de la República de Chile (1822) específicamente a su artículo 19 N° 23 se detalla que existe una amplia gama de derechos fundamentales, como el de la libertad para poder adquirir cualquier tipo de bienes digitales, se usa supletoriamente esta normativa para dar respuesta a estos escenarios, porque no existe una norma específica que ampare este tema.

Entendiéndose, que el artículo 19 número 23 de la Constitución Política de la República de Chile (1822), garantiza la libertad de adquirir bienes, sugiere que estos también podrían ser objeto de transmisión, a menos que exista una ley que lo prohíba explícitamente, dando así carta abierta para que cualquier bien sin importar su naturaleza pueda ser susceptible de transmisión hereditaria, inclusive no habiendo impedimento de que los herederos puedan acceder a estos bienes si el causante deja o no un testamento.

Al interpretar de manera amplia el derecho a adquirir bienes consagrado en el artículo 19 N° 23, se busca dar una respuesta flexible y adaptable a las nuevas realidades tecnológicas. En un contexto donde la legislación aún no ha alcanzado a regular exhaustivamente los bienes digitales, esta interpretación ofrece una vía para resolver los conflictos que puedan surgir en materia sucesoria.

Para la situación argentina se debe tomar en cuenta el artículo 14.4 de la Ley de Protección de los Datos Personales (2000), que reconoce el derecho de los sucesores universales a acceder a los datos personales de una persona fallecida siempre y cuando acrediten su condición de herederos, esto es muy importante porque algunos datos son de carácter personal, esto quiere decir que, si muere el titular, estos bienes se pierden.

La legislación argentina, a través de la citada norma, establece un precedente importante al reconocer el derecho de los sucesores universales a acceder a los datos personales de una persona fallecida, este reconocimiento implica un avance en la protección de los derechos patrimoniales de los herederos, al permitirles conocer y gestionar los bienes digitales del causante.

En lo que respecta a la normativa colombiana, se considera a los artículos 5 y 16 de la Ley Estatutaria 1266 (2008), que tiene una posición similar a la Argentina porque garantiza el derecho de los herederos a poder conocer la información personal de un fallecido que se encuentre almacenada en bases de datos para el manejo de los herederos.

En el marco colombiano se tiene a la Ley 1581 (2012), esta es una norma fundamental en Colombia que se encarga de proteger tus datos personales, esta ley garantiza que tu información privada sea manejada de manera segura y responsable por cualquier entidad, ya sea pública o privada, que la recolecta, almacene o utilice información. La mencionada ley aplica a todas las personas naturales o jurídicas, públicas o privadas, que recolecten, almacenen, utilicen o circulen datos personales.

Tanto las leyes 1266 y 1581, como las resoluciones complementarias, establecen un marco normativo claro para el ejercicio de este derecho, asegurando que los causahabientes puedan acceder a la información de los bancos, aseguradoras, entidades comerciales; como de servicios de manera oportuna y segura, logrando así poder acceder a la masa hereditaria.

Otro punto interesante en cuanto al país colombiano es que la Corte Constitucional colombiana, en su Sentencia C-1011/08, ha interpretado el derecho fundamental al habeas data de manera extensiva, incluyendo a los causahabientes como sujetos legitimados para ejercer este derecho en relación con la información financiera del fallecido, esta interpretación se fundamenta en el interés patrimonial que los herederos tienen en dicha información y en la necesidad de garantizar el ejercicio de sus derechos sucesorios (Ordelin & Oro, 2019).

Se entiende al habeas data como un mecanismo constitucional que impone a las entidades la obligación de transparentar el tratamiento de los datos personales, es decir, de informarnos sobre su contenido, finalidad y uso, asimismo, este derecho faculta a ejercer los mecanismos de acceso, actualización, rectificación y supresión de la información que resulte inexacta, incompleta, irrelevante o excesiva (Chiriboga, 2002).

Los ordenamientos jurídicos argentino y colombiano no contemplan de manera expresa la facultad del titular de los datos personales de disponer de ellos a título testamentario, si bien los sucesores tienen legitimación para acceder a estos datos, la designación de sucesores testamentarios no implica necesariamente una facultad dispositiva plena sobre los derechos inherentes a los datos personales, especialmente cuando se trata de derechos que no forman parte del patrimonio del causante.

Mientras que, en México, según la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados (2017), las solicitudes de protección de datos se extinguen con la muerte del titular, por lo tanto, es una ley mexicana que establece las reglas para proteger tu información personal, imagina que tus datos personales son como un tesoro muy valioso; esta ley se encarga de poner un candado muy fuerte para que nadie más pueda acceder a ese tesoro sin tu permiso.

Evidenciándose así que en materia de protección de datos personales tras el fallecimiento del titular, México y Colombia presentan enfoques opuestos, demostrándose que incluso en países del mismo continente puede haber opiniones divergentes. Por eso se habla de que no hay una unificación normativa en cuanto a la disposición post mortem de los bienes digitales.

La doctrina jurídica brasileña ha abordado la cuestión de la sucesión digital en ausencia de una regulación expresa, en su lugar toma protagonismo la Ley N°12.965 (2014), también conocida como Marco Civil de Internet, es una legislación brasileña de suma importancia que establece los principios, garantías, derechos y deberes para el uso de internet en ese país, es considerada una de las leyes más completas y avanzadas del mundo en materia de regulación del ciberespacio.

Lo que busca esta ley es garantizar la privacidad, la libertad de expresión, el acceso a la información y otros derechos fundamentales en el entorno digital, también define las responsabilidades de los proveedores de servicios de internet, los usuarios en el ciberespacio y protege la libertad de expresión en el entorno digital, pero establece límites para evitar la difusión de contenidos ilícitos.

También dentro de la normativa brasileña se encuentra la Ley N°13.709 (2018) que establece las normas para la protección de los datos personales de todos los ciudadanos brasileños, su objetivo principal es garantizar los derechos de libertad, privacidad y el libre desarrollo de la personalidad de cada individuo, al regular el tratamiento de sus datos personales.

Si bien en Brasil no existe una regulación clara sobre la herencia de bienes digitales, algunos expertos consideran que es posible incluirlos en un testamento, especialmente aquellos que tienen valor económico. Sin embargo, hay un debate sobre los bienes digitales de carácter personal, como las cuentas de correo electrónico, estas están ligadas a la identidad de la persona y no pueden transmitirse como una herencia tradicional.

En Perú, el único dispositivo legal que regula la sucesión hereditaria es el Código Civil Peruano (2015), pero este no menciona expresamente algo referente a la disposición de bienes digitales, por lo que la ley no lo prohíbe y el causante está en el derecho de hacer plena disposición de dichos bienes, dicha posición se sustenta en el artículo 2, inciso 24 literal a de la Constitución Política del Perú (1993) que prescribe lo siguiente: Nadie está obligado a hacer lo que la ley no manda, ni impedido de hacer lo que ella no prohíbe.

Como se ha podido observar la normativa en América Latina es diversa, en países como Perú es inexistente y en otros se sirven de leyes vigentes como auxiliares que ayudan en cuanto a la disposición de bienes digitales post mortem, se deja en evidencia que debe existir leyes especiales para regular este tema en específico lo que facilitará tanto al causante poder englobar a todos sus bienes en la masa hereditaria y a los herederos a reclamar.

4. Disposición del patrimonio digital mediante un testamento digital

Surge una duda recurrente respecto a la transmisión de los bienes digitales post mortem y esa es la siguiente: ¿Cómo dispongo de mis bienes digitales? Se tiene que la normativa es diversa, no se llega a una solución directa y clara, por lo que examinará en base a lo que sustentan diversos autores si es posible disponer de los bienes digitales en un testamento digital.

Argelich (2023) definió que la figura del “testamento digital” es una herramienta para regular la sucesión de los contenidos extrapatrimoniales en las plataformas en línea. Se usa como una cláusula testamentaria que permite al causante designar a un heredero digital para que gestione sus datos personales y perfiles en línea después de su fallecimiento.

Llopis (2016 como se citó en González, 2021) referían que la terminología ‘testamento digital’ presenta una cierta imprecisión, puede aludir tanto al conjunto de instrucciones sobre la gestión de nuestros bienes digitales tras nuestro fallecimiento como al acto de otorgar testamento a través de medios electrónicos.

A su vez el concepto de “testamento digital” presenta una doble vertiente, puede referirse tanto a la disposición sobre bienes digitales como a la utilización de medios electrónicos para formalizar cualquier testamento, esta dualidad refleja la creciente importancia de los activos digitales en el patrimonio de las personas y la adaptación del derecho a las nuevas tecnologías (Andrade et al., 2023).

Aparece una nueva terminología aparte del testamento digital, este es el testamento online, para ello Martínez (2019) explicó que es importante distinguir entre el “testamento digital” y el “testamento online”. El primero abarca un espectro más amplio, incluyendo tanto testamentos tradicionales con disposiciones digitales como aquellos redactados íntegramente en formato digital, el “testamento online”, en cambio, se refiere exclusivamente a la segunda categoría.

Respecto al testamento digital Romanowski y de Oliveira (2024) hacen referencia que en Brasil la pandemia de la COVID-19 aceleró la digitalización de la vida, incluyendo los procesos legales, esto ha puesto en el centro del debate la validez de los testamentos digitales, que surgieron como una necesidad durante el confinamiento, aunque estos testamentos han sido utilizados, su reconocimiento legal aún es incierto, generando dudas sobre su cumplimiento con las formalidades establecidas en el Código Civil.

Rodríguez y Martínez (2018) determinaron que el testamento digital plantea desafíos legales importantes, como lo demuestra el caso de Bruce Willis, quien le quiso dejar a sus hijas en herencia su plataforma de música iTunes, pero debido a los términos y condiciones de esta aplicación que no permite compartir con terceros la música almacenada, no pudo lograrlo.

El caso de Bruce Willis pone de manifiesto la necesidad urgente de abordar los desafíos legales planteados por el testamento digital. Es fundamental desarrollar un marco legal claro y flexible que permita a las personas disponer de sus activos digitales de manera autónoma y respetuosa con sus últimas voluntades.

Ante la ausencia de leyes específicas sobre herencia digital, la solución más práctica es que las personas decidan el destino de sus activos digitales a través de un testamento. En países como Brasil, aunque no hay una ley que lo regule explícitamente, tampoco existe una prohibición, lo que permite utilizar plataformas como Dropbox o Google Drive para dejar instrucciones a los herederos (Santana y Franco, 2023)

Seguendo con la conceptualización del testamento digital Aguas (2022) mencionó que, en realidad, cuando se hace mención al testamento digital, es a un testamento tradicional que incluye nuestras posesiones digitales, la confusión surge porque algunas empresas utilizan incorrectamente los términos ‘legado digital’ o ‘testamento digital’, dando a entender que existe un tipo de testamento exclusivamente digital, lo cual es un error.

Se debe mencionar que un testamento tradicional es un documento legal que determina el destino de los bienes materiales de una persona después de su muerte, un testamento digital, en cambio, es un instrumento jurídico que permite a los usuarios especificar cómo desean que se administren sus activos digitales (como cuentas en línea, archivos digitales y criptomonedas) tras su fallecimiento, facilitando así la gestión de su legado digital por parte de sus herederos (Farooqui et al., 2022).

Cámara (2019 como se citó en Salazar y Marín, 2020) determinaron que el artículo 96 Ley Orgánica de Protección de Datos de Carácter Personales establece el derecho al testamento digital, todos los usuarios de internet, independientemente de su popularidad o actividad en línea, tienen derecho a decidir qué ocurre con sus datos personales después de su fallecimiento. Esto se justifica porque incluso los usuarios comunes generan valor para las plataformas digitales y merecen que sus datos sean tratados con respeto.

En torno a las plataformas digitales Canals y Hülkamp (2020) mencionaron que indudablemente, la concepción de la economía como un sistema complejo ha evolucionado significativamente, revelando la multitud de interacciones y los inesperados efectos que pueden surgir, especialmente en el contexto de las plataformas digitales. Cuestión que al 2024 es abordada por los derechos sucesorios.

Para Cucurull (2024a) el testamento digital es un documento legal integral para disponer de bienes y contenidos digitales no está plenamente reconocido, la figura del albacea digital en el ordenamiento español sí lo está, sin embargo, sus funciones son más específicas: se limita a gestionar los archivos y cuentas digitales del fallecido. El testador puede dejar instrucciones detalladas al albacea digital sobre cómo quiere que se manejen estos activos digitales, convirtiéndolo en un gestor especializado de la herencia digital.

Es propio definir quién es el albacea, para Contreras (2011 como se citó en Oropeza, 2023) establecieron que la denominación tiene un origen

histórico, es el encargado de administrar, cuidar y liquidar los bienes de una persona fallecida hasta que son entregados a sus heredero, su función es esencial para el correcto desarrollo del proceso sucesorio garantizando que la voluntad del testador se cumpla en su totalidad.

En la misma línea y conforme la regulación estadounidense *Fiduciary to Digital Assets Act* (2016), varios autores sugieren que un albacea es para protección y resguardo del testamento, es así que para Rosales (2016) el albacea digital es una figura clave para gestionar el legado digital, pero su nombramiento está estrictamente vinculado a un testamento tradicional, un testamento digital, como tal, no existe legalmente, el albacea digital se limita a gestionar los activos digitales hasta que el heredero legítimo los recibe.

Se enfatiza que el nombramiento de un albacea digital garantizará que los activos digitales del fallecido sean gestionados de manera adecuada y segura, evitando su pérdida o acceso no autorizado, al respetar el nombramiento del albacea digital al testamento tradicional, se respeta la voluntad del fallecido en cuanto a la disposición de sus bienes, tanto físicos como digitales.

En lo que respecta al testamento digital y los derechos de los herederos García (2021) precisa un caso denominado *Sentencia de Bundesgerichtshof*, este caso se situó en Alemania y se refiere al intento de los padres y herederos legales de una menor fallecida por acceder a su cuenta personal en la red social Facebook, según el sistema legal alemán, Facebook inicialmente se niega a proporcionar acceso, argumentando la protección de la privacidad de la cuenta, en este caso, surge un conflicto de intereses y derechos: la red social considera que debe prevalecer la privacidad de la persona fallecida.

Los herederos pueden continuar con la protección de los bienes, aunque con ciertas complicaciones legales como se evidencia en el caso, entonces es posible que la herencia digital contenga todo, tanto bienes digitales patrimoniales como las cuentas personas de redes sociales, es una discusión recurrente, porque muchas veces se estima que no debería heredarse las cuentas personales porque incluso colisionan con el derecho a la intimidad de la persona fallecida. Si bien es cierto no hay una normativa que impida poder dejar un testamento digital en América Latina, tampoco hay una que la respalda jurídicamente lo que resulta es una gran problemática a la hora de disponer de nuestros bienes digitales.

CONCLUSIONES

- Se definió que la herencia digital está conformada por un patrimonio netamente virtual de bienes digitales, estos son una amplia gama de activos virtuales, desde cuentas bancarias en línea hasta perfiles en redes sociales o cualquier información almacenada digitalmente, ya sea de carácter personal o económico, este nuevo tipo de herencia plantea desafíos inéditos a los sistemas jurídicos tradicionales.
- Se identificó que los digitales tienen una naturaleza jurídica compleja y diversa, no pueden ser clasificados de manera uniforme, su naturaleza jurídica depende de diversos factores, como su función, su valor y su relación con la identidad digital del individuo, pero la que más resalta es su naturaleza híbrida que combinan aspectos patrimoniales y personales.
- Se explicó la sucesión de bienes digitales en América Latina se encuentra en un estado de desarrollo heterogéneo y con lagunas legales, si bien algunos países han avanzado en la regulación de ciertos aspectos relacionados con los datos personales y la privacidad, aún no existe una normativa específica y uniforme que aborde de manera integral la transmisión hereditaria de los bienes digitales.
- Se estudió que la transmisión de bienes digitales post mortem es un desafío legal en constante evolución, la creciente importancia de los bienes digitales en la vida contemporánea ha puesto de manifiesto una laguna legal significativa: la falta de una regulación clara y uniforme respecto a su transmisión hereditaria, si bien numerosos autores han abordado esta temática, las conclusiones son diversas y aún persisten incertidumbres si existe o no un testamento digital.

REFERENCIAS BIBLIOGRÁFICAS

- Adriano, A., y Hernández, M. (2021). Testamento y herencia digital. *Enfoques jurídicos*, 4 (julio-diciembre), 120-136.
- Aguas, G. (2022). El testamento digital. *Revista de derecho aragonés*, 28, 65-90.
- Anatolyevna, E., Evgenyevich, O., Zulfugarzade, T., Vladimirovich, A., y Yashevich, A. (2020). El estado legal de los tokens y su herencia The legal status of tokens and their inheritance. *Jurídicas CUC*, 16(1), 287-302. <https://doi.org/10.17981/juridcuc.16.1.2020.12>

- Andrade, R., Ron, E., Ordoñez, A. O., y Ponce, R. (2023). Smart Contracts y Activos Digitales a la Luz del Derecho Sucesorio Ecuatoriano. *Mikarimin. Revista Científica Multidisciplinaria*, 9(1), Article 1.
- Argelich, C. (2023). *Testamento blockchainizado, bienes digitales extrapatrimoniales y herencia de activos digitales (NFT y criptomonedas) [Blockchain Wills, Digital Goods and Inheritance of Digital Assets (NFTs and Cryptocurrencies)]*. (SSRN Scholarly Paper No. 4607253). Social Science Research Network. <https://doi.org/10.2139/ssrn.4607253>
- Barroilhet, A. (2019). Criptomonedas, economía y derecho. *Revista Chilena de Derecho y Tecnología*, 8(1), 29. <https://doi.org/10.5354/0719-2584.2019.51584>
- Canals, A., y Hülkamp, I. (2020). *Plataformas digitales: Fundamentos y una propuesta de clasificación*. https://sga.unemi.edu.ec/media/archivomateria/2023/05/07/archivomaterial_202357104311.pdf
- Cárdenas, C. (2024). La Transmisión Por Causa De Muerte Del Patrimonio Digital. *Actualidad Jurídica Iberoamericana*, 20, 642-661. Scopus.
- Carta de la UNESCO para la Preservación del Patrimonio Digital. (2003). *UNESCO*. https://unesdoc.unesco.org/ark:/48223/pf0000229034_spa
- Castillo, M., y Palancares, L. (2010a). *Bienes Digitales | PDF | Monopolio | Mercado (economía)*. Scribd. <https://es.scribd.com/document/639203718/bienes-digitales>
- Castillo, M., y Palancares, L. (2010b). *La naturaleza de los bienes digitales, su competencia y estrategias para capturar valor*.
- Chiriboga. (2002). La acción de Habeas Data. *Iuris Dictio*, 3(5), Article 5. <https://doi.org/10.18272/iu.v3i5.571>
- Código Civil Peruano. (2015). *Ministerio de Justicia y Derechos Humanos*. https://spijlibre.minjus.gob.pe/content/publicaciones_oficiales/img/Codigo-Civil.pdf
- Constitución Política de la República de Chile. (1822). *Cámara de Diputadas y Diputados*. https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf

- Constitución Política del Perú. (1993). *Ministerio de Justicia*. <https://www.gob.pe/institucion/minjus/informes-publicaciones/4787525-constitucion-politica-del-peru-y-nuevo-codigo-procesal-constitucional>
- Cucurull, T. (2022). La sucesión de los bienes digitales (patrimoniales y extrapatrimoniales). *Revista de Derecho Civil*, 9(2), 313-338.
- Cucurull, T. (2024a). Herencia 2.0. Explorando los límites legales del testamento digital. *Anales de Derecho*, 41(1), Article 1. <https://doi.org/10.6018/analesderecho.556651>
- Cucurull, T. (2024b). Más allá de lo tangible: La herencia de los activos digitales. *Claves Jurídicas*, 1 (Enero-Junio), 49-67.
- Díaz, J. (2017). Patrimonio Digital. *Derechos en Acción*, 5(5), Article 5. <https://doi.org/10.24215/25251678e111>
- Farooqui, Sharma, y Gupta. (2022). INHERITANCE OF DIGITAL ASSETS: ANALYZING THE CONCEPT OF DIGITAL INHERITANCE ON SOCIAL MEDIA PLATFORMS. *Novum Jus*, 16(3), 413-435. Scopus. <https://doi.org/10.14718/NovumJus.2022.16.3.15>
- Fernández, C. (2017). *Derecho de sucesiones*. Fondo Editorial PUCP. <https://www.fondoeditorial.pucp.edu.pe/lo-esencial-del-derecho/497-derecho-de-sucesiones.html>
- Fiduciary to Digital Assets Act. (2016). *Uniform Law Commission*. <https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecd22>
- Gámez, M., y Corredor, J. (2023). NFT (token no fungibles) y sus implicaciones en el mercado de valores. *Derecho PUCP*, 90, Article 90. <https://doi.org/10.18800/derechopucp.202301.015>
- García, U. (2021). Herencia digital: Comentario a la Sentencia del Bundesgerichtshof alemán de 27.08.2020 (Urteil vom 12.07.2018, Az.: III ZR 183/17). *Derecom: Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías*, 31, 6.
- Ginebra, M. (2020). Voluntades digitales en caso de muerte. *CUADERNOS DE DERECHO TRANSNACIONAL*, 12(1), Article 1. <https://doi.org/10.20318/cdt.2020.5229>

- Goic, P., y Martínez, I. (2023). Digital estate and its protection in the chilean legal system. *Revista Republicana*, 2023(35), 93-109. Scopus. <https://doi.org/10.21017/rev.repub.2023.v35.a150>
- González, D. (2021). Los perfiles digitales después de la muerte, una perspectiva europea. *Estudios en derecho a la información*, 11 (Enero-junio 2021), 3-26.
- Hernandez, Fernández, y Baptista. (1997). *Metodología de la Investigación*. <https://josetavarez.net/Compendio-Metodologia-de-la-Investigacion.pdf>
- Ley 1581. (2012). *Función Pública*. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Ley de Protección de los Datos Personales. (2000). *Ministerio de Justicia*. <https://www.argentina.gob.ar/justicia>
- Ley Estatutaria 1266. (2008). *Secretaría Jurídica Distrital*. <https://intranet.secretariajuridica.gov.co/transparencia/marco-legal/normatividad/ley-1266-2008#:~:text=Descripci%C3%B3n%3A,y%20se%20dictan%20otras%20disposiciones>.
- Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados. (2017). *Cámara de Diputados*. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPSO.pdf>
- Ley N°12.965. (2014). *Ministerio Da Justiça*. https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei_na__12-965__de_23_de_abril_de_2014_espanhol_final-docx.pdf
- Ley N°13.709. (2018). *Presidencia da República*. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm
- Martínez, N. (2019). *Reflexiones en torno a la protección post mortem de los datos personales y la gestión de la transmisión mortis causa del patrimonio digital tras la aprobación de la LOPDGDD*. <https://doi.org/10.18042/cepc/dpc.35.05>
- Ordellin, J., y Oro, S. (2019). La disposición post mortem de los bienes digitales: Especial referencia a su regulación en América Latina. *Derecho PUCP*, 83, 29-60. <https://doi.org/10.18800/derechopucp.201902.002>

- Oropeza, D. (2023). El albacea provisional en el juicio sucesorio en el Estado de Veracruz. *Enfoques Jurídicos*, 08, Article 08. <https://doi.org/10.25009/ej.v0i08.2604>
- Otero, M. (2019). La sucesión en los «bienes digitales». La respuesta plurilegislativa española. *Revista de Derecho Civil*, 6(4 (octubre-diciembre)), 89-133.
- Pérez, M. (2010). *Derecho de familia y sucesiones*. Nostra Ediciones. <https://repositorio.uide.edu.ec/bitstream/37000/3993/1/-Derecho-de-Familia-y-Sucesiones-Mari-a-de-Montserrat-Pe-rez-Contreras-pdf-1-1.pdf>
- Rodríguez, R., y Martínez, F. (2018). Herencia digital, términos y condiciones de uso y problemas derivados de la praxis social. Un análisis desde la filosofía del derecho. *Revista Internacional de Pensamiento Político*, 12. <https://upo.es/revistas/index.php/ripp/article/view/3225>
- Romanowski, J., y de Oliveira, A. (2024). Testamento digital: Desafios e possibilidades no direito brasileiro. *Academia de Direito*, 6, 565-588. <https://doi.org/10.24302/acaddir.v6.4418>
- Rosales, F. (2016). Testamento digital. *Testamento ¿Digital?*, 2016, ISBN 978-84-617-4521-0, págs. 26-38, 26-38. <https://dialnet.unirioja.es/servlet/articulo?codigo=5625088>
- Salazar, J., y Marín, E. (2020). *Testamento electrónico y testamento digital en Colombia*. <https://alejandria.poligran.edu.co/handle/10823/2159>
- Santana, C., y Franco, W. (2023). HERANÇA DIGITAL: A (IM) POSSIBILIDADE DA TRANSMISSÃO DOS BENS DIGITAIS. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, 9(5), Article 5. <https://doi.org/10.51891/rease.v9i5.9996>
- Santos, M. (2018). La denominada “herencia digital”: ¿necesidad de regulación? Estudio de Derecho español y comparado. *Cuadernos de derecho transnacional*, 10(1), 413-438.

VACÍOS JURÍDICOS EN LAS NORMATIVAS LATINOAMERICANAS QUE REGULAN EL TELETRABAJO: SALUD MENTAL Y POSIBLES RIESGOS LABORALES

Ana Lucía Gil-Morey ¹

RESUMEN

Esta investigación tuvo por objetivo determinar los riesgos físicos y mentales producto de la modalidad del Teletrabajo. El tipo de investigación es básica con un diseño no experimental - descriptivo. Los principales resultados conllevan a determinar que existe una vinculación entre la salud mental de un trabajador y la modalidad de trabajo remoto, asimismo se verificó las deficiencias en las legislaciones latinoamericanas que regulan el teletrabajo y los posibles riesgos laborales que su adopción conlleva. Finalmente se concluye que el análisis de las normativas que regulan el teletrabajo ha revelado importantes vacíos legales en la protección de la salud mental de los teletrabajadores.

Palabras Clave: *Riesgos laborales, salud mental, prevención, regulación, teletrabajo.*

¹ agilm3@upao.edu.pe

Programa de Estudio de Derecho, Universidad Privada Antenor Orrego

ABSTRACT

This research aimed to determine the physical and mental risks associated with the telework modality. The type of research is basic with a non-experimental descriptive design. The main results lead to the conclusion that there is a connection between a worker's mental health and the remote work modality. Additionally, deficiencies in Latin American legislation regulating telework and the potential occupational risks associated with its adoption were identified. Finally, it is concluded that the analysis of the regulations governing telework has revealed significant legal gaps in protecting the mental health of teleworkers.

Keywords: *Occupational risks, mental health, prevention, regulation, telework.*

INTRODUCCIÓN

Desde el año 2000, se ha evidenciado un avance tecnológico masivo con la implementación de medios digitales en el ámbito laboral, ello implica que se encuentra al alcance de las personas una computadora o un celular que permite la comunicación directa la mayor parte del tiempo, por lo que basta estar conectado a una red de internet para interactuar con personas de todo el mundo, no siendo un límite el espacio - tiempo. Tal es así que, no es una sorpresa que existan nuevas modalidades virtuales para realizar ciertas actividades en particular, como trabajar desde la comodidad del hogar

La implementación del teletrabajo permite que un empleado realice sus funciones desde cualquier lugar, sin necesidad de estar presente en un espacio físico de trabajo y que, a pesar de esta flexibilidad, se mantiene la relación laboral, donde el trabajador sigue bajo la supervisión del empleador y recibe una remuneración por su trabajo (Pintado & López, 2022). Es por ello que, para hablar de este tipo de modalidad laboral, el teletrabajador tiene que conocer las funciones específicas que va a realizar, esto de manera regular como habitual, entendiéndose que no necesita estar físicamente presente en el lugar de trabajo para llevarlas a cabo.

El teletrabajo y lo que conlleva su regulación no es un tema relativamente nuevo. Tal es así que, el 5 de junio de 2003, en el Perú se aprobó la Ley N°. 30036, conocida como la Ley del Teletrabajo, que integró esta modalidad en la legislación laboral, donde el empleado podría realizar sus tareas en un lugar diferente al centro de trabajo utilizando herramientas tecnológicas de comunicación para llevar a cabo sus actividades, estando sujeto a una supervisión o fiscalización. En tal implementación, la normativa peruana establece que el empleador debe proporcionar los equipos y herramientas

para trabajar desde casa, pero el empleado es responsable de usarlos y cuidarlos (Vega et al., 2022).

En el año 2020, con la propagación del sars – cov – 2 (COVID-19) a nivel mundial, donde millones de personas se vieron en la obligación de estar confinadas, el teletrabajo cobró una mayor importancia como una forma virtual; sobre todo, revolucionaría de empleo, llegando a redefinir la relación entre empleados. Es relevante mencionar que, el auge del teletrabajo se debió a la mencionada crisis sanitaria, con la finalidad de mejorar la flexibilidad laboral.

Para ese entonces, permanecer en un ambiente laboral cerrado implicaría un contagio masivo. Tal es así que, se tenía que evitar la concentración masiva de personas; asimismo, disminuir el tiempo y los gastos relacionados al desplazamiento, y ofrecer a los empleados un mayor control sobre su entorno de trabajo, por tal motivo se establecieron sistemas de teletrabajo como medidas obligatorias para salvaguardar el bienestar de los empleados y seguir trabajando cuando fuera posible (Carrizosa-Prieto, 2022). Ante la crisis, se convirtió en una forma de resolver las necesidades de los teletrabajadores y tele-empresarios (García *et al.*, 2019).

En definitiva, el teletrabajo cuando se combina con la tecnología permite una separación laboral al facilitar la comunicación a través de los distintos niveles dentro de una empresa. La mencionada tecnología y plataformas de comunicación digital permiten gestionar la información necesaria para el trabajo, incluyendo dispositivos como computadoras, laptops, smartphones y tabletas (Santillan, 2020).

El teletrabajo brinda muchas ventajas, pero también plantea desafíos importantes que impactan tanto a los empleados como a la comunidad en general, uno de ellos sería el impacto que tal modalidad ocasiona en la salud mental de los trabajadores. Si bien es cierto, es complicado definir este término como tal, ello está relacionado con los trastornos mentales, los problemas psicosociales y el bienestar general, dichos enfoques y prácticas se basan en distintas perspectivas de salud; por lo tanto, la manera en que se entiende y se aborda la salud mental varía según las teorías (Restrepo & Jaramillo, 2012).

Es relevante mencionar que esta modalidad virtual de trabajo también trae consigo aspectos negativos, uno de ellos es la sensación de estar siempre conectado. Es por ello que se puede decir que, la revolución digital ha

borrado las fronteras entre el trabajo y la vida personal, haciendo difícil separar el tiempo de trabajo del tiempo libre (Rubio & Barrera, 2024).

Esta modalidad ha generado nuevas formas de estrés como el aislamiento social, la dificultad para lograr una distinción clara entre el trabajo y la vida personal; por esta razón, la atención a la salud mental se ha convertido en una preocupación cada vez mayor en el ámbito laboral actual, aspectos como la falta de interacción con los colegas del entorno laboral, la presión para mantener la productividad sin la supervisión directa, y la dificultad para desconectar del trabajo pueden contribuir a un aumento en los niveles de ansiedad, estrés y agotamiento entre los teletrabajadores. Por tanto, es crucial abordar cómo el teletrabajo influye en el bienestar psicológico.

Esta investigación tiene como objetivo analizar los trastornos mentales y el deterioro de la salud mental que puede ocasionar el teletrabajo respecto a su implementación masiva, asimismo si la legislación peruana protege la salud mental de los teletrabajadores, además de las ventajas y desventajas que conlleva el trabajo remoto.

METODOLOGÍA

Según su objeto de estudio, esta investigación es de tipo básica, debido a que parte de un tema específico y se relaciona con el mismo, es por ello que la investigación realizada crea nuevos conocimientos a partir de uno ya conocido (Sanca, 2011). Asimismo, de acuerdo con el tipo de información que se recopila para abordar la cuestión de investigación, esta es de tipo cualitativo, la cual se caracteriza por combinar técnicas de recolección de datos, en donde el investigador participa activamente en la recopilación de información, siendo su propósito identificar las relaciones y significados asociados al fenómeno investigado.

Así, se realizó una técnica de revisión conceptual y bibliográfica, la cual requirió una búsqueda de material relacionado con el glosario de: trabajo digital, regulación normativa, salud mental y riesgos laborales. De esta forma se pudo obtener información documental relacionada con el tema de investigación, obteniéndose en un primer momento resultados generales, de los cuales se fueron descartando y, por ende, seleccionando de manera específica; ello con la finalidad de lograr un acercamiento al tema del teletrabajo en cuanto a las deficiencias de su regulación en Latinoamérica

Ante ello, se necesitó realizar una revisión exhaustiva de los artículos seleccionados para verificar que la información respondiera a las preguntas

de investigación que se establecieron, de los cuales se utilizó algunos como: *Implicación del Teletrabajo en Ecuador*, *Gestión de riesgos laborales en el Trabajo Móvil*, entre otros.

Los mismos que establecen bases para poder reconocer cuales son los tipos de riesgos laborales y los vacíos que presentan las diversas regulaciones que establecen el teletrabajo en relación con la protección de la salud mental de los empleados. Finalmente, los artículos se obtuvieron de la base de datos de Scopus, Redalyc, Dialnet y Doaj, siendo fuentes de información aprobadas por los rigurosos parámetros de las revistas.

RESULTADOS

1. Deterioro de la salud mental de los teletrabajadores

A raíz de la pandemia ocasionada por el virus SARS CoV 2 (COVID 19), se implementó en distintos países de Latinoamérica el teletrabajo, siendo una medida para evitar el contagio masivo. Al ser una modalidad relativamente nueva, se desconocía los desafíos que su regulación enfrentaba, lo que implicaba la condición de salud tanto mental, como física de los teletrabajadores presentándose riesgos psicosociales y ergonomía puesto que, a diferencia del teletrabajo habitual, los empleados tenían jornadas más largas, aumentándole la ansiedad y afectando su salud (Vega et al., 2022).

Al revisar la literatura, se puede evidenciar que, al no diferenciarse el centro de trabajo con el hogar, al ser el mismo espacio, podría generar riesgos psicosociales; es por ello que, el uso desmedido de la tecnología está borrando cada vez más la separación entre la vida personal y profesional de los empleados provocando que los límites entre el tiempo dedicado al trabajo y el destinado al descanso se vuelvan cada vez más difusos. Esto genera una situación en la que el trabajo ocupa todo el tiempo, impidiendo que el trabajador disfrute de un verdadero periodo de descanso y recuperación personal (Rubio & Barrera, 2024).

Si bien es cierto, el teletrabajo puede resultar ventajoso para disminuir gastos dentro de una empresa; sin embargo, no siempre la salud de sus empleados es una prioridad. Entre las afecciones que se pueden presentar se encuentran los dolores músculo esqueléticos causado por posturas inadecuadas, asimismo fatiga visual ocasionada por el uso excesivo de las pantallas digitales, llegando a causar irritación visual; así, esta modalidad

puede ocasionar en el trabajador deterioro físico cuando el entorno de trabajo no es el más adecuado para realizar sus tareas laborales (Santillan, 2020).

El teletrabajo puede aumentar la ansiedad, el estrés y la fatiga en los empleados, lo que ocurre especialmente cuando las condiciones laborales y las demandas cognitivas no se alinean con las necesidades del empleado. Así, esta modalidad puede ocasionar deterioro mental en los teletrabajadores, pese a las ventajas que la misma modalidad ofrece; es por ello que, es fundamental que las empresas presten atención a factores como la fatiga y la carga laboral, implementando medidas de prevención y seguimiento para proteger la calidad de vida de los teletrabajadores (Martínez et al., 2020).

Trabajar en estas plataformas sugiere independencia y flexibilidad por la misma naturaleza de la modalidad, sin embargo, los bajos salarios y la subordinación generan una necesidad de trabajar excesivamente para asegurar sus ingresos. El estrés también puede ser provocado por el temor que pueden sentir los teletrabajadores a perder su empleo, lo que aumenta su dependencia a su puesto de trabajo, limitando su capacidad para hacer reclamos; de esta manera, generando mayor inestabilidad emocional (Ramírez & Aguilar, 2022).

La literatura señala que la adopción del teletrabajo puede generar diversos problemas, tales como el aislamiento social, la sensación de estancamiento en el desarrollo profesional, tensiones familiares y una mayor percepción de carga laboral; además, existen riesgos potenciales para la salud física, como el sedentarismo, la falta de ejercicio y la alteración de los hábitos alimenticios (Martínez et al., 2020). Lo cual puede recaer en trastornos de la conducta alimentaria, siendo esta una enfermedad mental y física que mayormente se desarrolla en mujeres.

Por otro lado, a diferencia de algunos países de Latinoamérica que han incluido el teletrabajo en sus legislaciones, Ecuador ha dado un paso importante al reconocer el derecho de los teletrabajadores a la desconexión. Esta ley establece un periodo mínimo de 12 horas de descanso dentro de cada ciclo de 24 horas, lo que asegura que los empleados tengan un tiempo adecuado para desconectarse de sus responsabilidades laborales (Pérez, 2021).

Es relevante mencionar que, con el avance tecnológico es necesario adaptar las mismas a un contexto social; en este caso, a un ambiente laboral. Un

país no puede permitirse rezagarse en la adopción de tecnologías que favorezcan la mejora de la calidad de vida laboral de personas que no pueden trabajar 8 horas diarias presencialmente; por ejemplo, las mujeres que se dedican exclusivamente a las responsabilidades del hogar.

Las empresas deben promover un entorno de trabajo virtual en el que los empleados se sientan apoyados, valorados y escuchados; asimismo, organizar reuniones frecuentes, tanto de carácter profesional como más relajado, puede contribuir a mantener un espíritu de comunidad y cooperación. Además de establecer espacios virtuales para la interacción social, como chats grupales o encuentros informales, puede ayudar a disminuir el aislamiento y reforzar las relaciones entre los miembros del equipo.

Es esencial que las organizaciones proporcionen recursos para respaldar la salud mental de sus empleados, esto podría incluir servicios de asesoría psicológica o programas para el manejo del estrés, donde los teletrabajadores tengan acceso a profesionales de la salud mental. Además, las empresas pueden ofrecer talleres de mindfulness o técnicas de relajación para ayudar a los empleados a gestionar la ansiedad y el estrés de forma eficaz.

Los teletrabajadores pueden experimentar una mayor presión si no tienen una comprensión clara de las expectativas o si no reciben retroalimentación adecuada sobre su rendimiento. Por ello, las empresas deben establecer objetivos realistas, así como ofrecer retroalimentación constructiva y apoyo continuo; esto contribuye a disminuir la incertidumbre; como la ansiedad y fortalece la confianza del empleado en su trabajo.

2. Deficiencias en las legislaciones latinoamericanas que regulan el teletrabajo

En diversos ordenamientos jurídicos, el teletrabajo no fue objeto de regulación específica hasta épocas relativamente recientes; al no ser una figura utilizada con frecuencia dentro de las legislaciones de Latinoamérica, se descuidaron muchos aspectos importantes para la protección de los teletrabajadores. Durante la pandemia, esta falta de previsión normativa motivó que muchos países tuvieran que abordar su implementación de manera urgente y, en muchos casos, de forma incompleta (Carrizosa, 2022).

Al adoptarse principalmente como respuesta a necesidades urgentes derivadas de la pandemia del COVID-19, como ya se mencionó anteriormente, la implementación estuvo más centrada en cumplir con

demandas inmediatas que en una comprensión profunda del impacto y las características esenciales del teletrabajo. Se reconoce como uno de los principales obstáculos para la implementación del teletrabajo, el desconocimiento que tienen los directivos sobre el concepto y la verdadera naturaleza de esta modalidad laboral (Intriago & Cedeño, 2022).

Es así como los teletrabajadores se encuentran expuestos a mayores riesgos en términos de seguridad, salud y protección social, en comparación con los trabajadores del sector formal, aceptando remuneraciones más bajas, entre otras desventajas. Esta modalidad de trabajo ha puesto en evidencia las condiciones precarias de quienes laboran en el sector informal, particularmente aquellos considerados como contratistas autónomos, quienes quedan excluidos de la protección que brindan las leyes laborales (Pintado & López, 2022).

Es crucial establecer una regulación adecuada para el teletrabajo como una forma de legítima prestación de servicios, especialmente en el contexto actual de una sociedad digitalizada, es decir, como una institución dentro de los sistemas laborales. A pesar de que algunos países disponían de marcos normativos preexistentes, estos no fueron aplicados con la magnitud anticipada o, en ciertos casos, no se implementaron en absoluto, debido a una serie de factores contextuales; tal es así que, se han podido vulnerar los derechos laborales de los teletrabajadores.

Las personas que tienen la necesidad de laborar en este sistema, muchas veces no cuentan con todos los recursos para llevar a cabo sus funciones. Tal es así que, el teletrabajo ha evolucionado, pasando de ser una modalidad en la que se cumplen ciertos requisitos contractuales, como el suministro de herramientas y equipos, el acceso a redes y telecomunicaciones, y la adecuación de los espacios laborales en términos de prevención de riesgos, a una nueva forma de “trabajo en casa” (Idárraga *et al.*, 2020).

Así, el teletrabajo en el Perú fue formalizado como una modalidad específica, lo que permitió a los tele-empresarios, disponer a sus empleados desempeñar sus actividades laborales bajo un régimen de subordinación desde sus hogares o lugares de aislamiento. Con la Ley del Teletrabajo (Ley N°31572), se habilitó el uso de cualquier medio o mecanismo que facilitara la realización de las tareas fuera de las instalaciones laborales, implementando también que es el empleador el encargado de proporcionar las herramientas necesarias.

En la Ley mencionada en el anterior párrafo no se menciona explícitamente el cuidado directo de la salud mental de los teletrabajadores. Sin embargo, algunos de los artículos abordados en los capítulos sobre seguridad y salud en el teletrabajo podrían implicar medidas relacionadas indirectamente con la salud mental al centrarse en aspectos que afectan el bienestar general de los trabajadores.

Ante ello, se considera necesario que en la Ley N°31572 se establezca, por lo que la misma debería modificarse, en el capítulo V SALUD Y SEGURIDAD DEL TELETRABAJO, específicamente los aspectos de la salud de los teletrabajadores se protegen, no solamente físicamente, sino también la mental; pues si una persona no se encuentra estable emocionalmente, no podrá laborar de manera eficiente, al contrario, el estrés constante del trabajo sometido a esta modalidad, podría acabar colapsando sus emociones y si ello no se resguarda, el empleador podría cometer abusos.

En la misma línea de lo antes desarrollado, resulta complejo identificar con certeza el origen de muchas enfermedades, a veces no se sabe exactamente qué las causa; la normativa uruguaya para manejar esta incertidumbre utiliza un listado que enumera las enfermedades que se consideran oficialmente como enfermedades profesionales, las mismas que podrían desarrollarse con la modalidad del teletrabajo. No obstante, es importante señalar que lo establecido en esa normativa no constituye una lista exhaustiva (Garmendia, 2023).

En Colombia, finalmente se promulga en el año 2022, la Ley de desconexión laboral (Ley N°2191) que establece el derecho a la desconexión laboral, aplicable a todas las modalidades de trabajo, lo cual marca un hito importante porque también aplica para el teletrabajo. Por otro lado, el teletrabajo fue implementado como una modalidad de carácter excepcional, temporal y ocasional, lo que permitió a los empleadores recurrir a esta opción junto con otras medidas alternativas, tales como la reducción de la jornada laboral o la anticipación de las vacaciones (Carrizosa-Prieto, 2022).

Asimismo, la legislación laboral ecuatoriana ha incorporado el derecho a la desconexión digital en la última reforma al Código del Trabajo, no obstante, su implementación, al igual que los países antes mencionados, enfrenta varios retos; uno de los principales problemas es la falta de claridad en cuanto a la definición precisa de las horas laborales efectivas (Rubio & Barrera, 2024). Ello implica una gran deficiencia en la normativa

establecida debido a que, al generarse esta incertidumbre, el empleador podría abusar del horario de trabajo de sus teletrabajadores, obligándolos a trabajar horas extras sin ser remuneradas.

Existen deficiencias respecto a la salvaguarda de la salud mental en las legislaciones que regulan el teletrabajo lo cual ha quedado evidenciado. Sin embargo, también existen otras dificultades, ello también se refleja en la ausencia de guía tanto por parte de los trabajadores como de las entidades encargadas de la gestión de riesgos laborales, que no tienen en cuenta a los teletrabajadores dentro de las protecciones incluidas en los seguros empresariales y como resultado, los teletrabajadores quedan desprotegidos en cuanto a la seguridad y el bienestar en su entorno laboral doméstico (Cataño & Gómez, 2014).

3. Posibles riesgos en la salud y laborales ocasionados por el Teletrabajo

Suele haber una falta de protección social, contratos formales, salarios bajos y poca posibilidad de organización o acción colectiva para defender los derechos de los trabajadores. Así, existen varios problemas derivados del cambio repentino del trabajo presencial al trabajo digital debido a la pandemia, el trabajo en la economía de plataformas digitales ha sido especialmente criticado por generar condiciones laborales precarias. Diferentes estudios han señalado que este tipo de trabajo aumenta la vulnerabilidad de los trabajadores, especialmente en países con salarios bajos, como China o la India (Ramírez & Aguilar, 2022).

Así, realizar las mismas tareas en menos tiempo genera fatiga o incluso problemas de salud, usualmente ocurre cuando el trabajo remoto o digital no está bien organizado. Es por ello que, en este tipo de modalidad surgen problemas al trabajar en un entorno digital o en plataformas, especialmente cuando aumenta la carga de trabajo debido a una mayor productividad. A medida que la productividad crece, también puede incrementarse la cantidad de trabajo que realiza la persona, lo que puede generar estrés o agotamiento (Martínez *et al.*, 2020).

Los trabajadores que realizan sus tareas desde casa están expuestos a varios factores que pueden afectar su salud, tanto física como mental, incluidos factores psicosociales y ergonómicos, además, la falta de interacción social con compañeros de trabajo puede conducir a la soledad laboral. Los teletrabajadores pueden experimentar dificultades relacionadas con el

estrés, la falta de interacción social o la presión laboral, lo que impacta su bienestar psicológico y físico (Peña *et al.*, 2022).

Al revisarse la literatura sobre los riesgos laborales asociados al teletrabajo, los factores de riesgo ergonómicos están asociados con la posición del cuerpo, y el ambiente de trabajo y los psicosociales, como el estrés o el aislamiento social, son los más evaluados en la gestión de riesgos. Sin embargo, en el caso del teletrabajo móvil, cuando el trabajo se realiza desde distintos lugares, no necesariamente desde casa o una oficina fija, los factores de riesgo locativos, es decir, aquellos relacionados con el entorno físico donde se trabaja, podrían tener un mayor impacto en la salud del trabajador (Guarin-Arciniegas *et al.*, 2021).

En la línea de lo antes desarrollado, estos riesgos pueden impactar tanto la salud física como la psicológica del trabajador. El teletrabajo al ser principalmente una actividad cognitiva implica estar sentado frente a una pantalla durante largos períodos, lo que puede llevar a problemas de sedentarismo, que en realidad es propio de la naturaleza de la modalidad. Asimismo, se presentan dificultades para equilibrar la vida familiar y laboral, debido al aumento del tiempo dedicado al trabajo.

En los últimos años, se ha registrado una intensificación en los factores de riesgo psicosocial en los ambientes laborales. De acuerdo con los resultados de la tercera edición de la Encuesta Europea a Empresas sobre Riesgos Nuevos y Emergentes, realizada en 2019, uno de los riesgos más destacados en el ámbito laboral es el psicosocial. Hasta el 60% de los empleados informan síntomas como estrés, derivados de la necesidad de enfrentar situaciones con clientes, pacientes o estudiantes complicados (Pérez *et al.*, 2023).

Tal es así que, mientras que los riesgos ergonómicos y psicosociales son los más comunes en el teletrabajo tradicional, en el teletrabajo móvil surgen otros factores relacionados con el entorno cambiante de trabajo, que pueden tener efectos importantes en la salud de los empleados.

El estrés cuando se prolonga en el tiempo, puede estar vinculado a una serie de problemas de salud como fatiga constante, depresión y ansiedad. De los riesgos que se pueden producir en la salud, el estrés, siendo una reacción del cuerpo ante diversas circunstancias o factores, provocan estrés tanto a nivel mental, físico como emocional. Este fenómeno está relacionado con problemas como la fatiga, la depresión, la ansiedad y otras condiciones de

salud que pueden dificultar que una persona cumpla con sus actividades diarias (Benítez, 2024).

Es así que, el impacto del estrés no se limita solo a la salud física, también puede afectar el bienestar emocional y social, por lo que la irritabilidad puede aumentar, afectando las relaciones personales y laborales. Por lo tanto, los altos niveles de estrés, especialmente cuando no se gestionan adecuadamente, pueden deteriorar la calidad de vida de la persona, el bienestar emocional y las relaciones interpersonales.

En la misma línea de lo antes desarrollado, el estrés laboral se entiende como una respuesta adversa que se produce cuando las exigencias laborales exceden la capacidad de la persona para manejarlas, lo que provoca un deterioro en su salud y da lugar a síntomas de enfermedad y fatiga.

El síndrome de Burnout, también denominado agotamiento profesional, sobrecarga emocional, síndrome del quemado o fatiga laboral, fue reconocido en el año 2000 por la Organización Mundial de la Salud como un factor de riesgo relacionado con el entorno de trabajo (Saborío & Hidalgo, 2015). Esto se debe a su impacto en la calidad de vida, la salud mental y, en algunos casos, a su capacidad para poner en peligro la salud física del individuo afectado. Si bien es cierto, este tipo de afectación emocional se desarrolla en ambientes de oficina, podría también desarrollarse en la modalidad del teletrabajo.

La falta de una normativa adecuada que regule los riesgos laborales relacionados con la salud mental podría tener consecuencias serias tanto para los trabajadores como para las empresas. Sin una regulación clara y específica, los trabajadores estarían expuestos a un entorno laboral que no gestiona correctamente los factores de riesgo psicosocial, como el estrés crónico, la excesiva carga de trabajo y la carencia de apoyo social, o la presión constante, lo que podría desencadenar trastornos mentales como ansiedad, depresión o agotamiento severo (burnout).

Desde una perspectiva empresarial, no regular estos riesgos podrían aumentar las tasas de absentismo laboral, asimismo generar menor productividad, debido a que si los empleados enfrentan dificultades psicológicas severas pueden optar por abandonar sus puestos o ausentarse por problemas de salud. Además, la negligencia en el cuidado del trabajo puede deteriorar el clima laboral.

4. Medidas que adoptan o deberían adoptar las empresas para prevenir riesgos laborales

La prevención de riesgos laborales a lo largo del tiempo ha evolucionado, destacando su desarrollo en relación con el contexto organizacional. A lo largo de la historia, las sociedades, tanto antiguas como modernas, se ha observado una falta de interés en la salud y seguridad de los trabajadores, no obstante, la importancia de proteger su bienestar comenzó a reconocerse durante la Segunda Guerra Mundial (García *et al.*, 2019).

La adopción del teletrabajo, que depende exclusivamente de herramientas tecnológicas, requiere una mayor organización por parte del empleador, así como una inversión significativa en infraestructura y una protección más rigurosa de la información. Este modelo exige que las empresas minimicen los riesgos relacionados con la seguridad de los datos, lo que implica destinar recursos económicos para gestionar redes seguras, garantizar el uso adecuado de correos electrónicos, dispositivos y equipos, y asegurar los datos en servidores (Vega *et al.*, 2022).

En el caso del teletrabajo, los empleados pueden aumentar su seguridad si se ven a sí mismos como responsables de la misma, actuando de manera proactiva. Los accidentes laborales pueden prevenirse en cualquier tipo de entorno de trabajo si se modifican los comportamientos de los empleados. Esto implica trabajar en aumentar la conciencia sobre los riesgos, cambiar actitudes, cuestionar creencias equivocadas y corregir situaciones que puedan generar peligros (Martínez *et al.*, 2020).

Es imprescindible implementar estrategias preventivas para salvaguardar a los trabajadores de los riesgos laborales, con el propósito de prevenir accidentes y enfermedades que puedan impactar su salud y bienestar, para lograr esto, los empresarios deben centrarse en implementar medidas de seguridad y salud en el trabajo, siguiendo las leyes y regulaciones pertinentes, y evaluando los riesgos presentes en el entorno laboral (Bernal *et al.*, 2017).

Tomar medidas no solo asegura la productividad y la eficiencia del teletrabajo, sino que también protege la salud y el bienestar de los empleados. Para implementar el teletrabajo, el empleador debe tomar varias políticas para garantizar que el trabajo a distancia sea seguro y eficiente para los empleados, por ende, es necesario establecer las características y responsabilidades de los puestos de trabajo, lo que significa que el empleador debe aclarar las funciones de cada puesto del teletrabajo (Pintado & López, 2022).

Es fundamental que las empresas implementen mecanismos para gestionar y controlar de manera eficaz el resguardo anticipado de los equipos de computación. Así, las empresas deben efectuar análisis periódicos para reconocer los factores de riesgo que puedan impactar el entorno laboral. Estos estudios permitirán comprender mejor los peligros a los que están expuestos los empleados que trabajan desde ubicaciones variables, ya sea desde su hogar, cafeterías o espacios compartidos (Guarin-Arciniegas *et al.*, 2021).

En la línea con lo antes desarrollado, las organizaciones deben asegurarse de que los teletrabajadores tengan acceso a un soporte técnico adecuado en caso de problemas, así como protocolos de seguridad cibernética para proteger la información sensible. Es importante igualmente que se proporcionen herramientas y recursos para que los trabajadores puedan crear un espacio de trabajo físico apropiado, sin elementos de riesgo para la salud, como ergonomía y medidas de protección eléctrica.

En este sentido, las acciones que se desarrollan deben estar centradas en la preservación de la salud y el bienestar de los trabajadores, tanto a nivel físico como psicológico. Esto implica adaptar los planos de seguridad y salud para incluir no sólo los riesgos laborales, debido a que el programa y el plan de trabajo del área de seguridad y salud en el trabajo deben contemplar a todos los empleados, tanto a aquellos que trabajan de manera presencial como a los que realizan sus funciones en modalidad de teletrabajo, asegurando que ambos grupos reciban una protección integral (Cataño & Gómez, 2014).

Es fundamental que el plan contemple la adaptación de todos los elementos necesarios para un funcionamiento óptimo del teletrabajo, desde la ergonomía y el uso adecuado de equipos, hasta la implementación de estrategias de prevención adecuadas. En este punto, el papel de la psicología organizacional cobra una relevancia especial, los trabajadores remotos pueden estar expuestos a riesgos psicológicos específicos, como el estrés laboral, la ansiedad y la soledad.

El uso frecuente de plataformas digitales, redes sociales y herramientas de comunicación en línea puede aumentar la vulnerabilidad a ataques informáticos como phishing o robo de identidad. En el estudio relacionado con la protección de la información y la confidencialidad, se recomienda aplicar medidas para mantener al personal docente informado sobre los peligros asociados al uso de internet, fomentando hábitos de protección y cautela contra el robo de datos e información personal (López-Paz *et al.*, 2024).

En relación con la seguridad y salud en el trabajo, se sugiere continuar brindando información constante al personal sobre las acciones preventivas para minimizar los peligros laborales y prevenir accidentes. Es por ello que, la protección de datos y la salud laboral deben ser áreas prioritarias en el desarrollo de políticas para el profesorado, especialmente en un entorno donde la tecnología desempeña un papel crucial en las tareas diarias.

Para proteger la información sensible durante el teletrabajo, las empresas deben exigir que los teletrabajadores utilicen redes privadas virtuales (VPN) cuando se conecten a Internet; las VPN cifran la conexión, garantizando que los datos enviados y recibidos estén protegidos de accesos no autorizados. Esto es particularmente importante cuando los empleados trabajan desde lugares públicos o redes Wi-Fi no seguras, que son propensas a ser atacadas.

Las empresas deben definir políticas específicas sobre el uso de dispositivos destinados al teletrabajo, tales como laptops, teléfonos móviles y otros equipos electrónicos. Es crucial que los dispositivos proporcionados por la empresa cuenten con software de seguridad actualizado, como programas antivirus y firewalls. Además, es necesario implementar un control riguroso sobre el acceso a estos dispositivos, limitando su utilización únicamente a las tareas laborales. En caso de pérdida o robo de algún dispositivo, la empresa debe contar con procedimientos establecidos para bloquear el acceso a la información confidencial almacenada en él.

CONCLUSIONES

- El análisis de las normativas latinoamericanas que regulan el teletrabajo ha revelado importantes vacíos legales en la protección de la salud mental de los teletrabajadores. Si bien la implementación del teletrabajo ha ganado impulso desde la pandemia de COVID-19, las legislaciones actuales no han evolucionado lo suficiente para abordar de manera integral los riesgos psicosociales y ergonómicos que enfrenta esta modalidad laboral.
- El estudio demuestra que, aunque algunos países han dado pasos positivos, como Ecuador con la ley de desconexión digital, la mayoría de las normativas se enfocan en aspectos físicos del entorno laboral y dejan de lado la salud mental. Esta falta de cobertura adecuada provoca que los teletrabajadores se enfrenten a desafíos como el estrés crónico, la ansiedad, la fatiga y el aislamiento social, que impactan negativamente tanto en su bienestar como en su productividad.

- Es esencial que los legisladores revisen y amplíen los marcos normativos existentes para incluir políticas específicas que protejan la salud mental de los teletrabajadores. Las empresas también deben asumir un papel más activo en la prevención de riesgos laborales, implementando como el acceso a servicios de salud mental, talleres de manejo de estrés y programas de apoyo psicosocial.
- El teletrabajo requiere un enfoque integral que no solo contemple la provisión de equipos y tecnología, sino que asegure la creación de un entorno laboral equilibrado, respetando los límites entre la vida personal y profesional. Sin estas mejoras, las condiciones laborales de los teletrabajadores continuarán siendo precarias, lo que podría afectar tanto su desempeño como el clima laboral en general.
- Así, la revisión académica destaca la importancia de la regulación continua y adaptada a las transformaciones digitales y sociales, para que el teletrabajo sea una modalidad sostenible y beneficiosa tanto para los empleados como para los trabajadores.

REFERENCIAS BIBLIOGRÁFICAS

- Benítez, D. (2024). Impacto del teletrabajo en el estrés laboral de docentes universitarios por el covid-19. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, 14(28). <https://doi.org/10.23913/ride.v14i28.1781>
- Bernal, A., Ordoñez, J., y Quintero, M. (2017). Diseño de la fase del planear de un sistema de gestión de seguridad y salud en el trabajo. *Revista Colombiana de Salud Ocupacional*, 7(2), 72-78. <https://www.redalyc.org/journal/7337/733776354006/>
- Carrizosa-Prieto, E. (2022). La Regulación Del Teletrabajo Estructural En Iberoamérica. *Archivos de Prevención de Riesgos Laborales*, 25(2), Article 2. <https://doi.org/10.12961/aprl.2022.25.02.08>
- Cataño, S. L., y Gómez, N. E. (2014). El concepto de Teletrabajo: Aspectos para la Seguridad y Salud en el Empleo. *CES Salud Pública*, 5(1), Article 1. https://revistas.ces.edu.co/index.php/ces_salud_publica/article/view/2772

- García, L. M., Guerrero, H., y Jiménez, E. A. (2019). Condiciones de Seguridad y Salud en el Trabajo de los Teletrabajadores: Revisión Sistemática. *Pensamiento Americano*, 12(23), 94-104. <https://doi.org/10.21803/pensam.v12i22.249>
- Garmendia, M. (2023). La regulación del teletrabajo (ley n° 19978, de 20 de agosto de 2021 y dec. N° 86/022, de 17 de marzo de 2022). *Revista de la Facultad de Derecho*, 55. <https://doi.org/10.22187/rfd2023n55a1>
- Guarín-Arciniegas, I. Y., Gómez-Romero, S. I., Uribe-Montaña, S. L., y Vergel-Vila, L. C. (2021). Gestión de riesgos laborales en el Teletrabajo Móvil. *ORINOQUIA*, 25(1), 95-101. <https://www.redalyc.org/journal/896/89669917008/>
- Idárraga, A. M., Ramírez, C., y González, A. (2020). El teletrabajo desde la perspectiva de la salud laboral. *Poliantea*, 15(26), 73-74. <https://dialnet.unirioja.es/servlet/articulo?codigo=7629795>
- Intriago, C. P., y Cedeño, M. M. (2022). Teletrabajo e incidencia en el clima organizacional del Instituto Ecuatoriano de Seguridad Social, administración Portoviejo. *RECUS. Revista Electrónica Cooperación Universidad Sociedad*. ISSN 2528-8075, 7(1), Article 1. <https://doi.org/10.33936/recus.v7i1.3657>
- López-Paz, P. M., López-Cueva, L. A., López-Cueva, M. A., y Quispe-Velázquez, R. B. (2024). Satisfacción laboral y trabajo remoto: Análisis de la relación en el personal catedrático de una universidad pública en Puno Perú. *Revista Electrónica Educare*, 28(1), 168-187. <https://doi.org/10.15359/ree.28-1.18504>
- Martínez, L. P., Martínez, M. C., y Martínez, S. C. (2020). Seguridad y salud en el trabajo en teletrabajo autónomo en Colombia. *SIGNOS-Investigación en Sistemas de Gestión*, 12(1), 83-101. <https://www.redalyc.org/journal/5604/560465477005/>
- Peña, M., Saliba, S., Ísper, A., y Saliba, T. (2022). Impacto en la salud integral de profesionales del área de tecnología de la información que teletrabajan durante la COVID-19. *Población y Salud en Mesoamérica*, 19(2 (enero-junio)), 3. <https://dialnet.unirioja.es/servlet/articulo?codigo=8977444>
- Pérez, E. F. (2021). Los Vacíos Jurídicos De Los Riesgos Laborales Del Teletrabajo En Ecuador. *Foro: Revista de Derecho*, 35, Article 35. <https://doi.org/10.32719/26312484.2021.35.2>

- Pérez, E., Jové, D., y García, V. (2023). La Salud Mental En El Ámbito Laboral: ¿Son Efectivas Las Intervenciones Para Lograr El Regreso Al Trabajo? *Archivos de Prevención de Riesgos Laborales*, 26(3), 224-228. <https://doi.org/10.12961/aprl.2022.26.03.07>
- Pintado, H., y López, D. (2022). Implicación del teletrabajo en Ecuador. *Revista Metropolitana de Ciencias Aplicadas*, 5(2), 167-177. <https://www.redalyc.org/articulo.oa?id=721778114020>
- Ramírez, E., y Aguilar, R. (2022). El Trabajo Digital Como Transición Hacia Los Nuevos Entornos Laborales. *Denarius. Revista de Economía y Administración*, 2(43), 141-167. <https://www.redalyc.org/journal/6956/695676058005/>
- Restrepo, D., y Jaramillo, E. (2012). Concepciones De Salud Mental En El Campo De La Salud Pública. *Revista Facultad Nacional de Salud Pública*, 30(2), 202-211. <https://www.redalyc.org/articulo.oa?id=12023918009>
- Rubio, W., y Barrera, E. (2024). El derecho de los trabajadores a la desconexión digital en la legislación laboral ecuatoriana. *Enlace Universitario*, 23(1), 86-104. <https://doi.org/10.33789/enlace.23.1.141>
- Saborío, L., y Hidalgo, L. F. (2015). Síndrome de Burnout. *Medicina Legal de Costa Rica*, 32(1), 119-124. http://www.scielo.sa.cr/scielo.php?script=sci_abstract&pid=S1409-00152015000100014&lng=en&nrm=iso&tlng=es
- Sanca, M. (2011). *Revista de Actualización Clínica Volumen 12*.
- Santillan, W. (2020). El Teletrabajo En El Covid-19. *CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica*, 9(Extra 2), 65-76. <https://dialnet.unirioja.es/servlet/articulo?codigo=7746439>
- Vega, C., Ramirez, J., y Narcisa, M. (2022). Ventajas Y Desventajas Del Teletrabajo En Sudamérica Frente A La Pandemia Del Covid-19. *Civilizar. Ciencias Sociales y Humanas*, 22(42). <https://www.redalyc.org/articulo.oa?id=100274292007>

TELETRABAJO Y SALUD LABORAL: RIESGOS FÍSICOS, PSICOSOCIALES E IMPACTO EN EL DESEMPEÑO Y BIENESTAR

Claudia F. Lozano-Arteaga¹

RESUMEN

El objetivo principal del trabajo es analizar los desafíos del teletrabajo en Latinoamérica en una perspectiva de salud laboral, identificando los riesgos físicos y psicosociales. Se trata de una investigación cualitativa basada en la revisión de 30 fuentes documentales; entre los principales resultados, se identificaron riesgos físicos como problemas ergonómicos (dolores musculares y fatiga visual) y psicosociales (aislamiento, estrés y tecnoestrés), agravados por la falta de límites entre la vida laboral y personal. En cuanto a las políticas laborales y normativas, existen desigualdades en la regulación del teletrabajo; mientras algunos países avanzaron significativamente, otros muestran rezagos que afectan la implementación efectiva. Para garantizar un teletrabajo seguro, se proponen mejores prácticas, como la implementación de sistemas de gestión de salud laboral, ajustes en políticas empresariales, promoción de pausas activas y capacitación en ciberseguridad. Respecto al impacto en el rendimiento, el teletrabajo aporta flexibilidad y autonomía, pero puede alargar jornadas, aumentar el estrés y reducir la productividad debido a la sobrecarga laboral y la falta de interacción social. Además, esta modalidad favorece la conciliación de la vida laboral y personal al permitir mayor flexibilidad y fortalecer vínculos familiares, aunque requiere medidas claras para evitar la fusión entre ambos ámbitos. En conclusión, el teletrabajo representa una oportunidad valiosa, pero plantea desafíos significativos que requieren estrategias integrales en salud laboral,

¹ clozanoa1@upao.edu.pe

Programa de Estudio de Derecho, Universidad Privada Antenor Orrego

políticas inclusivas y normativas claras para maximizar sus beneficios y mitigar sus riesgos; su éxito depende de equilibrar la productividad empresarial con el bienestar de los trabajadores, garantizando un entorno laboral seguro, inclusivo y sostenible.

Palabras Clave: Salud laboral, teletrabajo, impacto, riesgos físicos y psicosociales

ABSTRACT

The main objective of this work is to analyze the challenges of teleworking in Latin America from an occupational health perspective, identifying physical and psychosocial risks. This is a qualitative research based on the review of 30 documentary sources; among the main results, physical risks such as ergonomic problems (muscle pain and visual fatigue) and psychosocial problems (isolation, stress and technostress) were identified, aggravated by the lack of boundaries between work and personal life. Regarding labor policies and regulations, there are inequalities in the regulation of teleworking; while some countries have made significant progress, others show lags that affect effective implementation. To ensure safe teleworking, best practices are proposed, such as the implementation of occupational health management systems, adjustments in company policies, promotion of active breaks and training in cybersecurity. Regarding the impact on performance, teleworking provides flexibility and autonomy, but can lengthen workdays, increase stress and reduce productivity due to work overload and lack of social interaction. Furthermore, this modality favours the reconciliation of work and personal life by allowing greater flexibility and strengthening family ties, although it requires clear measures to avoid the fusion of both areas. In conclusion, teleworking represents a valuable opportunity, but it poses significant challenges that require comprehensive occupational health strategies, inclusive policies and clear regulations to maximise its benefits and mitigate its risks; its success depends on balancing business productivity with the well-being of workers, guaranteeing a safe, inclusive and sustainable work environment.

Keywords: Occupational health, teleworking, impact, physical and psychosocial risks

INTRODUCCIÓN

El teletrabajo ha ganado relevancia mundial en el siglo XXI, Impulsado por los progresos tecnológicos y la digitalización de las actividades laborales, esta modalidad, reconocida por diversas legislaciones como el trabajo realizado fuera de las instalaciones del empleador mediante tecnologías de la información, ha permitido a empresas optimizar recursos y ofrecer mayor flexibilidad, su adopción masiva también ha planteado

retos importantes, particularmente en lo relacionado con la salvaguardia de la salud y el bienestar de los empleados.

A nivel psicológico, el teletrabajo puede tener un impacto significativo, pues el aislamiento social y la tendencia a extender las horas laborales incrementan el riesgo de estrés, ansiedad y otros trastornos mentales. Estas condiciones se agravan por la falta de una clara delimitación entre las actividades laborales y personales, lo que dificulta el establecimiento de horarios adecuados de trabajo y descanso, afectando directamente el bienestar del trabajador (Chacchi *et al.*, 2024).

Diversos estudiosos se refieren a este fenómeno como la ‘enfermedad de la excelencia’, destacando los efectos adversos que los enfoques de gestión conocidos como modelos gerenciales generan en el bienestar de los trabajadores. Este escenario subraya la necesidad de repensar las dinámicas laborales para equilibrar la eficiencia empresarial con la salud y el bienestar en un contexto cada vez más digitalizado (Tomasina & Pisani, 2022).

A nivel mundial, el teletrabajo ha sido aclamado por ofrecer beneficios significativos, como la reducción de los tiempos de desplazamiento, la posibilidad de conciliar la vida laboral y personal, y la creación de oportunidades laborales más inclusivas. No obstante, el uso de nuevas técnicas para evaluar la productividad individual ha impuesto mayores demandas sobre los empleados, lo que puede incrementar el sedentarismo y la obesidad, afectando la salud física (Espinoza & Sáurez, 2020).

En América Latina, el teletrabajo ha sido recibido de diferentes formas; sin embargo, un problema recurrente es la falta de adaptación de los espacios domésticos para funcionar como áreas laborales. Además, la ausencia de condiciones ergonómicas en el hogar ha elevado la incidencia de dolencias musculoesqueléticas, como cervicalgias y lumbalgias, afectando también la productividad y el bienestar general de los trabajadores (Chinchay, 2023).

Entonces como sabemos, el teletrabajo puede ser una herramienta valiosa si se implementan programas que promuevan la actividad física y una buena nutrición, así como políticas de salud mental que permitan desconectar de las tareas laborales. Las empresas y los gobiernos deben trabajar de la mano para asegurar un teletrabajo más seguro y saludable, en beneficio de todos los (Cataño & Gómez, 2014).

Este artículo tiene como propósito analizar los principales desafíos que enfrenta el teletrabajo en Latinoamérica esto debido a la perspectiva del bienestar laboral; para ello, se abordarán tanto los riesgos físicos, como los relacionados con la falta de ergonomía en el hogar, así como los riesgos psicosociales, derivados de la sobrecarga laboral, la falta de interacción social y la dificultad para desconectar del trabajo. Asimismo, se discutirán posibles estrategias para mitigar estos riesgos, tomando en cuenta la legislación vigente y las mejores prácticas internacionales.

El análisis propuesto busca no solo destacar las áreas de mejora en la regulación del teletrabajo, sino ofrecer también recomendaciones que permitan a las empresas y a los trabajadores adaptarse a esta nueva realidad de forma más saludable y sostenible. En este sentido, los objetivos del trabajo son: 1) identificar los principales riesgos físicos y psicosociales asociados al teletrabajo en el contexto peruano; 2) evaluar la efectividad de la legislación vigente en la protección del bienestar laboral en Latinoamérica; 3) proponer estrategias y mejores prácticas que contribuyan a un teletrabajo más seguro y saludable para todos; 4) analizar los factores que afectan el rendimiento de los trabajadores en el teletrabajo y 5) examinar los impactos del teletrabajo en la conciliación de la vida laboral y personal.

METODOLOGÍA

El estudio se enmarcó en un enfoque cualitativo con el objetivo de analizar los riesgos físicos y psicosociales del teletrabajo en el contexto laboral de Latinoamérica, así como su impacto en el desempeño y bienestar de los trabajadores. El diseño de la investigación es básica y no experimental; este enfoque permite no solo describir los problemas asociados al teletrabajo, sino también identificar áreas de mejora en la regulación y en las prácticas empresariales.

Para ello, se utilizó una estrategia de revisión documental, permitió analizar estudios y artículos académicos relacionados con los efectos del teletrabajo sobre la salud física y psicosocial de los trabajadores, identificando tanto los riesgos como las mitigadoras. La recopilación de información se fundamentó en una revisión exhaustiva de 30 fuentes documentales donde se utilizaron bases de datos jurídicas y académicas para recopilar información relevante sobre el teletrabajo, aplicables a la protección de datos personales en países como Chile, Bolivia, Argentina,

Venezuela, Colombia, México, Costa Rica y Perú. Entre las bases de datos utilizadas, se encuentran SCIELO, SCOPUS, REDALYC, DOAJ y DIALNET.

Este enfoque cualitativo se seleccionó porque permite profundizar en el análisis de fenómenos complejos como el teletrabajo, considerando las particularidades de los contextos laborales de Latinoamérica; se incluyeron únicamente artículos académicos revisados por pares, informes de organismos internacionales y estudios publicados entre 2009 y 2024. Se excluyeron fuentes que no presentaran datos empíricos o cuyo alcance estuviera limitado a contextos fuera de Latinoamérica, la recolección de datos se realizó desde septiembre y culminó en diciembre del 2024.

Los datos recopilados fueron analizados mediante un enfoque de análisis temático, que permitió identificar patrones recurrentes y categorizarlos según los objetivos específicos de la investigación. Se reconoce como limitación la exclusión de fuentes no accesibles en las bases de datos seleccionadas, así como la imposibilidad de generalizar los hallazgos debido a la naturaleza cualitativa del estudio.

Los documentos revisados incluyen investigaciones de diversos países de Latinoamérica, donde se ha regulado el teletrabajo de manera específica, permitiendo analizar sus desafíos y oportunidades para mejorar las condiciones laborales y el bienestar de los trabajadores. En este contexto, el teletrabajo se define como una modalidad de organización empresarial que implica la prestación de servicios de un lugar básicamente distante de la empresa, manteniendo o no una interacción directa con el cliente (Solís, 2021).

Para la recolección de datos, se utilizaron bases de datos académicas y artículos especializados en temas de derecho laboral y salud ocupacional, como también reportes de organismos. La búsqueda documental incluyó estudios clave sobre teletrabajo en la región de América Latina, analizaron los efectos del entorno doméstico en la salud de los empleados, como la falta de ergonomía en el hogar (Chinchay, 2023).

A continuación, se desarrolla el siguiente esquema temático: en primer lugar, es necesario identificar los principales riesgos físicos y psicosociales asociados al teletrabajo en Latinoamérica; en segundo lugar, analizar cómo se pueden adaptar las políticas laborales a las necesidades de diferentes sectores y contextos globales; en tercer lugar, plantear estrategias y

mejores prácticas para garantizar un teletrabajo seguro y saludable; en cuarto lugar, evaluar el impacto del teletrabajo en el rendimiento laboral, y, finalmente, examinar los efectos en la conciliación entre la vida laboral y personal, con énfasis en la salud mental y el bienestar general.

RESULTADOS

1. Principales riesgos físicos y psicosociales del teletrabajo en Latinoamérica

El teletrabajo, especialmente en Latinoamérica, ha aumentado notablemente, pero también presenta riesgos físicos y psicosociales; la falta de estaciones ergonómicas y espacios adecuados puede generar dolores de espalda, cuello y fatiga visual, agravados por el uso prolongado de computadoras sin el equipo necesario. Se identifican efectos negativos sobre la salud y bienestar de los teletrabajadores debido a la escasa interacción social y el aumento del individualismo, sumado a la exposición continua a dispositivos informático (Guayacán *et al.*, 2022).

El teletrabajo puede favorecer la inactividad física y modificaciones en los horarios de comida, pues la dinámica propia de esta modalidad afecta la percepción del tiempo; esto provoca que los trabajadores omitan descansos importantes, como las meriendas, el almuerzo o la cena; además, al no requerir desplazamientos, se reduce la actividad física, lo que incrementa el sedentarismo, especialmente en aquellas personas que ya tienen una baja actividad física (Espinoza & Sáurez, 2020).

El teletrabajo puede contribuir al sedentarismo y trastornos en los horarios de las comidas, la dinámica propia de esta modalidad afecta la percepción del tiempo, lo que puede llevar a omitir los descansos y, por ende, saltarse las comidas, como meriendas o almuerzos. y cenas; además, al no ser necesario desplazarse, se reduce la actividad física, lo que incrementa el sedentarismo en aquellas personas que ya no tienen una rutina activa (Arce & Rojas, 2020).

Por eso; se debe promover un entorno laboral saludable en el teletrabajo implicando adaptar espacios ergonómicos, garantizar equipos adecuados y fomentar pausas activas que reduzcan los riesgos físicos; también es esencial implementar políticas que equilibren la carga laboral, promuevan la desconexión digital y refuercen la interacción social virtual. Además, campañas sobre hábitos saludables y actividad física ayudarán a prevenir

el sedentarismo, mejorando el bienestar integral y el desempeño de los teletrabajadores.

Existen también riesgos ergonómicos, como la fatiga visual y problemas musculoesqueléticos, que surgen por la falta de condiciones adecuadas en el espacio de trabajo (Ramírez *et al.*, 2021). Por ello; existen nuevos desafíos, factores como el aislamiento social, la falta de avance en la carrera profesional, los conflictos familiares y una creciente sensación de sobrecarga laboral, junto con riesgos para la salud física, como la inactividad, malos hábitos alimenticios, y problemas visuales y musculoesqueléticos, han sido identificados (Martínez *et al.*, 2020).

Estas observaciones enfatizan la urgencia de diseñar políticas laborales integrales que vayan más allá de la mera prevención de riesgos; esto implica la creación de normativas y estrategias que promuevan ambientes de trabajo saludables, donde las condiciones ergonómicas sean una prioridad, garantizando mobiliario y equipos adecuados para evitar lesiones musculoesqueléticas y problemas visuales. Asimismo, es esencial fomentar la adopción de rutinas que incluyan pausas activas y hábitos alimenticios saludables, mitigando los efectos del sedentarismo y las alteraciones en las rutinas diarias.

Estos factores pueden afectar tanto el bienestar físico como emocional de los trabajadores, generando consecuencias negativas en su salud integral. Los principales riesgos para la salud de los teletrabajadores incluyen la falta de equipos ergonómicos adecuados y un espacio de trabajo dedicado, el exceso de trabajo y las implicaciones psicosociales derivadas del trabajo remoto (Morán *et al.*, 2022).

La intensificación de la actividad derivada del uso de las TIC ha dado lugar a un tipo de estrés denominado tecnoestrés, el cual se define como las reacciones psicosociales negativas, tanto cognitivas, afectivas como conductuales, provocadas por el uso constante de estas tecnologías (Tomasina & Pisani, 2022).

Es fundamental que se puedan eliminar los límites físicos entre la casa y la oficina, puesto que llevan a la sobrecarga laboral y al agotamiento, lo que requiere una gestión más efectiva del tiempo de trabajo y descanso; además, el uso constante de tecnologías puede generar tecnoestrés, afectando la productividad y la salud mental. Por eso, es crucial implementar medidas que promuevan un equilibrio adecuado entre el trabajo y la vida personal,

asegurando que los teletrabajadores no solo tengan un entorno cómodo y seguro, sino también el apoyo necesario para manejar el estrés y evitar el aislamiento social.

En cuanto a las condiciones del espacio de trabajo, es esencial que éste esté bien definido y aislado de las demás áreas del hogar, con elementos básicos como una silla y mesa adecuadas, junto a un equipo informático de calidad, aunque la variabilidad de situaciones dificulta la implementación de estas condiciones en todos los hogares (Benavides *et al.*, 2022).

Esta investigación ha demostrado que a comienzos del siglo XXI, los estudios sobre el impacto del teletrabajo en el bienestar de los teletrabajadores se han enfocado principalmente en aspectos como el manejo del estrés, los problemas psicológicos y ergonómicos asociados con esta modalidad, así como en la conciliación entre la vida laboral y personal. Sin embargo, recientemente ha comenzado a haber un cambio hacia el análisis de otros temas, como los problemas psicosociales y la preocupación por cuestiones legales y normativas que garanticen la salud de los trabajadores a distancia (Sanchez & Toledo, 2021).

Se examinan múltiples aspectos vinculados al teletrabajo, enfocándose en los riesgos que este modelo laboral puede generar tanto en el ámbito físico como en el psicosocial. Dentro de los riesgos físicos, se mencionan problemas musculoesqueléticos, fatiga visual y sedentarismo, los cuales se asocian a la ausencia de condiciones ergonómicas adecuadas en los espacios de trabajo. Además, se describe cómo la falta de actividad física, junto con alteraciones en los horarios de alimentación, contribuye a hábitos poco saludables.

En cuanto a los riesgos psicosociales, se resalta el aislamiento social, el aumento del individualismo y el tecnoestrés, problemas que surgen debido a la interacción constante con tecnologías y la falta de límites claros entre el entorno laboral y personal. Asimismo, se señala cómo la sobrecarga laboral y el uso intensivo de dispositivos informáticos afectan la salud mental de los trabajadores.

El análisis pone en evidencia la importancia de diseñar políticas laborales que prioricen la ergonomía, promuevan pausas activas y fomenten hábitos saludables. También se resalta la necesidad de normativas que protejan la salud integral de los teletrabajadores y garanticen un equilibrio adecuado entre la vida laboral y personal. Finalmente, el análisis concluye que el

teletrabajo, aunque ofrece beneficios significativos, plantea desafíos críticos que deben abordarse de un enfoque integral.

Los riesgos físicos y psicosociales asociados a esta modalidad laboral subrayan la necesidad de adaptar los espacios de trabajo, establecer políticas que protejan la salud integral de los teletrabajadores y promover un equilibrio adecuado entre el ámbito laboral y personal. Además, la evolución de los estudios hacia un enfoque multidimensional refleja la creciente relevancia de considerar no sólo los aspectos ergonómicos y psicológicos, sino también los legales y normativos, para garantizar un entorno laboral seguro, saludable y sostenible.

2. Adaptaciones de las políticas de teletrabajo a las necesidades específicas de diferentes sectores y tipos de trabajo en distintas partes del mundo

En Latinoamérica, durante la pandemia, el Estado implementó medidas de precaución y cuarentena, incluyendo disposiciones legales que declaraban el estado de emergencia sanitaria y adoptaban medidas preventivas contra la propagación del Sars-Cov-2(COVID-19). Dentro de estas medidas, se destacó la introducción del teletrabajo, como una forma de proteger la salud y seguridad de los trabajadores; además, se promovió que las organizaciones debían cumplir con la ejecución de ciertas normativas anuales (Chacchi *et al.*, 2024).

Estas decisiones reflejan un enfoque renovado hacia la protección de la salud laboral, reconociendo la importancia de abordar tanto los aspectos físicos como psicosociales, con especial énfasis en la prevención de trastornos mentales y el bienestar de los empleados. El teletrabajo requiere el acuerdo entre las partes involucradas, el cual puede ser establecido tanto al inicio de la relación laboral como en su transcurso; es fundamental que este acuerdo no afecte los derechos reconocidos por la normativa laboral, garantizando que los trabajadores continúen disfrutando de todos sus derechos individuales y colectivos (Pinto, 2021).

Se podría ampliar sobre los desafíos que enfrenta su implementación, como las desigualdades tecnológicas y el riesgo de desequilibrio en las negociaciones laborales. Además, resulta clave reflexionar sobre si las normativas en vigencia son suficientes para garantizar equidad y sostenibilidad, considerando que el teletrabajo podría trascender el contexto de la pandemia hacia una modalidad más permanente; por ello el análisis

podría complementarse con un enfoque comparativo, identificando cómo otras regiones han implementado el teletrabajo y qué lecciones podrían adoptarse en Latinoamérica para mejorar su desarrollo y sostenibilidad en el tiempo.

Países como Chile, Bolivia y Argentina han fortalecido la regulación jurídica del teletrabajo y su implementación tras los efectos causados por la pandemia; por otro lado, en Venezuela, Paraguay y Uruguay se fomenta la implementación del teletrabajo en los sectores público y privado, aunque no se ha desarrollado un régimen jurídico adecuado para su correcta implementación (Ramírez *et al.*, 2022).

Por otro lado, el gobierno respaldado por la identidad organizacional, juega un papel crucial en equilibrar la productividad y la calidad de vida laboral mediante políticas que guían las acciones dentro de la organización, si se prioriza la productividad, es posible que se logren mejoras a corto plazo en las utilidades de la organización, pero esto podría comprometer la calidad de vida laboral; tal enfoque puede generar efectos negativos a largo plazo, como la pérdida de talento humano y una disminución de la cooperación espontánea, lo que impactaría la eficiencia y limitaría el potencial del teletrabajo para mejorar los resultados orgánicos (Peláez y López, 2013).

Se ofrece un contraste interesante entre países con diferentes niveles de desarrollo normativo sobre teletrabajo, lo que evidencia desigualdades en su regulación y aplicación; además, resalta el papel clave del gobierno y la identidad organizacional en la creación de políticas que equilibren productividad y calidad de vida laboral. Un enfoque excesivo en las utilidades puede generar consecuencias adversas a largo plazo, como la fuga de talento y una menor colaboración; esto subraya la necesidad de un balance estratégico que garantice sostenibilidad y bienestar en las relaciones laborales.

Es necesario implementar políticas que promuevan un entorno de trabajo inclusivo para los teletrabajadores con discapacidad, con el objetivo de minimizar el aislamiento social al que están expuestos debido a sus limitaciones, al tiempo que se maximiza su participación en la comunidad laboral. Para ello, se deben considerar tres líneas de actuación fundamentales: investigación, divulgación e intervenciones efectivas (Vicente *et al.*, 2018).

En algunos contextos, el poder puede verse como opresión, mientras que en otros es un medio definitorio de la comunicación, resultado de la

contraposición de nociones jurídicas, sociológicas y políticas, las cuales a menudo se tornan irreconciliables. Lo cierto es que el poder surge de la naturaleza social del ser humano, quien, por su esencia, tiende a relacionarse de forma jerárquica con sus semejantes (Ortiz, 2022).

Se resalta la importancia de crear un entorno inclusivo para los teletrabajadores con discapacidad, enfocándose en la necesidad de políticas que combatan el aislamiento social y favorezcan la integración laboral. La propuesta de investigación, divulgación e intervenciones efectivas refleja una estrategia integral que podría mejorar significativamente la participación de este grupo en el mercado laboral; además, se aborda una reflexión sobre el poder, destacando su dualidad como herramienta de opresión y comunicación, lo que invita a reconsiderar las dinámicas jerárquicas y las tensiones inherentes a las estructuras sociales y laborales; esto abre un espacio para analizar cómo se ejerce el poder dentro del contexto organizacional y su impacto en la inclusión y el bienestar de los trabajadores.

En Colombia, la Constitución establece que la salud es un estado de bienestar integral, incluyendo el físico, mental y social, y que el acceso a servicios de salud y saneamiento ambiental es responsabilidad del Estado; esto garantiza a todas las personas la disponibilidad de servicios para la promoción, protección y recuperación de la salud, bajo principios de eficiencia, universalidad y solidaridad (Betancur & Bedoya, 2022).

Ante los efectos de la pandemia, el Ministerio del Trabajo de Colombia emitió directrices para la implementación del teletrabajo, exigiendo a los trabajadores que adopten esta modalidad como medida excepcional en sectores afectados, asegurando la protección del empleo y la salud de los trabajadores, y diferenciando claramente esta modalidad de teletrabajo de otras formas de trabajo en casa (Ramírez *et al.*, 2021).

El enfoque en Colombia sobre la salud como un bienestar integral es acertado, reconoce la interconexión entre los aspectos físicos, mentales y sociales, lo cual es esencial para garantizar un entorno laboral saludable; la respuesta del Ministerio del Trabajo ante la pandemia, al regular el teletrabajo como una medida excepcional, demuestra un esfuerzo por proteger a los trabajadores en tiempos difíciles, aunque puede generar desafíos en la práctica.

Es importante avanzar en la adecuación normativa de los principios del convenio No 156 de la OIT, especialmente en lo que respeta a la igualdad de

género en el ámbito laboral, para promover un cambio de roles y sancionar efectivamente las prácticas discriminatorias, lo cual es esencial. para una inclusión laboral plena y equitativa (Sánchez & Mozo, 2009).

En la adecuación normativa del convenio No. 156 de la OIT es fundamental para avanzar hacia una mayor equidad en el ámbito laboral. La igualdad de género no solo requiere de la modificación de las normas, sino también de un cambio cultural profundo que desafíe los roles tradicionales y erradique las prácticas discriminatorias; promover una inclusión laboral plena y equitativa no solo beneficia a las trabajadoras, sino que también enriquece el entorno laboral en su conjunto, es clave que las políticas laborales no solo se queden en el papel, sino que se acompañen de medidas efectivas que garanticen que se cumplan en todos los niveles organizacionales.

Se refleja una perspectiva integral sobre cómo las políticas de teletrabajo deben adaptarse a las necesidades de diversos sectores y contextos en todo el mundo, particularmente en América Latina; se destaca la importancia de la legislación y las normativas que buscan equilibrar los derechos laborales con la protección de la salud de los trabajadores, lo que se ha vuelto aún más relevante en el contexto de la pandemia. Sin embargo, se hace evidente que la implementación del teletrabajo no es uniforme en todos los países, y existen importantes disparidades en cuanto a la infraestructura tecnológica, la capacitación y la regulación adecuada para su implementación efectiva.

A medida que los gobiernos y las organizaciones intentan equilibrar la productividad con el bienestar laboral, surgen tensiones entre la eficiencia empresarial y la calidad de vida de los trabajadores. Es fundamental que se promuevan políticas que garanticen no solo la protección de los derechos laborales, sino también un entorno de trabajo inclusivo, especialmente para grupos vulnerables como los teletrabajadores con discapacidad.

Lo más relevante de este análisis es que pone de manifiesto la necesidad de enfoques más flexibles y personalizados en las políticas de teletrabajo, considerando las realidades sociales, económicas y culturales de cada país; a través de la investigación, la divulgación y las intervenciones efectivas, se puede avanzar hacia un modelo de teletrabajo más inclusivo y justo que no solo promueva la productividad, sino que también garantiza el bienestar y la equidad en el entorno laboral. La inclusión de aspectos como la igualdad de género y la lucha contra la discriminación laboral refuerza aún más la idea de que las políticas de teletrabajo deben ser no

solo eficaces, sino también justas y accesibles para todos los trabajadores, independientemente de su contexto.

3. Estrategias y mejores prácticas que pueden implementarse para garantizar un teletrabajo seguro y saludable para todos los trabajadores

Para garantizar un entorno de teletrabajo seguro y saludable, es necesario adoptar un enfoque integral que aborde factores ergonómicos, de salud mental, seguridad digital y equilibrio entre la vida personal y laboral; el diseño e implementación de un Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) resulta fundamental. Este proceso incluye etapas como la construcción de políticas para teletrabajo, ajustes en los reglamentos internos de trabajo y la capacitación de los empleados en la gestión de riesgos, es necesario anticipar, reconocer y controlar los riesgos que afectan la seguridad y la salud del teletrabajador (Cataño & Gómez, 2014)

El diseño ergonómico del espacio de trabajo es una de las principales medidas recomendadas para prevenir lesiones musculoesqueléticas en teletrabajadores, las empresas deben proporcionar equipamiento ergonómico adecuado, como sillas y escritorios ajustables, además de capacitar a los empleados en su uso correcto. Las pausas activas son también esenciales para contrarrestar la fatiga física y mental, permitiendo a los empleados mantener una postura adecuada y prevenir problemas de salud a largo plazo (Escalante *et al.*, 2020).

Es fundamental que las organizaciones adopten un enfoque integral para garantizar un entorno de teletrabajo seguro y saludable; la implementación de un Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) resulta crucial para abordar diversas áreas como la ergonomía, la salud mental, la seguridad digital y el equilibrio entre la vida personal y laboral; la construcción de políticas específicas, ajustes en los reglamentos internos y la capacitación adecuada en la gestión de riesgos contribuyen a anticipar y controlar los peligros que pueden afectar la salud y seguridad de los teletrabajadores. En cuanto al diseño ergonómico, además de la importancia de proporcionar equipamiento adecuado y fomentar las pausas activas, que son esenciales para prevenir la fatiga y mantener el bienestar físico y mental de los empleados.

La salud mental es otro pilar fundamental en el teletrabajo, porque el aislamiento y los cambios en las rutinas pueden impactar significativamente

el bienestar emocional de los empleados; cuidar la salud mental es crucial “no solo para mejorar la salud sino también para evitar otros problemas sociales, tales como la estigmatización de personas, la falta de adherencia a medidas de prevención, y el duelo frente a la pérdida de seres queridos”; en esta línea, se subraya que el desarrollo de la capacidad emocional de las personas es imposterizable, quienes realizan teletrabajo no están exentos del impacto emocional de la pandemia (Kajat *et al.*, 2021)

La importancia de capacitar a los teletrabajadores en la identificación y manejo de factores psicosociales como el aislamiento social y la sobrecarga es crucial. Asimismo, es necesario crear mecanismos que ayuden a reducir la fatiga, en especial para quienes tienen responsabilidades familiares, como niños y adultos mayores. Los médicos ocupacionales deben recibir formación en estrategias para prevenir o corregir el impacto de la fatiga en los trabajadores (Daga & Gonzales, 2022).

La salud mental juega un papel crucial en el teletrabajo, dado que el aislamiento y las alteraciones en las rutinas pueden tener un impacto significativo en el bienestar emocional de los empleados; cuidar la salud mental es esencial no solo para mejorar la calidad de vida, sino también para evitar problemas sociales como la estigmatización y la falta de adherencia a las medidas preventivas. Asimismo, es importante capacitar a los teletrabajadores para que identifiquen y gestionen factores psicosociales como el aislamiento y la sobrecarga; la implementación de mecanismos para reducir la fatiga es vital, especialmente para aquellos que tienen responsabilidades familiares.

La utilización de tecnologías modernas es clave en la implementación efectiva del teletrabajo, pero debe ir acompañada de una cultura de productividad y prevención en salud y seguridad laboral. Esto implica una organización adecuada del teletrabajo dentro de las empresas y una inversión en la formación integral de los recursos humanos (Solís, 2021)

Por otro lado, el teletrabajo debe ser considerado dentro de un contexto más amplio de políticas laborales y gubernamentales. Esta modalidad de trabajo está alineada con la transición hacia modelos de gobernanza que promueven el mejoramiento del empleo, reflejando cambios político-administrativos (Betancur & Bedoya, 2022)

La adopción de tecnologías modernas resulta esencial para el teletrabajo, pero su implementación debe ir acompañada de una cultura organizacional que favorezca la productividad y la prevención en salud y seguridad

laboral; para que el teletrabajo sea eficaz, es necesario que las empresas cuenten con una estructura adecuada y realicen una inversión constante en la formación de su personal, garantizando que los empleados puedan utilizar las herramientas tecnológicas de manera óptima y segura. Esta modalidad de trabajo se inserta dentro de un proceso de transformación hacia modelos de gobernanza que buscan mejorar la calidad del empleo y adaptarse a las nuevas necesidades del mercado laboral.

La capacitación en seguridad digital también es crucial en el teletrabajo, trabajar fuera del entorno controlado de una oficina incrementa los riesgos relacionados con la protección de datos sensibles; se enfatiza que las empresas deben capacitar a sus empleados en prácticas de ciberseguridad, como el uso seguro de plataformas digitales y la protección de datos personales (Valencia, 2018).

Se debe lograr un balance entre la vida personal y laboral representa uno de los mayores desafíos del teletrabajo, por ello se propone la creación de espacios de trabajo dedicados en el hogar y la implementación de horarios fijos para reducir distracciones, evitar la sobrecarga y mejorar la productividad (Guayacán *et al.*, 2022).

Los acuerdos de trabajo flexible, como la opción de ajustar los horarios laborales, contribuyen a que los empleados gestionen mejor el equilibrio entre su vida personal y profesional, lo que reduce el estrés y el agotamiento, mejorando así su bienestar. En un estudio realizado durante la pandemia de COVID-19, se observó que la implementación de prácticas organizacionales adaptativas, como el trabajo flexible, el teletrabajo, el pago de licencias personales y la implementación de planes de seguridad, ayudó a disminuir la percepción de inseguridad laboral entre los trabajadores (Yeves *et al.*, 2022).

Las tecnologías modernas resultan esenciales para el teletrabajo, pero su implementación debe ir acompañada de una cultura organizacional que favorezca la productividad y la prevención en salud y seguridad laboral. Para que el teletrabajo sea eficaz, es necesario que las empresas cuenten con una estructura adecuada y realicen una inversión constante en la formación de su personal, garantizando que los empleados puedan utilizar las herramientas tecnológicas de manera óptima y segura.

Un teletrabajo seguro y saludable requiere de un enfoque integral que atienda tanto los aspectos físicos como los emocionales y digitales del entorno laboral; las estrategias revisadas no solo permiten que el teletrabajo

sea más productivo y menos riesgoso, sino que también fomentan una cultura de responsabilidad compartida entre empleadores y trabajadores. La capacitación en ergonomía, salud mental y ciberseguridad es esencial para que los empleados trabajen de manera eficaz y sin riesgos.

Asimismo, los arreglos de trabajo flexible y el respeto por los tiempos de desconexión fortalecen el bienestar y el compromiso del trabajador, aspectos que son fundamentales para el éxito sostenible del teletrabajo en un entorno cada vez más digital; los esfuerzos en teletrabajo no deben enfocarse únicamente en maximizar la productividad, sino en crear un modelo de trabajo en el que el bienestar del empleado esté en el centro de las políticas.

4. Cómo Afecta el Teletrabajo al Rendimiento de los Trabajadores

En los últimos años, el teletrabajo ha evolucionado hasta consolidarse como una modalidad laboral predominante, especialmente tras la pandemia de COVID-19. Este fenómeno ha generado efectos diversos en el rendimiento laboral, destacando tanto oportunidades como desafíos para los trabajadores y las organizaciones; aunque aporta flexibilidad y autonomía, también implica riesgos significativos para el bienestar físico y emocional.

Se sugiere que las entidades estatales adopten un instrumento de gestión, como directivas, lineamientos u otros mecanismos, destinado a regular la implementación del trabajo remoto y garantizar el derecho a la desconexión digital para los trabajadores administrativos, considerando las recomendaciones previamente expuestas (Daga & Gonzales, 2022).

La gestión de esta pandemia pone en evidencia la capacidad de adaptación tanto individual como colectiva en la vida de las personas, mientras las significativas transformaciones generadas por esta crisis y su impacto social promueven comportamientos adecuados frente a los nuevos escenarios (Escalante *et al.*, 2020). En contextos de alta demanda familiar, el estrés relacionado con las responsabilidades domésticas y laborales se incrementa, afectando no solo la productividad individual, sino también la dinámica del equipo de trabajo (Espinoza & Sáurez, 2020).

La pandemia ha puesto de manifiesto cómo las personas pueden adaptarse rápidamente a nuevas circunstancias, el aumento de las responsabilidades tanto laborales como domésticas ha generado un gran estrés, afectando no solo la productividad, sino también el bienestar emocional. La dificultad

de equilibrar estos aspectos ha resaltado la importancia de contar con estrategias que apoyen la conciliación de la vida laboral y familiar, como horarios flexibles o el teletrabajo, para evitar que este estrés se transforme en un obstáculo mayor, en definitiva, la crisis ha mostrado la necesidad urgente de promover un enfoque más equilibrado que considere el bienestar integral de las personas.

La interacción entre las responsabilidades familiares y laborales, junto con el aislamiento social, se asocia de manera negativa, mientras que el autoliderazgo y la autonomía se vinculan positivamente con la productividad y el compromiso del teletrabajador domiciliario; por otro lado, el conflicto entre las obligaciones familiares y laborales, así como el aislamiento social, se relacionan con el incremento del estrés en el teletrabajador (Tomasina & Pisani, 2022).

En investigaciones realizadas en 2008, se sostiene que el aislamiento profesional influye de manera negativa en el desempeño laboral y, en contra de lo que se podría esperar, disminuye las intenciones de rotación del trabajador; este efecto se intensifica con la cantidad de tiempo dedicado al teletrabajo, mientras que las interacciones personales directas y el acceso a tecnologías que mejoran la comunicación tienden a mitigar dicho impacto; a partir de estos hallazgos, se abre un amplio campo de estudio sobre el aislamiento profesional en el teletrabajo, especialmente en un contexto donde la demanda de esta modalidad organizativa de trabajo sigue en aumento en nuestra sociedad (Vicente *et al.*, 2018).

El teletrabajo presenta una dinámica compleja, donde el aislamiento social y la falta de interacción directa pueden tener un impacto negativo en el bienestar y la productividad de los trabajadores, la interacción entre las responsabilidades laborales y familiares también contribuye a una mayor carga de estrés, lo que puede afectar tanto el desempeño como la satisfacción laboral. Sin embargo, es importante señalar que la autonomía y el autoliderazgo pueden ayudar a contrarrestar estos efectos negativos, impulsando la productividad y el compromiso del trabajador; haciendo necesario un enfoque que favorezca tanto el bienestar como la eficiencia laboral en esta modalidad.

Los inconvenientes pueden manifestarse en aspectos ergonómicos, como la ubicación inadecuada del puesto de trabajo en el hogar, la mala distribución del espacio destinado al trabajo, así como problemas relacionados con la iluminación, la temperatura y la disposición general

del entorno; asimismo, surgen complicaciones vinculadas con la gestión de los horarios, tales como la sobrecarga laboral o la escasa cantidad de trabajo, la desorganización en los tiempos de comida, el sedentarismo y la descoordinación entre el horario laboral y los biorritmos naturales del trabajador (Martínez *et al.*, 2020)

El teletrabajo impacta las relaciones laborales tradicionales, alterando sus esquemas de protección y garantías normativas. En particular, la atomización, que se pretende analizar, constituye una forma de subordinación laboral que acentúa la asimetría en la relación de trabajo. Aislar el desarrollo profesional representa una modalidad de fragmentación del colectivo laboral, impide el ejercicio conjunto de sus sistemas de garantías y, evidentemente, la implementación de las mismas (Lenguita, 2010).

El teletrabajo ha generado retos ergonómicos y organizativos que afectan la salud y productividad de los trabajadores, como la mala distribución del espacio y la gestión inadecuada de los horarios; además, ha alterado las relaciones laborales tradicionales, creando una forma de subordinación más difusa que dificulta la implementación de garantías y protecciones laborales. Esto puede aumentar la precariedad y desprotección, por lo que es esencial encontrar un equilibrio para proteger los derechos de los trabajadores en esta modalidad.

El control incrementado del trabajador sobre las demandas laborales diarias guarda una relación directa con la extensión de las horas de trabajo, lo que implica que los teletrabajadores experimentan una prolongación habitual de su jornada laboral, la dinámica del teletrabajo no logra equilibrar las horas dedicadas a las responsabilidades laborales y al cuidado del hogar y los hijos, dado que, al alargarse la jornada laboral, se reduce el tiempo disponible para la vida familiar, limitando la capacidad del colectivo laboral para protegerse de posibles abusos patronales a través de sus mecanismos sindicales (Sanchez & Toledo, 2021).

Las enfermedades profesionales tienden a manifestarse en mayor medida que los accidentes de trabajo, debido a las actividades vinculadas con el aislamiento y la autonomía en el trabajo remoto, los teletrabajadores se exponen a diversos riesgos. Estos efectos suelen desarrollarse a mediano y largo plazo, y pueden ser tanto agudos como crónicos (Muy Pérez, 2021).

El teletrabajo ofrece beneficios como flexibilidad y autonomía, lo que

permite a los trabajadores gestionar mejor su tiempo y conciliar las responsabilidades laborales y personales. Sin embargo, también presenta desafíos significativos para el bienestar físico y emocional; el aislamiento social y la dificultad para equilibrar las responsabilidades laborales y familiares generan un aumento del estrés, lo que impacta negativamente en la productividad. Los problemas ergonómicos derivados de un entorno doméstico inadecuado, como la mala distribución del espacio, el mobiliario inadecuado y la iluminación deficiente, son comunes.

Asimismo, el teletrabajo ha alterado las relaciones laborales tradicionales; la modalidad remota dificulta la implementación de las protecciones laborales, pues los trabajadores no tienen acceso fácil a los mecanismos de defensa que ofrecen las estructuras sindicales y de protección laboral en las modalidades presenciales. La creciente autonomía en la gestión del trabajo puede llevar a la prolongación de las jornadas laborales, el control sobre el horario de trabajo suele recaer sobre el propio trabajador.

Por todo lo anterior, es esencial que se adopte un enfoque integral que combine la flexibilidad del teletrabajo con medidas claras y reguladas para proteger el bienestar de los trabajadores, las organizaciones y las entidades estatales deben implementar políticas sobre desconexión digital, que aseguren que los trabajadores puedan disfrutar de tiempo personal sin la presión de responder a demandas laborales fuera de su horario. Además, deben establecer límites claros para la jornada laboral, garantizar un entorno de trabajo ergonómico y promover el uso de tecnologías que faciliten la comunicación y el trabajo colaborativo, minimizando así los efectos negativos del aislamiento.

5. Impactos del Teletrabajo en la Conciliación de la Vida Laboral y Personal y sus Efectos en la Salud Mental y Bienestar de los Trabajadores

El teletrabajo ha transformado las dinámicas laborales, y la propuesta es ir más allá de las normas tradicionales que, aunque valiosas, no deben ser el único enfoque; en lugar de centrarse en cumplir horarios estrictos, asistir a las instalaciones de la empresa o utilizar exclusivamente los equipos proporcionados por la organización, el foco debería estar en fomentar el trabajo en equipo y la participación activa en la gestión de riesgos laborales; estos riesgos podrían afectar la salud del teletrabajador y deben ser gestionados de manera continua y efectiva (Cataño & Gómez, 2014).

En cuanto a los aspectos específicos del teletrabajo, este presenta características particulares que requieren un enfoque diferenciado en la seguridad y salud ocupacional; entre ellas se destacan el uso intensivo de tecnologías, la falta de una clara división entre la vida laboral y la vida familiar, y las mayores exigencias de control y productividad; estas particularidades hacen imprescindible abordar la salud mental de los trabajadores de forma especial, para proteger su bienestar en este entorno laboral (Chinchay, 2023).

Por ello el teletrabajo debe verse como una oportunidad para transformar los modelos laborales tradicionales; más que un simple cambio en el lugar de trabajo, el teletrabajo requiere un enfoque integral que considere no solo los riesgos físicos, sino también los psicológicos. Las empresas deben ofrecer apoyo para gestionar estas nuevas demandas y encontrar un balance entre la vida laboral y familiar, garantizando el bienestar de los empleados.

El teletrabajo también brinda una mejor calidad de vida, se asocia con menos estrés, menores gastos en transporte y ropa, y mejores condiciones de alimentación. Además, fomenta una mayor vida familiar, pues permite que los padres pasen más tiempo en casa, lo que les permite compaginar sus tareas con las de los niños, fortaleciendo los lazos familiares y la educación en el hogar (Havriluk, 2010).

Se reducen los conflictos debido a que es trabajo en casa por eso, los gastos adicionales y el estrés relacionado con los traslados; aquellos que poseen vehículo también pueden enfrentar dificultades económicas por el gasto en combustible, lo que además contribuye a la contaminación ambiental; en cambio, el teletrabajo fomenta el ahorro de tiempo y dinero, así como la protección de la salud y el medio ambiente, a nivel familiar, permite que el teletrabajador pase más tiempo con su familia, lo que fortalece los lazos familiares y contribuye al desarrollo integral de los hijos (Valencia, 2018).

A nivel organizativo, es fundamental ofrecer capacitación básica para la creación de brigadas de emergencias y la implementación de sistemas de gestión de seguridad y salud en el trabajo; en empresas con más de diez empleados, se debe capacitar al Comité Paritario de Seguridad y Salud en el Trabajo, mientras que en las empresas con menos de diez empleados, los vigías ocupacionales desempeñan funciones similares; además, se deben desarrollar actividades que fomenten estilos de vida saludables, adaptadas a los perfiles epidemiológicos de cada empresa. (Betancur & Bedoya, 2022).

Al eliminar desplazamientos, beneficia a los trabajadores en términos de ahorro de tiempo y dinero, pero también implica riesgos que deben ser gestionados adecuadamente; la capacitación continua y la preparación para emergencias son esenciales para asegurar que los teletrabajadores, a pesar de estar físicamente alejados de la empresa, cuenten con las herramientas necesarias para mantener un ambiente de trabajo seguro y saludable.

No obstante, el teletrabajo también ha traído desafíos, especialmente en la adaptación de la mentalidad de las personas; la necesidad de superar barreras sociales y laborales ha sido un esfuerzo considerable; aunque el teletrabajo puede generar estrés, debido a la sobrecarga de tareas laborales y la fusión de la vida familiar con el trabajo, también representa una oportunidad para la inclusión de personas con discapacidad, madres cabeza de hogar y madres lactantes, ampliando las posibilidades laborales para quienes enfrentan desafíos adicionales (Gómez *et al.*, 2020).

El teletrabajo también tiene un impacto significativo en la reconfiguración de los roles de género; el reconocimiento de las mujeres como trabajadoras plenas, con igualdad de oportunidades laborales frente a los hombres, es crucial, esto no solo mejora su desarrollo profesional, sino que también permite un equilibrio entre las responsabilidades laborales y familiares (Caamaño Rojo, 2010).

El teletrabajo tiene el potencial de ser una herramienta poderosa para la inclusión, especialmente de mujeres y personas en situaciones vulnerables al ofrecer mayor flexibilidad, se pueden equilibrar las responsabilidades laborales y familiares, mejorando la calidad de vida de estos grupos; sin embargo, para que esto sea efectivo, es necesario que las empresas implementen políticas inclusivas y de apoyo que eliminen las barreras tradicionales.

Esto implica que da una oportunidad única para la realización personal y permite a los trabajadores gestionar sus tiempos de manera flexible; esto incluye acompañar a los hijos en momentos clave, organizar las tareas domésticas cuando más convenga, o atender a asuntos familiares; esta autonomía no solo mejora la calidad de vida del trabajador, sino que también contribuye a un entorno laboral más saludable y equilibrado (Sánchez & Mozo, 2009).

El teletrabajo ofrece ventajas claras, como la reducción de tiempo y costos en los desplazamientos, así como la posibilidad de equilibrar mejor la vida personal y profesional; no obstante, también presenta desafíos,

principalmente en la gestión de la salud mental y los riesgos laborales, que deben ser tratados de manera específica. Si bien el teletrabajo facilita la organización del tiempo y fortalece los lazos familiares, es fundamental contar con una planificación adecuada para maximizar estos beneficios.

Además, la capacitación en seguridad sigue siendo importante, incluso para quienes trabajan desde casa, esta modalidad también permite la inclusión de grupos vulnerables, como personas con discapacidad o madres cabeza de hogar; si se maneja bien, el teletrabajo mejora la autonomía del trabajador y promueve un entorno equilibrado, lo que puede aumentar la productividad y la satisfacción.

CONCLUSIONES

- Se identificaron los principales riesgos físicos asociados al teletrabajo en Latinoamérica incluyen problemas musculoesqueléticos, fatiga visual y sedentarismo, derivados de la ausencia de condiciones ergonómicas adecuadas en los espacios laborales domésticos. En el ámbito psicosocial, se destacan el aislamiento social, la sobrecarga laboral y el estrés relacionado con la falta de desconexión digital.
- Se evaluaron las legislaciones en Latinoamérica y presentan avances significativos en la regulación del teletrabajo, aunque persisten limitaciones en su efectividad; si bien se han implementado normativas que buscan proteger a los trabajadores, aún se requiere fortalecer la supervisión del cumplimiento de las medidas de desconexión digital y garantizar condiciones ergonómicas en los hogares.
- Se propone implementar estrategias que incluyan la capacitación en ergonomía, pausas activas, gestión del estrés y ciberseguridad. Además, se sugiere establecer políticas de desconexión digital, horarios flexibles y programas que fomenten la actividad física y una buena salud mental. Las empresas y el Estado deben trabajar conjuntamente para garantizar condiciones laborales inclusivas y seguras.
- Se analizaron los factores que afectan el rendimiento de los teletrabajadores incluyendo la autonomía y el autoliderazgo como elementos positivos, mientras que el aislamiento social, la carga laboral excesiva y la inadecuada gestión de horarios disminuyen la productividad. La falta de interacción directa y el mal diseño del entorno de trabajo también contribuyen a un impacto negativo en el desempeño laboral.

- Se examinó el impacto del teletrabajo en la conciliación entre la vida laboral y personal mostró beneficios como mayor tiempo con la familia y ahorro en transporte, pero también retos como la falta de límites claros entre ambos ámbitos, lo que genera estrés y dificulta la gestión adecuada de responsabilidades. La inclusión de medidas específicas puede potenciar los beneficios de esta modalidad.

REFERENCIAS BIBLIOGRÁFICAS

- Arce & Rojas. (2020). Satisfacción laboral y estrés en teletrabajadores y trabajadores presenciales de una universidad estatal de Costa Rica. *Cuadernos de Investigación UNED*, 12(2), 484-495. <https://doi.org/10.22458/urj.v12i2.3141>
- Benavides, F. G., Silva-Peñaherrera, M., Benavides, F. G., & Silva-Peñaherrera, M. (2022). Datos y evidencias del teletrabajo, antes y durante la pandemia por COVID-19. *Archivos de Prevención de Riesgos Laborales*, 25(2), 133-146. <https://doi.org/10.12961/aprl.2022.25.02.06>
- Betancur, C. M. M., & Bedoya, A. F. R. (2022). Teletrabajo y trabajo en casa: Tendencias contemporáneas de contratación laboral en Colombia*. *Vniversitas*, 71. <https://www.redalyc.org/journal/825/82570824020/html/>
- Caamaño Rojo, E. (2010). El teletrabajo como una alternativa para promover y facilitar la conciliación de responsabilidades laborales y familiares. *Revista de derecho (Valparaíso)*, 35, 79-105. <https://doi.org/10.4067/S0718-68512010000200003>
- Cataño, & Gómez. (2014). El concepto de teletrabajo: Aspectos para la seguridad y salud en el empleo: The concept of telecommuting: aspects for health and safety in employment. *Revista CES Salud Pública*, 5(1), 82-91. <https://search.ebscohost.com/login.aspx?direct=true&db=lth&AN=98680251&lang=es&site=ehost-live>
- Chacchi, D. V. G., Sotelo, C. G. M., Pacherrres, M. Á. A., Castañeda, M. L.-, Pacherrres, P. A., y Pacherrres, J. H. A. (2024). Telework in Administrative Management within the Framework of the SDG, in a Peruvian Public Institution. *Journal of Lifestyle and SDGs Review*, 4(1), e01957-e01957. <https://doi.org/10.47172/2965-730X.SDGsReview.v4.n00.pe01957>

- Chinchay, D. J. G. (2023). Need for inclusion of social determinants and effective mental health approach. A critical look at the Peruvian telework legislation. *Revista Oficial del Poder Judicial*, 15(20), 163-208. Scopus. <https://doi.org/10.35292/ropj.v15i20.810>
- Daga & Gonzales, R. A. (2022). Remote Work and Digital Disconnection: Implementation and Regulation in the Peruvian Public Sector. *Boletín Mexicano de Derecho Comparado*, 55(165), 93-119. Scopus. <https://doi.org/10.22201/ijj.24484873e.2022.165.18607>
- Escalante, Mejías, & Martínez. (2020). Gestión de la Administración Escolar en el Desarrollo de Actividades Académicas: Mirada en Tiempos de Pandemia. *Revista Scientific*, 5(18), Article 18. <https://doi.org/10.29394/Scientific.issn.2542-2987.2020.5.18.1.24-45>
- Espinoza, L. A., & Sáurez, K. R. (2020). Actividad física y tiempos de comida en teletrabajadores y trabajadores presenciales de una universidad estatal de Costa Rica. *UNED Research Journal / Cuadernos de Investigación UNED*, 12(2). <https://www.redalyc.org/journal/5156/515664454021/>
- Gómez, S., Guarín, I., Uribe, S. L., y Vergel, L. (2020). Prevención de los peligros y promoción de entornos saludables en el teletrabajo desde la perspectiva de la salud pública. *AiBi Revista de Investigación, Administración e Ingeniería*, 8(1). <https://doi.org/10.15649/2346030X.802>
- Guayacán, I. N., Zárate Jiménez, A. L., y Contreras-Pacheco, O. E. (2022). Satisfacción laboral en el contexto del teletrabajo forzoso: Un estudio empírico en el sector de la educación superior. *Estudios Gerenciales*, 222-234. <https://doi.org/10.18046/j.estger.2022.163.4994>
- Havriluk, L. O. (2010). El Teletrabajo: Una opción en la era digital. *Observatorio Laboral Revista Venezolana*, 3(5), 93-109. <https://www.redalyc.org/articulo.oa?id=219014912006>
- Kajat, J. U., Aliaga, K. M. J. de, Dávila, J. G. V., Hidalgo, D. E. R. de C., Pérez, M. Á. B., y Campos, L. A. G. (2021). El trabajo remoto y la gestión de las emociones en tiempos de la COVID-19: Una mirada de estudiantes de maestría desde el rol de trabajadores, Lima-Perú (2020). *Industrial Data*, 24(1). <https://www.redalyc.org/journal/816/81668400009/html/>

- Lenguita, P. (2010). *Las reLaciones de teLetrabajo: Entre La protección y La reforma*.
- Martínez, L. P. A., Martínez, M. C. A., y Martínez, S. C. A. (2020). Seguridad y salud en el trabajo en teletrabajo autónomo en Colombia. *SIGNOS-Investigación en Sistemas de Gestión*, 12(1), 83-101. <https://www.redalyc.org/journal/5604/560465477005/>
- Morán, R. C. D., Agüero Corzo, E. D. C., Sánchez Soto, J. M., y López Gómez, H. E. (2022). Impact of Teleworking on the Health and Well-Being of Peruvian Workers in Times of Pandemic. *Sustainability (Switzerland)*, 14(23). Scopus. <https://doi.org/10.3390/su142315876>
- Muy Pérez, E. F. (2021). Los vacíos jurídicos de los riesgos laborales del teletrabajo en Ecuador. *Foro: Revista de Derecho*, 35, 27-46. <https://doi.org/10.32719/26312484.2021.35.2>
- Ortiz, E. R. A. (2022). El teletrabajo como mecanismo paradigmático del poder en las sociedades de control modernas. *Foro: Revista de Derecho*, 38, Article 38. <https://doi.org/10.32719/26312484.2022.38.10>
- Peláez, R. H. C., y López, D. H. (2013). *Teletrabajo con calidad de vida laboral y productividad. Una aproximación a un modelo en una empresa del sector energético*. <https://www.redalyc.org/pdf/646/64629832005.pdf>
- Pinto (2021). Teletrabajo como nuevo paradigma laboral. Algunos aspectos críticos de su regulación en Chile en relación a la seguridad de los trabajadores. *Revista de derecho (Valparaíso)*, 57, 31-66. <https://doi.org/10.4151/s0718-68512021000-1355>
- Ramírez, Tapia, Vega Abad, y Villagómez. (2021). Teletrabajo en Sudamérica: Un desafío jurídico frente al covid-19. *Revista Venezolana de Gerencia*, 26(94), 662-677. <https://doi.org/10.52080/rvgv26n94.12>
- Ramírez, Vega Abad, Narcisa Villagómez, Ramírez Velásquez, Vega Abad, y Narcisa Villagómez. (2022). Ventajas y desventajas del teletrabajo en Sudamérica frente a la pandemia del covid-19. *Civilizar Ciencias Sociales y Humanas*, 22(42). <https://doi.org/10.22518/jour.ccsch/20220107>

- Sánchez, & Mozo. (2009). Teletrabajo y vida cotidiana: Ventajas y dificultades para la conciliación de la vida laboral, personal y familiar. *Athenea Digital. Revista de Pensamiento e Investigación Social*, 15, 57-79. <https://www.redalyc.org/articulo.oa?id=53712929004>
- Sanchez & Toledo. (2021). *Efectos del teletrabajo sobre el bienestar de los trabajadores*. 30.
- Solís, J. I. C. (2021). El teletrabajo, la utilidad digital por la pandemia del COVID-19. *Revista latinoamericana de derecho social*, 32, 125-155. <https://www.redalyc.org/journal/4296/429671777006/html/>
- Tomasina, F., & Pisani, A. (2022). Pros and cons of teleworking in relation to the physical and mental health of the working general population: A narrative exploratory review. *Archivos de Prevencion Riesgos Laborales*, 25(2), 147-161. Scopus. <https://doi.org/10.12961/aprl.2022.25.02.07>
- Valencia, A. M. C. (2018). Aspectos regulatorios del teletrabajo en el Perú: Análisis y perspectivas. *REVISTA IUS*, 12(41). <https://doi.org/10.35487/rius.v12i41.2018.319>
- Vicente, M. T., Torres Alberich, J. I., Torres Vicente, A., Ramírez Iñiguez de la Torre, M. V., y Capdevila García, L. (2018). El teletrabajo en salud laboral. *Revista CES Derecho*, 9(2), 287-297. <https://dialnet.unirioja.es/servlet/articulo?codigo=6805230>
- Yeves, J., Bargsted, M., Orlandini, E., y Ureta, S. (2022). Flexibilidad Laboral en Pandemia y sus Efectos en Estrés, Inseguridad y Satisfacción Laboral. *Psykhē*, 33(1), Article 1. <https://doi.org/10.7764/psykhe.2021.41401>

SOMBRAS DIGITALES: EL CIBERCRIMEN Y SU AFECTACIÓN EN LA CIBERSEGURIDAD INTERNACIONAL

Luhana V. Rodríguez-Ramos¹

RESUMEN

Esta investigación tuvo como objetivo general diagnosticar la afectación del cibercrimen a la ciberseguridad, para ello se utilizó un estudio fundamental, con un diseño descriptivo y no experimental, que permitió analizar la problemática de manera integral, además, se realizó una revisión bibliográfica de 30 artículos científicos obtenidos de bases de datos como Scopus, Dialnet, Redalyc y SciELO. Los resultados fueron los delitos informáticos que conforman el cibercrimen, las principales afectaciones que genera el fenómeno del cibercrimen, la normativa internacional que regula el cibercrimen y la efectividad de las normativas de ciberseguridad en diferentes legislaciones internacionales. Como conclusión se obtuvo que se ha abordado la complejidad del cibercrimen, identificando sus diversas modalidades y el impacto significativo que tiene en ámbitos económicos, sociales y políticos, pues estos delitos no solo causan daños patrimoniales y psicológicos, sino que también afectan la confianza en las instituciones y procesos democráticos, lo que convierte la lucha contra el cibercrimen en un desafío global y si bien existen normativas internacionales como el Convenio de Budapest y esfuerzos de cooperación internacional, la rápida evolución de las tecnologías y la transnacionalidad de estos delitos requieren una actualización constante de los marcos legales y el fortalecimiento de las medidas de seguridad.

Palabras Claves: cibercrimen, delitos informáticos, ciberseguridad

¹ lrodriguezr2@upao.edu.pe

Programa de Estudio de Derecho, Universidad Privada Antenor Orrego

ABSTRACT

This research aimed to diagnose the impact of cybercrime on cybersecurity. A fundamental study was used with a descriptive, non-experimental design, which allowed for a comprehensive analysis of the issue. Additionally, a literature review of 30 scientific articles was conducted, sourced from databases such as Scopus, Dialnet, Redalyc, and SciELO. The results revealed the computer crimes that make up cybercrime, the main impacts caused by the phenomenon of cybercrime, the international regulations governing cybercrime, and the effectiveness of cybersecurity regulations in different international legislations. In conclusion, it was found that the complexity of cybercrime has been addressed by identifying its various modalities and the significant impact it has on economic, social, and political spheres. These crimes not only cause economic and psychological damage but also undermine trust in institutions and democratic processes, making the fight against cybercrime a global challenge. While there are international regulations such as the Budapest Convention and international cooperation efforts, the rapid evolution of technologies and the transnational nature of these crimes require constant updates to legal frameworks and strengthened security measures.

Keywords: cybercrimen, computer crimes, cybersecurity.

INTRODUCCIÓN

La sociedad, en su constante transformación, ha experimentado cambios profundos en múltiples áreas como la economía, la tecnología, lo social y lo cultural, entre ellos, la incorporación del Internet se presenta como un fenómeno revolucionario que redefinió las dinámicas humanas; sin embargo, en algunos países no se encuentra o se encuentra mal normado.

Como bien se mencionó, existen beneficios a ciencia cierta que demuestran que la era digital resultó ser esperanzadora, empero, la falta de regulación y un mal marco normativo establecido en algunos países trae a colación el retraso hacia una nueva transformación en la era telemática como un avance tecnológico (Escuela Superior Politécnica del Litoral, 2023, citado por De León, 2024).

En base a ello, el problema también radica en que la masificación del uso de Internet incrementó significativamente los riesgos de vulneración de bienes jurídicos, dado que muchos usuarios comparten su información personal en la red sin plena conciencia de las posibles consecuencias, tales como el cibercrimen, Valdez (2009) definió dicho término como un delito informático que utiliza internet u otras redes tecnológicas para llevar a cabo actividades

ilícitas, destacando cómo estas plataformas digitales se convierten en herramientas clave para transgredir la legalidad y el orden social.

En esa línea, complementando lo mencionado anteriormente, Miró (2012) señaló que el cibercrimen es una parte inherente de la realidad criminológica contemporánea, vinculada a los riesgos que conlleva el uso de las TIC, pues estas tecnologías, concebidas como un conjunto dinámico de herramientas para gestionar, intercambiar y comunicar información, han creado un entorno propicio para el desarrollo y constante adaptación del cibercrimen.

De esa manera, lo distintivo del cibercrimen radicaría en su dependencia del entorno digital, puesto que no solo amplía las posibilidades de perpetrar delitos a nivel global, sino que también plantea desafíos únicos para los sistemas de justicia, pues el anonimato y la rapidez que ofrece la tecnología dificultan la identificación y persecución de los responsables.

En cuanto a ello, es fundamental destacar que el cibercrimen, como fenómeno asociado al entorno digital, dio lugar a una amplia variedad de delitos informáticos que aprovechan las herramientas tecnológicas para vulnerar derechos y bienes jurídicos, puesto que estas actividades ilícitas se han diversificado junto con el avance de las TIC, afectando tanto a individuos como a instituciones, pues la capacidad de operar en un ámbito global y la dificultad de rastrear a los responsables han convertido a estos delitos en un desafío significativo para los sistemas de justicia.

Por ello, a modo de ejemplificar, resulta pertinente señalar que en América Latina, el entorno digital se transformó en un medio propicio para la comisión de delitos cibernéticos, como el *phishing*, la sextorsión y el ciberacoso, por lo que estas actividades ilícitas han generado un impacto significativo, vulnerando derechos fundamentales como el honor y la intimidad de las personas (Rojas & Yepes, 2022).

Asimismo, Rodríguez (2007, citado por Sánchez, 2012) señaló otros delitos que constituyen una problemática a la ciberseguridad, tales como, el fraude informático, el robo, la falsificación, el hacking, el espionaje, el sabotaje, la extorsión, la piratería comercial y otros crímenes vinculados a la propiedad intelectual, también la invasión de la privacidad, la difusión de contenido ilegal y perjudicial, la incitación a la prostitución y acciones que atentan contra la moral, así como actividades del crimen organizado, desarrollado en el ciberespacio.

Por un parte, en palabras de Cisco (2024, citado en Jiménez, 2024) la dificultad para identificar a los ciberdelincuentes aumenta los ciberdelitos, puesto que suelen utilizar servidores que les brindan una red privada virtual, lo cual enmascara su dirección IP y hace que rastrear su ubicación sea prácticamente imposible, además, emplean diversas herramientas para mantener su anonimato, esto dificulta aún más la labor de las autoridades y complica considerablemente la lucha contra el cibercrimen.

Por otra parte, Choo (2011, citado por Setiabudi, 2023) explicó que los ciberdelincuentes utilizan tecnología avanzada para crear programas maliciosos, como virus y malware, con el objetivo de atacar redes y sistemas esenciales en sectores clave como el financiero y energético, de forma que estos ciberataques no solo generan pérdidas económicas considerables, sino que también pueden afectar gravemente infraestructuras críticas, como las redes eléctricas y los sistemas de transporte, poniendo en riesgo el funcionamiento de servicios básicos.

Por lo que en ese contexto, es preciso señalar el caso emblemático de John Draper, un ingeniero arrestado en 1972 por fraude telefónico, tras descubrir que un silbato promocional de la empresa Quaker Oats emitía un tono de 2600 Hz que permitía manipular el sistema telefónico, de modo que gracias a ello, desarrolló la *blue box* que era un dispositivo usado para realizar llamadas gratuitas, lo que ocasionó pérdidas significativas a las compañías y marcó el inicio del *phreaking*, precursor del movimiento hacker (Fernández-Rodríguez *et al.*, 2019).

Ante dicha problemática, resulta evidente la falta de investigaciones exhaustivas que aborden el cibercrimen desde una perspectiva crítica, analizando de manera integral su impacto en la ciberseguridad a nivel internacional. Aquella carencia limita la comprensión de los riesgos asociados al uso de tecnologías digitales, así como las estrategias necesarias para prevenir y mitigar las amenazas, en ese sentido, se requiere un enfoque que no solo identifique las modalidades delictivas, sino que también examine la afectación respecto de del marco internacional.

Bajo esa óptica, mientras que el Derecho adopta un enfoque sancionador, actuando principalmente después de que el delito se ha consumado, su eficacia como herramienta preventiva es limitada y ello se debe a que muchas veces las personas que cometen delitos informáticos no se ven disuadidas por posibles sanciones, pues las probabilidades de identificar y procesar a los responsables son bajas, y los factores como el uso de identidades falsas

y puntos de conexión públicos dificultan la persecución penal, haciendo que los hackers operen sin preocuparse por las consecuencias legales inmediatas (Sain, 2017, citado por Parada y Errecaborde, 2018).

En ese contexto, la presente investigación se orienta a cumplir cuatro objetivos principales, primero, definir los delitos informáticos que conforman el cibercrimen, destacando sus características y modalidades; segundo, identificar las principales afectaciones que el fenómeno del cibercrimen genera en diversos ámbitos; tercero, examinar la normativa internacional vigente que regula el cibercrimen, analizando su alcance, y finalmente, estudiar la efectividad de las normativas de ciberseguridad implementadas en diferentes legislaciones internacionales.

El artículo propone una perspectiva novedosa al contemplar un análisis integral que combina la identificación de delitos cibernéticos, su afectación a ciberseguridad y el alcance de las normativas internacionales, por lo que esta aproximación permitirá no solo un entendimiento más profundo del fenómeno, sino también aportar conocimiento respecto a esta modalidad de criminalidad en el ámbito tecnológico.

METODOLOGÍA

Esta investigación emplea un enfoque cualitativo con el propósito general de abarcar el cibercrimen y su afectación en la ciberseguridad internacional, se trata de un estudio fundamental, con un diseño descriptivo y no experimental, que permite analizar la problemática de manera integral, de manera que el presente marco metodológico establece las bases necesarias para comprender las múltiples dimensiones del cibercrimen y su repercusión en la ciberseguridad internacional.

En ese sentido, Guerrero (2016) señaló que el enfoque cualitativo se basa en comprender los fenómenos y poder analizarlos desde el punto de vista de los sujetos que lo rodean; esto permitirá generar nuevas preguntas durante el proceso interpretativo, de manera que el presente enfoque permite una comprensión más profunda y flexible del tema en estudio, adaptándose a medida que emergen nuevos hallazgos o perspectivas.

Bajo ese contexto, es preciso señalar que esta investigación se desarrolló entre abril y noviembre de 2024, utilizando una revisión bibliográfica de 30 artículos científicos que fueron recopilados de bases de datos como Scopus, Dialnet, Redalyc y SciELO; lo cual sirvió para sintetizar

la información y verificar su actualidad, así como conocer el estado en el que se encuentra el tema a investigar (Pedráz, 2004). A su vez, se emplearon fichas bibliográficas seleccionadas en un Excel, en la cual se registraron datos clave como el año de publicación, revista, autores, país de origen, objetivos y conclusiones, en ese sentido, el análisis se realizó con un enfoque deductivo y una argumentación estructurada, permitiendo identificar la información concerniente al cibercrimen.

Por lo que, el esquema temático de la investigación abordó el cibercrimen desde cuatro perspectivas clave: primero, se definió a los delitos informáticos que conforman el cibercrimen, destacando sus características y modalidades; segundo, se identificó las principales afectaciones que el fenómeno del cibercrimen genera en diversos ámbitos; tercero, se examinó la normativa internacional vigente que regula el cibercrimen, analizando su alcance, y finalmente, se estudió sobre efectividad de las normativas de ciberseguridad implementadas en diferentes legislaciones internacionales.

RESULTADOS

1. Delitos informáticos que conforman el cibercrimen

El cibercrimen abarca una amplia gama de delitos informáticos que aprovechan las tecnologías digitales para cometer actos ilícitos, en ese caso, estos delitos no solo afectan a individuos, sino también a organizaciones y gobiernos, y pueden tener repercusiones graves tanto a nivel económico como social, lo que representa un desafío significativo para las autoridades y organismos encargados de la seguridad en el ciberespacio.

Pero, qué son los delitos informáticos en sí, para ello, resulta preciso indicar la perspectiva de Acosta *et al.* (2020), quien indicó que estos delitos corresponden a actos ilícitos que se cometen extrayendo información personal del ciberespacio y no solo afectan los entornos privados de las personas, sino que también generan daños patrimoniales, tanto a individuos como a empresas, debido al uso indebido de los datos obtenidos, además, suelen ser transfronterizos, lo que requiere respuestas rápidas y eficaces.

Bajo ese marco, corresponde analizar cada una de los delitos informáticos que se puede abordar según el bien jurídico protegido, tal como lo señala Parada y Errecaborde (2018), estos incluyen: a) violaciones a la intimidad: honor e integridad moral a través de redes sociales; b) el stalking: acoso en línea; c) ciberpornografía infantil: tráfico de material ilegal; d) delitos

contra la propiedad intelectual; y e) estafas y fraudes: que afectan el patrimonio de las víctimas, de modo que estos delitos reflejan la variedad de conductas ilícitas que se cometen en el ciberespacio.

En primer lugar, corresponde examinar el tema de las violaciones a la intimidad, honor e integridad moral a través de redes sociales, en donde existen espacios interactivos mediante los cuales se llega a vulnerar estos derechos mediante la difusión no consentida de contenido audiovisual muchas veces de connotación sexual (Machado *et al.*, 2020).

En segundo lugar, en cuanto al *stalking* o ciberacoso, también denominado *cyberbullying*, Cuesta *et al.* (2020, citado por Neyra, 2021) señalaron que esta práctica consiste en la hostigación constante de una persona a través de medios digitales, siendo su impacto inmediato, puesto que, mensajes, imágenes y videos ofensivos pueden difundirse rápidamente en redes sociales, exponiendo a las víctimas a insultos, burlas, suplantación de identidad y chantajes; agravando así el daño psicológico y social de las mismas.

En tercer lugar, sobre el tema de la ciberpornografía infantil y el tráfico de material ilegal, es crucial señalar que el presente delito constituye uno de los crímenes más graves contra los menores, pues involucra la producción, distribución, consumo de imágenes y videos con contenido sexual explícito en el que participan niños; en ese sentido, es que se generan adicciones que posteriormente podría repercutir en el comportamiento de los usuarios de la red, llevándolos a otros aspectos oscuros (Vega-Almeida y Arencibia-Jorge, 2019).

Al respecto, Negredo y Herrero (2016) señalaron que la creación, distribución y descarga de pornografía infantil establece un delito de creciente preocupación, vinculado al abuso sexual y la explotación de menores, pues las víctimas del presente crimen sufren graves secuelas en torno a su autoestima y su salud mental, además, la expansión de internet agravó dicho problema, permitiendo una distribución masiva y anónima del material, lo cual dificultaría tanto la identificación de los responsables como la eliminación de ese contenido de la red.

En cuarto lugar, el autor hace referencia a los delitos contra la propiedad intelectual, los cuales constituyen una grave infracción a los derechos de autor en el entorno digital, pues estas acciones incluyen la reproducción, distribución o modificación no autorizada de obras protegidas, como libros,

música, películas o software, aprovechando la facilidad que ofrece internet para acceder y compartir contenido sin consentimiento (Tapia, 2022).

Por último, otro delito informático relevante es la estafa y el fraude, que perjudican el patrimonio de las víctimas mediante actividades ilegales realizadas en el entorno digital; en ese sentido, Bustos (2023) refirió que dicho delito es un injusto que mantiene como tal su origen en la estafa como delito contra el patrimonio, empero, lo único que cambió sería la modalidad para cometerlo “medios informáticos” convirtiéndose así en un nuevo ilícito penal”.

Según Sánchez (2012), los ciberdelincuentes utilizan internet para cometer fraudes y obstruir sistemas en busca de beneficios económicos ilegítimos que les permite operar de forma dispersa y difícil de rastrear, en ese contexto, el fraude en línea incluye el robo de identidad, donde organizaciones suplantan a otras para robar información confidencial, representando así una amenaza social.

Adicionalmente a ello, también existe otro delito que posteriormente se convirtió en informático, el cual resulta pertinente señalar en aras de una mayor investigación, el cual es, el espionaje, que refiere ser una actividad enfocada en recopilar información para transmitirla a otra persona o entidad, siendo esta relevante por su valor táctico o estratégico, y generalmente de naturaleza confidencial (Lara, 2024).

Ahora abarcando sobre el espionaje informático, se puede decir que se relaciona con el concepto de “violación de secretos”, el cual puede manifestarse de dos maneras, por un lado, mediante la intromisión indebida en ámbitos protegidos de información confidencial, y por otro, a través de la divulgación no autorizada de secretos a los que se tuvo acceso de forma legítima, implicando así un grave quebrantamiento de la confianza y la protección de datos (Etcheberry, 2010, citado en Mayer y Vera, 2020).

Desde ese punto de vista, los culpables se aprovechan de los fallos de seguridad, infecciones de malware o utilizan los sofisticados métodos de piratería, como el phishing, la ingeniería social o el uso de troyanos para realizar su cometido, por ello a menudo ese delito está relacionado con la obtención de secretos de estado o datos confidenciales de competidores internacionales.

No obstante, debido a que el espionaje informático arruinó la vida de las víctimas, la seguridad global y la integridad corporativa; las personas que

cometieron estos delitos se enfrentaron a graves consecuencias, que iban desde cuantiosas multas hasta largas penas de prisión, según el tipo de delito cometido y el ámbito del derecho, por lo que esta manera de transgresión aceleró el establecimiento de regulaciones globales de ciberseguridad para proteger tanto al sector público como al privado.

Por otro lado, también resulta fundamental mencionar al ciberterrorismo, como otra forma de delito, que utiliza tecnologías digitales con fines terroristas, causando daño, de modo que, los ataques pueden dirigirse a infraestructuras críticas, como redes de energía y sistemas financieros, utilizando tácticas como malware, sabotaje, secuestro de datos y difusión de desinformación, esto genera caos y miedo en la sociedad.

En relación con ello, Nieto (2018) definió el ciberterrorismo como un ataque deliberado y con motivaciones políticas dirigido contra información, sistemas informáticos, software y datos, con el propósito de generar violencia contra objetivos civiles, llevado a cabo por grupos subnacionales o actores clandestinos.

En explicación a ello, los grupos terroristas han adaptado el ciberespacio como una herramienta clave para llevar a cabo diversas actividades, como la recaudación de fondos, el reclutamiento de seguidores, la planificación y coordinación de ataques, la formación de sus miembros, la propaganda, causando así desconcierto en diversas sociedades.

Por lo tanto, se concluye que el ciberterrorismo representa una amenaza significativa para la seguridad internacional, dado que los ataques pueden ser realizados desde cualquier parte del mundo, afectando tanto a gobiernos como a empresas y ciudadanos, es así que las medidas de ciberseguridad y cooperación internacional se han convertido en elementos fundamentales para prevenir y combatir todo tipo de amenaza.

2. Principales afectaciones que genera el fenómeno del cibercrimen

El fenómeno del cibercrimen transformó profundamente la manera en que se perciben y enfrentan las amenazas en el entorno digital, generando múltiples afectaciones tanto individuales como colectivas, pues dicho tipo de criminalidad impacta derechos fundamentales, como la privacidad, el honor y la seguridad, al tiempo que compromete la integridad de datos personales y financieros, además, fomenta un clima de desconfianza en el uso de tecnologías y redes, obstaculizando el desarrollo social y económico, por ello, es crucial examinar las principales consecuencias que el referido fenómeno acarrea.

Bajo esa óptica, los autores Rayón y Gómez (2014) conceptualizan que el desarrollo de Internet y las tecnologías de la información, así como las comunicaciones relacionadas ha convertido el ciberespacio en un entorno en donde se violan diversos derechos fundamentales básicos, lo cual incluye la privacidad, el honor, la propiedad, la libertad sexual e incluso el derecho a la integridad física y a la vida.

En la misma línea, los autores quieren dar a conocer que la evolución del internet y las tecnologías de la información transformaron el ciberespacio en un lugar donde los derechos fundamentales están en constante vulnerabilidad; al mencionar derechos como la privacidad, el honor, la propiedad y la libertad sexual, se subraya que actividades en línea podrían generar riesgos significativos, desde la exposición indebida de datos personales hasta situaciones graves como el ciberacoso.

Por otro lado, se puede decir que diversas naciones sufrieron una afectación de manera multidimensional a causa del cibercrimen, siendo que ésta dependería del caso y de la intención que tendría el delincuente (Izaguirre & León, 2018). De esa idea se interpreta que el impacto del cibercrimen en una sociedad es amplio y diverso, afectando múltiples dimensiones, como la económica, social, política y de seguridad.

A partir de la mencionada problemática, el gasto mundial hasta el año 2017 reflejó que se habría invertido 86.400 millones de dólares de acuerdo a la consultoría tecnológica Gartner, puesto que los países buscaban protegerse ante el cibercrimen, el cual llega a ser generador de ciertas implicancias en un Estado (Oficina Económica y Comercial de España, 2018).

En ese sentido, el aumento en el presupuesto destinado a ciberseguridad respondería a la necesidad de proteger datos y fortalecer la confianza de los usuarios, consolidándose como una prioridad global, en ese contexto, la UIT (2010, citada por Ormachea, 2020) define la ciberseguridad como el conjunto de herramientas, políticas y medidas destinadas a gestionar los riesgos de seguridad, con el fin de proteger los activos de organizaciones y usuarios del ciberespacio.

No obstante a la inversión, la ciberseguridad se haya vulnerada constantemente por amenazas que impulsan a las víctimas y su círculo cercano, a implementar medidas de autoprotección para reducir el riesgo de futuros ataques, lo que evidencia que las estrategias institucionales, aunque necesarias, no siempre son suficientes para garantizar la protección total en el entorno digital.

Por otro lado, a nivel social, el cibercrimen alteró significativamente la percepción de seguridad de la ciudadanía, pues con el auge de las redes sociales y la creciente dependencia de los servicios digitales, la población se vió cada vez más vulnerable ante amenazas como el ciberacoso, el robo de datos personales y los fraudes en línea, de tal manera que dicho panorama generó una mayor inquietud y desconfianza en el entorno digital, afectando la tranquilidad de los usuarios.

De esta manera, se creó una atmósfera de desconfianza, afectando la vida cotidiana de las personas produciendo un impacto psicológico negativo, especialmente en los sectores más jóvenes y en aquellos menos capacitados en seguridad digital quienes no sabían como afrontar una problemática de tal magnitud.

Por otro lado, el temor no está necesariamente relacionado con la cantidad de casos de cibercrimen, sino con una percepción cualitativa que tiende a exagerar sus consecuencias, pues para los usuarios, el cibercrimen puede percibirse como algo incontrolable o enigmático, lo que aumenta su ansiedad, debido a que en gran parte, existe desconocimiento o la falta de comprensión sobre las verdaderas características y riesgos del cibercrimen.

Finalmente, en el ámbito político, el cibercrimen causó consecuencias significativas, dado que las campañas de desinformación y los hackeos estratégicos, utilizados para manipular resultados electorales o influir en la opinión pública, socavaron la confianza en los procesos democráticos y generaron tensiones entre países, asimismo, estas amenazas llevaron a los gobiernos a destinar recursos y esfuerzos considerables en mejorar la ciberseguridad nacional, colaborando, en muchos casos, con otras naciones para abordar el cibercrimen como un desafío transnacional que afecta la estabilidad global.

Por lo tanto, el cibercrimen reveló vulnerabilidades significativas en la economía, la seguridad social y los sistemas políticos globales, dada la constante amenaza digital ha obligado a gobiernos y empresas a destinar recursos considerables a la ciberseguridad, mientras que ha generado desconfianza en los usuarios, afectando su percepción de seguridad en línea a nivel mundial.

3. Normativa internacional que regule el cibercrimen

La regulación del cibercrimen a nivel internacional se considera un desafío constante debido a la naturaleza transnacional de los delitos

digitales, no obstante, es pertinentes examinar las diversas normativas y convenios que existen y que buscan establecer marcos legales para prevenir y sancionar las actividades delictivas en el ciberespacio. Entre los principales instrumentos internacionales se encuentran la Convención de Budapest sobre Cibercriminalidad, adoptada por el Consejo de Europa y la Organización Internacional de Policía Criminal (INTERPOL), en ese sentido, abordaré cada una de la siguiente manera:

Por un lado, Chicharro (2009) refirió que en Europa, la Convención sobre Cibercrimen, es uno de los tratados internacionales más inclusivos que las naciones han llevado a cabo para abordar el crimen computacional, sus bases se encuentran creadas bajo la pretensión de crear un estado unificado bajo el cual combatir el crimen cibernético, pues contiene obligaciones en tres áreas: normas penales sustantivas, procedimientos penales y cooperación internacional.

En cuanto a las normas penales sustantivas, la convención describe los tipos penales que los estados deben implementar en sus sistemas legislativos para castigar los delitos de ciberdelincuencia, por ejemplo: el acceso ilegal y la alteración de datos. Por su parte, los procedimientos penales contienen herramientas y acciones relativas al proceso de investigación del crimen computarizado, como la recolección y la preservación de pruebas digitales.

Asimismo, en cuanto al ámbito de cooperación internacional, el tratado contribuye al hecho de que los países cooperen en la investigación y enjuiciamiento penal, lo que es fundamental en el caso de un crimen en un entorno digital, puesto que no conoce fronteras. Por consiguiente, dicho tratado es también aplicable a un ataque cibernético terrorista, debido que las disposiciones del tratado son útiles cuando un acto terrorista se realiza contra un sistema de computación o utilizando un sistema de computación en pos de dicho acto.

Por otro lado, la INTERPOL, juega un rol crucial al facilitar la cooperación internacional, pues su alcance global le permite coordinar operaciones policiales y fomentar alianzas multisectoriales, además de proporcionar plataformas seguras para el intercambio de información, asimismo, apoya a sus países miembros con análisis, formación y recursos, aumentando su capacidad para prevenir, detectar, investigar y combatir los ciberdelitos, contribuyendo así a un entorno digital más seguro para las comunidades en todo el mundo.

Ahora bien, es importante destacar cómo los países abordan esta problemática a través de sus normativas nacionales, dado que la regulación interna juega un papel esencial en la lucha contra el cibercrimen, pues cada nación busca equilibrar la protección de derechos fundamentales con la lucha contra las amenazas digitales.

Partiendo de ese punto, Rojas (2016) destacó que en España, el delito de “delincuencia informática” está tipificado en la Ley Orgánica 10/1995, de 23 de noviembre, señalando que uno de los delitos más graves en esta categoría es la alteración o reproducción de tarjetas de crédito o débito, por lo cual esta tipificación refleja el compromiso de España con la protección frente a delitos digitales.

De acuerdo a ello, se resalta cómo España integró en su marco legal mecanismos específicos para enfrentar los delitos informáticos, adaptándose a los riesgos que surgen con el avance de las tecnologías; y al señalar que la falsificación o manipulación de tarjetas de crédito o débito es uno de los delitos más graves en esta categoría, pone de manifiesto la importancia de proteger la economía y la confianza en los sistemas digitales.

En cuanto a República Dominicana, el cibercrimen se clasifica como crímenes y delitos de alta tecnología, y su principal objetivo es la protección de las tecnologías de la información y la comunicación; además, se aborda una amplia gama de delitos como el sabotaje y la comisión de actos terroristas mediante el uso de sistemas electrónicos, de modo que al tipificar estos crímenes, la ley buscaría proteger los derechos fundamentales de los ciudadanos frente a las amenazas cibernéticas (Rojas, 2016).

Resulta fundamental resaltar que, aunque República Dominicana avanzó en la regulación del cibercrimen, sigue enfrentando desafíos en la implementación efectiva de estas normativas, pues la rapidez con la que evolucionan las tecnologías plantea la necesidad de adaptaciones constantes en la legislación.

En ese contexto, el mismo autor, refirió que en Panamá, la Ley 14 de 2007, tipifica los delitos informáticos en el Título VIII, que abarca los delitos contra la seguridad jurídica de los medios electrónicos y los delitos sexuales. Dicha normativa logra establecer sanciones específicas para delitos relacionados con el uso indebido de la tecnología, tales como la producción y distribución de material pornográfico infantil y el uso de Internet con fines terroristas.

Por ende, la referida legislación también penaliza severamente la creación, distribución o exhibición de material pornográfico que involucre a menores de edad, ya sea en actividades sexuales reales o simuladas, así como el uso de internet para fines ilícitos, como la capacitación en la fabricación de explosivos o el reclutamiento de personas con fines terroristas.

En Perú, el autor refiere que el cibercrimen se encuentra regulado por la Ley N° 30096, conocida como la Ley de Delitos Informáticos, asimismo, tiene como objetivo prevenir y sancionar delitos cometidos mediante tecnologías de la información, protegiendo los sistemas informáticos y otros bienes jurídicos frente a las amenazas digitales, de manera que su enfoque integral busca combatir la creciente incidencia de ciberdelincuencia en el país.

Por tanto, la regulación del cibercrimen es un desafío global que requiere la cooperación internacional y una armonización de normativas nacionales para ser efectiva, y aunque países como España, República Dominicana, Panamá, Perú y Colombia han adoptado leyes específicas para enfrentar delitos informáticos, la rápida evolución de la tecnología plantea dificultades en la implementación y actualización de las referidas normativas.

Es por ello, que la cooperación internacional, como la promovida por la Convención de Budapest y la INTERPOL, juega un papel fundamental en la lucha contra el cibercrimen, sin embargo, es esencial que cada nación ajuste su legislación para equilibrar la protección de los derechos fundamentales con la lucha contra las amenazas digitales, asegurando una respuesta efectiva y oportuna a los delitos transnacionales.

4. Efectividad de las normativas de ciberseguridad en diferentes legislaciones internacionales

La lucha contra el cibercrimen resulta ser un desafío global que requiere esfuerzos coordinados entre naciones, y aunque existen normativas internacionales como el Convenio de Budapest, aún persisten obstáculos en la implementación y efectividad de las leyes a nivel local, las cuales merecen una solución rápida.

Para reforzar la idea planteada Lorenzana (2021) refirió que resulta necesario asumir que se debe hacer un esfuerzo para poder afrontar retos tan dispares como comprender el estado del arte del cibercrimen, revisar la estrategia de lucha contra dicho fenómeno, y establecer colaboraciones entre varias personas para afrontarlo.

Bajo ese panorama, Jimenez (2024) mencionó que una de las medidas que se pueden optar es filtrar los datos ingresados mediante la web en un servidor privado, lo cual implicaría que se le daría importancia a la protección y gestión de la información almacenada, posiblemente para evitar accesos no autorizados o errores en los datos, asegurando así un mayor nivel de seguridad y precisión en la información que se guardaba.

Asimismo, el autor señaló la eliminación inmediata de contenido ilegal para evitar la complicidad de los Proveedores de Servicios de Internet (ISP) en la comisión de delitos y destacó el uso de tecnologías avanzadas como las redes neuronales, conocidas como “deep learning”, que permiten identificar contenidos ilícitos antes de su publicación, asegurando una mayor precisión en la protección de la información.

Por otra parte, Toro (2023) destacó que sería posible reducir la victimización secundaria y permanente en línea, mediante la educación de los ciudadanos sobre las consecuencias del crimen en Internet, en ese sentido, subrayó la importancia de implementar medidas como el “derecho al olvido”, que permite la eliminación definitiva de datos irrelevantes de la red, asegurando que no quede ningún rastro de información.

Considerando lo anteriormente citado, existen diversas estrategias y métodos para enfrentar el cibercrimen; sin embargo, alcanzar un sistema completamente infalible a nivel global es prácticamente imposible debido a las limitaciones de la nueva tecnología. Aunque dichos mecanismos están automatizados, el sistema puede fallar, entonces, partiendo de esta idea, se entiende que a pesar de los esfuerzos por mantenerlos actualizados, la injerencia de servicio en internet no es infalible (Jimenez, 2024).

Por ello, Megías (2019) destacó que los delincuentes cibernéticos emplean herramientas como la esteganografía, la cual se define como una técnica que permite ocultar información dentro de una imagen, un archivo de audio, un video o incluso un texto; de acuerdo a ello, es casi imposible saber hasta qué punto los criminales y los terroristas se encontraban utilizando dichos mecanismos.

De ello, se destaca que uno de los principales obstáculos para el seguimiento de los ciberdelincuentes es su capacidad para cambiar constantemente sus nombres de usuario y ubicaciones en tiempo real, de tal forma que dicho cambio es fácil de realizar, lo que les permite alterar su localización y dificultar el rastreo de sus actividades en línea, por lo cual esta flexibilidad

aumenta la complejidad de la vigilancia y de las estrategias para prevenir el cibercrimen.

Un problema constante, según lo refiere Toro (2023) sería que, como tal en los ciberdelitos, las penas severas que se aplican en situaciones comunes no sería lo más factible, puesto que la complicada persecución y la lentitud de las investigaciones resultan un problema al momento de emitir alguna sentencia.

Entonces, uno de los principales motivos de esta ineficacia es que tanto las leyes como los profesionales siguen enfrentando dificultades para rastrear y capturar a los delincuentes virtuales. Por lo tanto, es necesario adoptar enfoques más específicos que tomen en cuenta diversos factores, así como la gravedad de los daños causados a las víctimas, para lograr una respuesta más efectiva y ágil frente a los referidos delitos.

Para reforzar la idea, se presenta como tal un posible enfoque, el cual sería “Detectar-Investigar-Responder”, ello se basaría en el componente denominado como “Adapt”, el cual se basaría en el enfoque de de Inteligencia de Seguridad (SI), lo que permitiría una veloz respuesta a las vulneraciones que lleguen a presentarse (Castillo, 2019).

En ese contexto, y para seguir con la mejoría de la ciberseguridad en un mundo de cibercrimen, se realizaron actividades, tales como la International CyberEx, la cual consistió en la ejecución de un ejercicio virtual en donde se buscaría aumentar las capacidades de respuesta ante incidentes, mejorando la cooperación entre los sujetos (Rubio, 2019).

Por lo tanto, la efectividad de las normativas de ciberseguridad a nivel internacional sigue enfrentando grandes desafíos debido a la rápida evolución tecnológica y la complejidad del cibercrimen, y aunque instrumentos como el Convenio de Budapest han sentado bases importantes para la cooperación global, su implementación práctica y alcance siguen siendo limitados, especialmente en países que no lo han ratificado formalmente, asimismo, las estrategias actualizadas, como el aumento de penas y la cooperación internacional, son avances significativos, no abordan plenamente la naturaleza dinámica y globalizada del cibercrimen.

Por lo cual, es evidente que para lograr un impacto más significativo se necesitan enfoques integrales que combinen normativas actualizadas, tecnología avanzada y una colaboración internacional sólida, y resulta crucial diferenciar los delitos cibernéticos de los tradicionales, adaptando

las leyes y las penas a la naturaleza específica de estos crímenes, pues sólo a través de un marco legal armonizado, será posible avanzar hacia una ciberseguridad más robusta y proteger tanto a las víctimas como a los sistemas vulnerables ante dichas amenazas.

CONCLUSIONES

- Se definió a los delitos informáticos que conforman el cibercrimen, destacando sus características y modalidades; los cuales abarcan desde violaciones a la intimidad y ciberacoso hasta la ciberpornografía infantil, el espionaje informático y el ciberterrorismo, todos los cuales evidencian la vulnerabilidad del entorno digital frente a actos ilícitos que afectan tanto a individuos como a organizaciones y gobiernos, de manera que estos delitos no solo generan daños patrimoniales, psicológicos y sociales, sino que también representan un desafío global debido a su naturaleza transfronteriza y el uso de tecnologías avanzadas para su ejecución.
- Se identificó las principales afectaciones que el fenómeno del cibercrimen genera en diversos ámbitos, en el ámbito económico, ocasiona pérdidas a empresas y gobiernos, y demanda inversiones en ciberseguridad; en lo social, deteriora la percepción de seguridad y afecta psicológicamente a grupos vulnerables; y en lo político, debilita la confianza en procesos democráticos mediante hackeos y desinformación, por lo que dicho panorama exige medidas integrales como cooperación internacional, educación en ciberseguridad y estrategias efectivas de mitigación.
- Se examinó la normativa internacional vigente que regula el cibercrimen, analizando su alcance, destacando instrumentos como la Convención de Budapest y la labor de la INTERPOL en la cooperación global, y aunque países como España, República Dominicana, Panamá, Perú y Colombia han implementado leyes específicas, la rápida evolución tecnológica exige actualizaciones constantes, pues la armonización de normativas y la cooperación internacional son esenciales para combatir eficazmente el cibercrimen, protegiendo derechos fundamentales y fortaleciendo la seguridad digital.
- Se estudió la efectividad de las normativas de ciberseguridad en diversas legislaciones internacionales, destacando avances como el Convenio de Budapest, el fortalecimiento de penas, el uso de tecnologías avanzadas y la cooperación internacional, sin embargo, estas medidas aún no logran

abordar completamente la complejidad del cibercrimen debido a la rápida evolución de las amenazas y las dificultades en su implementación, por lo tanto, es crucial adoptar un enfoque integral que combine marcos legales armonizados, innovación tecnológica y esfuerzos colaborativos, con el fin de lograr una ciberseguridad más sólida y eficaz.

REFERENCIAS BIBLIOGRÁFICAS

- Acosta, M. G., Benavides, M. M., y García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 25(89). <https://www.redalyc.org/journal/290/29062641023/html/>
- Bustos, M. (2023). La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal. *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, 38, 6.
- Castillo, C. (2019). Ciberseguridad: Por dónde Empezar.... *Revista de Tecnología*, 18(1), 89-100.
- Chicharro, A. (2009). La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas.
- De León, D. (2024). Transformación digital como factor de cambio de la matriz productiva de Ecuador. *Economía y Desarrollo*, 168(2). http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S0252-85842024000200014&lng=es&nrm=iso&tlng=es
- Fernández-Rodríguez, J., Muñoz, F., y Cuevas, L. (2019). Perfil psicosociológico en el ciberdelincuente. *RICSH Revista Iberoamericana de las Ciencias Sociales y Humanísticas*, 8(16), Article 16. <https://doi.org/10.23913/ricsh.v8i16.179>
- Guerrero, M. (2016). La Investigación Cualitativa. *INNOVA Research Journal*, 1(2), 1-9.
- Izaguirre, J., y León, F. (2018). Análisis de los Ciberataques realizados en América Latina. *INNOVA Research Journal*, 3(9), 180-189.
- Jimenez, L. (2024). El estado actual del cibercrimen en Perú y el derecho alemán. *Boletín Mexicano de Derecho Comparado*, 197-219. <https://doi.org/10.22201/ij.24484873e.2023.167.18367>
- Lara, R. (2024). El delito de espionaje en México. *Tla-melaua: revista de ciencias sociales*, 56, 3.

- Lorenzana, C. (2021). Año 2021 en la lucha contra el Ciberdelito...: Cambiar o Morir. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 30(143 (Febrero 2021)), 98-101.
- Machado, M., Mainato, K., y Núñez, A. (2020). La violación del derecho a la intimidad por medio de las redes sociales. Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas y Criminológicas, 5(Extra 3), 468-480.
- Mayer, L., y Vera, J. (2020). El delito de espionaje informático: Concepto y delimitación. Revista Chilena de Derecho y Tecnología, 9(2), Article 2. <https://doi.org/10.5354/0719-2584.2020.59236>
- Megías, D. (2019). Los secretos que oculta la red: Esteganografía y ciberdelito: ¿hay motivos para la alarma? Telos: Cuadernos de comunicación e innovación, 88-93.
- Miró, F. (2012). El ciberdelito: Fenomenología y criminología de la delincuencia en el ciberespacio. Ediciones Jurídicas y Sociales. <https://dialnet.unirioja.es/servlet/libro?codigo=756351>
- Negro, L., y Herrero, Ó. (2016). Pornografía Infantil En Internet. Papeles del Psicólogo, 37(3), 217-223.
- Neyra, O. (2021). Cyberbullying: El acoso escolar en el ciberespacio e implicancias psicológicas. HAMUTAY, 8(1), Article 1. <https://doi.org/10.21503/hamu.v8i1.2238>
- Nieto, I. (2018). La letalidad del ciberterrorismo. Revista general de marina, 275(7), 133-142.
- Oficina Económica y Comercial de España. (2018). Inversión estratégica en el sector de la ciberseguridad: El caso israelí. Boletín Económico de ICE, 3096, Article 3096. <https://doi.org/10.32796/bice.2018.3096.5690>
- Ormachea, J. (2020). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. Revista de Ciencia e Investigación en Defensa, 1(4), Article 4. <https://doi.org/10.58211/recide.v1i4.36>
- Parada, R., y Errecaborde, J. (2018). Ciberdelito y delitos informáticos: Los nuevos tipos penales en la era de Internet [Recursos electrónicos]. Erreius.

- Pedráz, A. (2004). La revisión bibliográfica. NURE investigación: Revista Científica de enfermería, 2, 7.
- Rayón, M. C., y Gómez, J. A. (2014). Cibercrimen: Particularidades en su investigación y enjuiciamiento. Anuario jurídico y económico escurialense, 47, 209-234.
- Rojas, J. (2016). Análisis de la penalización del cibercrimen en países de habla hispana. Revista Logos Ciencia & Tecnología, 8(1), 220-231. <https://doi.org/10.22335/rlct.v8i1.339>
- Rojas, J., y Yepes, J. (2022). Panorama de riesgos por el uso de la tecnología en América Latina*. Trilogía Ciencia Tecnología Sociedad, 14(26). <https://www.redalyc.org/journal/5343/534369208004/html/>
- Rubio, Y. (2019). Los claroscuros de la ciberseguridad. Tribuna Norteamericana, 30, 16-21.
- Sánchez, G. (2012). Ciberespacio Y El Crimen Organizado. Los Nuevos Desafíos Del Siglo Xxi. Revista Enfoques: Ciencia Política y Administración Pública, X(16), 71-87.
- Setiabudi, W. (2023). CYBERCRIME AND GLOBAL SECURITY THREATS: A CHALLENGE IN INTERNATIONAL LAW. Russian Law Journal, 11(3), Article 3. <https://doi.org/10.52783/rlj.v11i3.1112>
- Tapia, D. (2022). Control penal de las infracciones contra la propiedad intelectual. Revista de Investigación de la Academia de la Magistratura, 4(6), Article 6. <https://revistas.amag.edu.pe/index.php/amag/article/view/rev.amag.2022.v4n6.04>
- Toro, M. (2023). El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión. Revista Logos Ciencia & Tecnología, 15(2), 162-173. <https://doi.org/10.22335/rlct.v15i2.1768>
- Valdez, A. (2009). Revista de Información, Tecnología y Sociedad—El Cibercrimen. http://revistasbolivianas.umsa.bo/scielo.php?pid=S1997-40442009000200030&script=sci_arttext&tlng=es
- Vega-Almeida, R., y Arencibia-Jorge, R. (2019). El lado oscuro de Internet: Un estudio bibliométrico de la literatura sobre comportamientos adictivos en línea. Revista española de documentación científica, 42, 251.

EL DERECHO A LA PRIVACIDAD Y PROTECCIÓN DE DATOS EN LA SOCIEDAD DE INFORMACIÓN DIGITAL

Ibeth Nayeli Vargas Reyna¹

RESUMEN

Esta investigación tuvo como objetivo analizar los elementos fundamentales de los datos personales y la privacidad. Bajo un enfoque cualitativo, con un diseño de investigación básica, no experimental y descriptiva, para la recolección de información, se consultaron bases de datos académicas como Redalyc, Scopus y Dialnet, obteniendo un total de 35 artículos relevantes. Entre los principales hallazgos se destacan el origen del derecho a la privacidad y la protección de datos, las principales amenazas en el ámbito digital, el marco legal que regula estos aspectos y la relevancia de garantizar la seguridad de la información personal. En conclusión, se determinó que la protección de datos y la privacidad en línea son fundamentales en la sociedad actual, especialmente en un contexto marcado por el avance tecnológico y la globalización, donde el flujo constante de información personal aumenta los riesgos de exposición, uso indebido y vulneraciones a la seguridad digital. Por ello, resulta esencial contar con marcos normativos claros y actualizados, junto con mecanismos de supervisión eficientes, para garantizar la protección de los derechos individuales ante estas amenazas.

Palabras Clave: Derecho a la privacidad; Privacidad; Protección de Datos; Información digital.

¹ Ivargasr2@upao.edu.pe

<https://orcid.org/0009-0004-3197-2424?lang=es>

Programa de estudio de Derecho, Universidad Privada Antenor Orrego

ABSTRACT

This research aimed to analyze the fundamental elements of personal data and privacy. Under a qualitative approach, with a basic, non-experimental and descriptive research design, for the collection of information, academic databases such as Redalyc, Scopus and Dialnet were consulted, obtaining a total of 35 relevant articles. Among the main findings are the origin of the right to privacy and data protection, the main threats in the digital field, the legal framework that regulates these aspects and the relevance of guaranteeing the security of personal information. In conclusion, it was determined that data protection and online privacy are fundamental in today's society, especially in a context marked by technological advancement and globalization, where the constant flow of personal information increases the risks of exposure, misuse and violations of digital security. Therefore, it is essential to have clear and updated regulatory frameworks, along with efficient supervision mechanisms, to guarantee the protection of individual rights against these threats.

Keywords: Right to Privacy; Privacy; Data Protection; Digital Information.

INTRODUCCIÓN

El derecho a la protección de datos personales está estrechamente vinculado al crecimiento de la economía digital, el internet y las tecnologías de la información, sin embargo, sus antecedentes pueden rastrearse hasta fallos relevantes, como la sentencia de 1983 del Tribunal Constitucional Federal Alemán. Dicha resolución, basada en los principios de dignidad humana y libre desarrollo personal, expandió los derechos de la personalidad y estableció el derecho a la autodeterminación informativa, otorgando a los individuos la facultad de decidir sobre el manejo de sus datos personales (Mendoza, 2021).

En este mismo contexto, garantizar el desarrollo pleno de cada persona dentro de su entorno requiere la protección de sus datos personales, no obstante, este derecho ha sufrido ciertas limitaciones en el ámbito digital, especialmente en relación con la libertad de expresión en internet y en relación con los menores de edad; de acuerdo con las normativas nacionales e internacionales, los menores requieren una protección prioritaria debido a su mayor vulnerabilidad. En este sentido, una gestión inadecuada de la información puede exponerlos a múltiples riesgos y atentar contra derechos como la privacidad, cuyo propósito es salvaguardar datos que el titular desea mantener en reserva (Ordóñez y Calva, 2020).

Asimismo, se debe tener en cuenta que la protección de los datos personales está marcada por profundas contradicciones, puesto que,

aunque crece la conciencia sobre su importancia para salvaguardar la privacidad y garantizar la libertad individual, cada vez resulta más complicado preservar su esencia debido a que estas herramientas no solo ofrecen oportunidades innovadoras, sino que también presentan desafíos significativos relacionados con la seguridad, la anonimización y el consentimiento informado (Castillejos *et al.*, 2016).

Las nuevas tecnologías han cambiado cómo nos comunicamos y accedemos a la información, se utilizan de manera indiscriminada y sin control, lo que se refleja en las inconformidades y desafíos actuales relacionados con la falta de regulación en su uso, afectando la interacción de los usuarios en internet, donde las responsabilidades por prácticas informales como la difusión de información sin autorización y el uso de redes sociales, constituyen una gran fuente de exposición de datos personales y elementos que forman parte de la vida privada (Moreno y Olmeda, 2021).

La salvaguarda de la información personal se vincula estrechamente con la protección del derecho a la privacidad, reconocido a nivel internacional como un derecho humano fundamental que garantiza la participación cívica en las naciones (Barinas, 2019). La ausencia de restricciones en el manejo de esta información pone en peligro la libertad individual y los valores fundamentales del sistema democrático, por lo cual debe considerarse un límite necesario para salvaguardar a las personas, debido que el abuso en la recolección de datos por terceros puede resultar en graves violaciones de derechos humanos (Nahabetián, 2015).

En definitiva, la protección de la vida privada abarca múltiples dimensiones relacionadas con la dignidad del individuo, como la posibilidad de desarrollar su personalidad, definir su identidad y establecer vínculos personales. Además, comprende elementos de la identidad tanto social como física, incorporando el derecho a la autodeterminación personal, lo que permite garantizar de manera efectiva la protección de los datos personales. Sin este resguardo, la vida privada quedaría expuesta a prácticas invasivas que podrían poner en riesgo tanto la libertad como la dignidad humana (Castillo, 1998).

METODOLOGÍA

La investigación adoptó un enfoque cualitativo con el propósito de profundizar en el tema de la protección de datos y la privacidad en línea, con el fin de captar, interpretar y comprender el significado socialmente

compartido, incorporando el derecho a la autodeterminación personal en un contexto donde los conflictos derivados del uso y explotación de la información en la era digital son cada vez más evidentes; situación que expone a las personas a riesgos constantes relacionados tanto con la privacidad como con la seguridad de su información personal, dentro de un entorno digital.

La investigación fue clasificada como investigación básica, con un enfoque no experimental y de tipo descriptivo (Macías et al., 2007). Para la recolección y estructuración de los datos, se llevó a cabo una revisión bibliográfica de 30 artículos extraídos de bases de datos académicas como Redalyc, Scopus y Dialnet. La recolección de datos se efectuó mediante fichas bibliográficas, las cuales fueron sistematizadas en una planilla de Excel, lo que facilitó una sistematización eficiente de la información. El análisis de los datos se realizó a través de un enfoque deductivo, orientado al desarrollo estructurado de ideas.

Por ello, el 13 de agosto de 2024 se estableció el siguiente esquema temático: en primer lugar, se consideró fundamental precisar que el derecho a la protección de la información personal y a la privacidad tiene su origen en el artículo 12 de la DUDH. Este artículo prohíbe las intromisiones injustificadas en la vida privada de los individuos y establece los cimientos para el reconocimiento del derecho a la protección de datos personales como una garantía independiente (López-Torres, 2014).

En segundo lugar, señalar sobre los riesgos que vulneran la salvaguarda de la información personal y privacidad en línea; los problemas vinculados a la pérdida de privacidad han surgido gradualmente, lo que ha llevado a la limitación de derechos y exponiendo nuestra privacidad, incluso en los aspectos más insignificantes. Además, la violencia ha migrado al entorno digital, donde se ha incrementado la violencia digital, especialmente contra mujeres, junto con delitos como la extorsión, secuestros virtuales, ciberacoso y suplantación de identidad (Sánchez, 2023).

En tercer lugar, se examinó la legislación que regula la protección de datos personales en el ámbito digital, un área de creciente importancia debido al desarrollo de las tecnologías de la información. Se analizaron tanto las normativas locales como internacionales que establecen las directrices para el manejo de información personal en la web. Entre las normativas estudiadas se incluyen la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México, y marcos internacionales como el

Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Estas leyes buscan asegurar la protección de la información personal, controlar su acceso y regular su transferencia, aspectos esenciales en un entorno cada vez más globalizado y conectado (Mendoza, 2021).

Finalmente, se enfatizó la importancia del derecho a la protección de datos personales y su alcance a la información en línea, reconocer el derecho a la privacidad sobre información o conocimiento implica, en esencia, respetar la libertad de cada persona de mantener ciertos aspectos en privado, sin embargo, desde una perspectiva ética, es necesario establecer límites que garanticen que la información no compromete la seguridad o el bienestar social, en esos casos, la protección de la sociedad debe prevalecer sobre el derecho.

RESULTADOS

1. El origen del Derecho a la Privacidad y Protección de Datos

El derecho a la privacidad ha sido objeto de estudio y protección jurídica desde el siglo XIX; el 15 de diciembre de 1890, los abogados Louis D. Brandeis y Samuel D. Warren publicaron *The Right of Privacy*, un artículo clave que sentó las bases para la protección de la vida privada al diferenciarlo del derecho a la libertad, argumentando que el derecho a disfrutar de la vida y a estar solo debe considerarse una extensión de los derechos individuales, no solo como una defensa de la libertad sino como una salvaguarda contra la violación de la intimidad personal (Nieves, 2012).

De esta manera, el *Right to Privacy* fue conceptualizado como un derecho autónomo que protege los aspectos inmateriales y espirituales de los individuos, desvinculándose de derechos de propiedad o de libertad; es así como, Warren y Brandeis argumentaron que el derecho a la libertad garantiza “extensive civil privileges”, pero esto no ofrece protección contra las ofensas emocionales derivadas de la intromisión en la privacidad personal, mientras que el derecho a la privacidad resguarda los aspectos más inmateriales y los intereses espirituales del individuo, consolidándose como un derecho autónomo con sustantividad propia (Warren et.al., 1890, citado por Lopez-Torres, 2014).

Entre 1891 y 1893, los tribunales en Nueva York reconocieron el derecho a la intimidad en dos sentencias, subrayando en la segunda sentencia la

importancia de proteger tanto la integridad personal como la propiedad, en ese contexto, se determinó que los jueces debían garantizar el derecho de las personas a “vivir sin interferencias”. Posteriormente en 1902, en el caso *The Franklin Mills Co. vs. Abigail Roberson*, un juez disidente defendió la idea de que el derecho a la protección de la intimidad personal (entendido como el derecho a estar en solitario) debía ser reconocido por el sistema judicial como una extensión del derecho a la inviolabilidad personal. Esta posición fue reafirmada en 1903 con la promulgación de la Ley de Derechos Civiles de Nueva York, la cual establece como infracción el uso del nombre, retrato o imagen de una persona viva con fines comerciales sin su consentimiento por escrito, o sin la autorización de los padres o tutores en el caso de menores de edad (Morris et al., 1962, citado por Dermizaky, 2000).

La devastación de la Segunda Guerra Mundial y la persistencia de violaciones masivas de derechos humanos, evidenciaron la necesidad urgente de un nuevo marco global para su protección. Este impulso llevó a la creación de instrumentos internacionales clave (como la Declaración Universal de Derechos Humanos de 1948) que buscaban específicamente salvaguardar la vida privada.

Dada su temprana aparición como una de las primeras demandas frente al Estado Absolutista, la protección de la vida privada se considera un derecho fundamental de primera generación. Estos documentos sentaron las bases para un orden mundial renovado, cuyo objetivo primordial es prevenir intromisiones arbitrarias en la esfera íntima de las personas y garantizar la protección de la familia y el hogar como espacios de resguardo (Robles, 2021).

La protección de la vida privada alcanzó reconocimiento global a través de la DUDH de 1948, específicamente, su artículo 12 protege a los individuos de intromisiones injustificadas en su vida personal, su núcleo familiar, su hogar y su correspondencia, el cual se consolidó más adelante con la adopción del Pacto Internacional de Derechos Civiles y Políticos en 1966, que reafirma estas garantías en su artículo 17, y por la Convención sobre los Derechos del Niño de 1989, cuyo artículo 16 extiende dicha protección específicamente a la infancia. Estos desarrollos normativos evidencian la creciente preocupación por la privacidad como un derecho fundamental, particularmente frente a los retos que plantea el entorno digital y tecnológico (Porcelli, 2020).

En este sentido, el investigador de la Universidad de Columbia, Alan Westin, amplió el concepto de privacidad en 1967 al introducir la expresión autodeterminación informativa o “informational privacy” en respuesta al creciente uso no consentido de información personal, destacando la facultad de cada individuo para decidir cómo, cuándo y en qué medida su información debe ser conocida por otros, subrayando además que la privacidad es esencial para el proceso de toma de decisiones y constituye un elemento fundamental en cualquier sociedad libre (Westin, 1967, citado por Moreno y Olmeda, 2021).

La década de 1970 marcó el nacimiento del derecho a la salvaguarda de la privacidad, un concepto relativamente nuevo en el ámbito de los derechos humanos, cuando países europeos comenzaron a promulgar leyes para regular las tecnologías y, en particular, las bases de datos de información, aunque dichas legislaciones fueron posteriormente modificadas y el derecho a la protección de datos personales pasó a interpretarse en el marco del resguardo de la información personal (Gonzales, 2010, citado por Orellana, 2017). En tal sentido, la privacidad se redefine enfocándose en otorgar control sobre los datos personales, fortaleciendo el control individual sobre la información personal frente a las tecnologías invasivas, y estableciendo obligaciones para quienes manejan y acceden a esta información (García, 2007).

La rápida evolución tecnológica de las últimas décadas ha transformado profundamente la forma en que entendemos y protegemos la intimidad; la definición de privacidad se ha vuelto compleja debido a la influencia de factores sociales, situacionales y, cada vez más, tecnológicos. Aunque tradicionalmente la intimidad se ha vinculado a conceptos como la autonomía, el secreto, la libertad, evolución personal y la dignidad, en la actualidad se concibe principalmente como el derecho a la autodeterminación informativa (Lucena, 2012).

Así, muchos países han implementado regulaciones sobre resguardo de la información personal, con la finalidad de proteger los derechos de la población y promover el crecimiento de empresas dedicadas a la gestión de información, las políticas deben tener un enfoque transnacional, lo que implica que el marco jurídico debe adaptarse y alinearse con los avances tecnológicos de acorde al tiempo. Además, la regulación adecuada de la salvaguarda de información es crucial para fomentar la confianza del público en los servicios digitales, lo que a su vez impulsa la innovación y el crecimiento en el sector tecnológico, establecer normas claras, los

gobiernos pueden asegurar un balance entre la protección de la vida privada y el impulso de la economía digital (Enríquez, 2017).

Por otro lado, derecho a la privacidad de la información personal emergió en el contexto del avance tecnológico iniciado en la década de los sesenta, cuando surgieron sistemas informáticos capaces de procesar, interconectar y transmitir información a alta velocidad, marcando una auténtica revolución, puesto que este progreso tecnológico eliminó las barreras espaciales y temporales que anteriormente restringen el uso y almacenamiento de la información (Castro, 2008).

Está claro que, el derecho a la privacidad es una cuestión de suma relevancia social, y aunque se comenzó a proteger hace mucho tiempo, sigue siendo un desafío en la era digital. Todo empezó con un artículo de dos abogados, Louis D. Brandeis y Samuel D. Warren, quienes en 1890 hablaron sobre la importancia de proteger la esfera de privacidad de los individuos. Ellos argumentaron que el derecho a estar solo y disfrutar de la vida debería ser reconocido como un derecho fundamental, diferente al de la libertad; esto fue algo muy novedoso en ese momento y ayudó a que los jueces empezaran a proteger la privacidad en Estados Unidos.

Después de la Segunda Guerra Mundial, se dieron cuenta de que los derechos humanos, entre los que se encuentra la privacidad, debían ser protegidos a nivel global. Por eso, en 1948, se creó la Declaración Universal de Derechos Humanos, que incluye el derecho a la privacidad en su artículo 17, esta declaración inspiró a otros tratados y convenciones que reconocen que nadie debería sufrir interferencias en su vida privada. A medida que avanzó la tecnología, el concepto de privacidad se volvió más complicado, en Europa y en otros lugares, las leyes empezaron a adaptarse para proteger la información personal de las personas, especialmente con la llegada de las computadoras e internet al igual que en Estados Unidos.

Proteger la privacidad es más importante que nunca porque las vidas están cada vez más conectadas a internet y las redes sociales, las leyes deben ser actualizadas constantemente para proteger a los ciudadanos de las amenazas modernas, como el mal uso de los datos personales. En conclusión, La privacidad como derecho ha sufrido muchos cambios desde el siglo XIX, pero con la rapidez de los avances tecnológicos, es crucial que las leyes sigan mejorando para protegernos en este nuevo mundo digital, sin privacidad, la libertad y la dignidad podrían estar en peligro.

2. Principales Amenazas de la Protección de datos y Privacidad en Línea

La privacidad y la confidencialidad suelen quedar vulneradas en un gran número de situaciones de intercambio de información, que terceros accedan a información sin la autorización o el permiso del usuario, lo que también afecta la autonomía personal al limitar la capacidad de decisión del individuo (Soto, 2017). De esta manera, se tiene en cuenta que los problemas relacionados con la recopilación de datos personales, se originan principalmente en la transformación de información privada en pública sin el consentimiento del interesado y en su permanencia indefinida en Internet (Sabater, 2010).

Los conflictos legales originados por actos de odio, discriminación, extorsión y acoso sexual representan algunos de los riesgos más significativos en una sociedad donde la información personal, capaz de identificar o hacer identificable a un individuo, demanda un cuidado especial debido a la posible sobreexposición. Por esta razón, resulta fundamental destacar la importancia de la corresponsabilidad digital, especialmente en el entorno familiar (Ordóñez y Calva, 2020).

El ciberespacio es el nuevo escenario donde convergen numerosas amenazas actuales, las cuales se clasifican en diferentes categorías: Agentes de perfil bajo, que son individuos aislados o poco organizados con fines personales, como hackers, crackers y otros delincuentes del ciberespacio; cibercrimen o crimen organizado, que involucra a organizaciones mafiosas o criminales con el propósito de obtener beneficios económicos o causar daños según sus intereses; ciberterrorismo, que abarca a organizaciones terroristas y extremistas que emplean el ciberespacio para llevar a cabo acciones de propaganda, reclutamiento y atentados contra sistemas de información (Davara, 2013, citado por Gonzalez, 2017).

El Internet ha facilitado la difusión de información, a través de la red los usuarios comparten archivos, expedientes y correos electrónicos que incluyen información personal protegida, ya sea relacionada con autoridades públicas o con usuarios particulares, pero debilita el resguardo y protección de derechos fundamentales como la privacidad (Castillo, 1998). La recolección continua de datos en múltiples plataformas intensifica que la información se encuentre en riesgo, debido a que los usuarios crean perfiles detallados, exponiéndose a posibles vulneraciones y manipulaciones (Estrada et al., 2015).

La transformación de las tecnologías de la información y comunicación representa una posible amenaza para la protección de los derechos fundamentales de niños, niñas y adolescentes, especialmente en cuanto a la protección de sus datos personales, puesto que el uso de estas tecnologías exige no sólo un marco regulatorio adecuado, sino también el cumplimiento de las responsabilidades de la familia, mientras que el internet y las redes sociales convierten a los menores en objetivos vulnerables para quienes abusan de la información personal disponible en línea, lo que deriva en fenómenos como grooming, cyberbullying, sexting y otros, particularmente debido a la práctica familiar de compartir datos personales conocida como sharenting (Ordóñez y Calva, 2020).

En este escenario, tal como se ha señalado, los avances en las tecnologías de la información y la comunicación han dado forma a una compleja realidad social marcada por Internet y sus vastas posibilidades, destacándose aspectos clave como: a) el papel de la información como fuente de poder en todos los niveles; b) la globalización, que incluye diversas modalidades, entre ellas la mundialización de la información; y c) el papel de las nuevas tecnologías como impulsores de estas dinámicas (Ballesteros, 2005, citado por Lucena, 2012).

Es importante considerar la gran cantidad de casos en los que personas, incluidos menores de edad, vulneran la dignidad humana mediante publicaciones en redes sociales cuyo contenido y veracidad pueden ser cuestionables o incluso corresponder a información anónima, lo que evidencia irresponsabilidad por parte de quienes emiten dicha información, al ofrecer servicios en internet que para muchos resultan imprescindibles, aumentan la solicitud, exposición y compartición de datos personales (Moreno y Olmeda, 2021). Sin embargo, se presentan a menudo amenazas comunes como el ciberacoso, la suplantación de identidad y la exposición no autorizada de datos personales, problemas que se agravan con las vulnerabilidades en los sistemas de seguridad (Ojeda y Cutié, 2021)

Asimismo, un informe de Pricewaterhouse Coopers, “Key Findings from the 2015 US State of Cybercrime Survey”; en el 2014 los ciberataques fueron destructivos, resultando en el robo de mil millones de registros de información; en el 2016, hubo un ataque que estuvo orientado a dañar la reputación de empresas o a interrumpir el comercio electrónico (Amaro y Rodríguez, 2016).

Frente a estos riesgos, el Estado peruano ha actualizado su legislación con modificaciones que serán examinadas para identificar nuevas áreas

de protección en la gestión automatizada de información, asimismo, se ofrecerán recomendaciones para evitar problemas legales en el creciente y diverso mercado de manejo de datos personales, que incluye sectores como call center y bancos. Además, las conductas sancionables ahora se limitan a la comercialización y venta ilegítima de información personal, más allá de la venta de bases de datos, castigando no solo los actos ilegales, sino también aquellos considerados ilegítimos (Téllez, 2015).

De esta manera, la violencia en la web abarca modalidades física, psicológica, sexual, económica, objetual y social, y se presenta en diversos escenarios que son atacados por grupos o individuos que aprovechan el anonimato, la rapidez y la masividad de la comunicación en línea, presentan una amenaza en internet cómo los cibercriminales, expertos en cibersecuestro, obtienen información de sus víctimas a través de distintos métodos; entre ellos, se destaca la participación en chats o foros en línea, recurren a infiltrarse en listas de correo y en plataformas de mensajería instantánea, donde los propios usuarios suelen proporcionar información personal (Trujano et al., 2009).

En Latinoamérica, Ecuador ocupa el séptimo lugar en ciberseguridad, según un estudio sobre seguridad y protección de datos. Sin embargo, muchos usuarios de redes sociales han reportado ser víctimas de ciberacoso, así como de phishing y sextorsión, situación en donde extorsionadores amenazan con divulgar contenido sexual (Escobar y Álvarez, 2022).

De igual manera, la comunidad internacional considera que Chile no cumple con estándares adecuados de privacidad, principalmente debido a la ausencia de una autoridad de control imparcial e independiente con las facultades necesarias para resolver conflictos en materia de privacidad y protección de datos. Además, la inexistencia de un registro de bancos de datos privados restringe la posibilidad de los ciudadanos de ejercer derechos fundamentales como el acceso, la rectificación y la cancelación de sus datos personales, lo que representa un obstáculo para garantizar una adecuada protección de la información (Herrera, 2016).

Otra amenaza en línea es el uso de cookies, que permiten a los proveedores personalizar la publicidad mediante un rastreo automático de los hábitos de navegación de los usuarios, vinculándolos a su dirección IP y permitiendo que se identifiquen dispositivos específicos conectados a la red, el cual se considera un dato personal y requiere del consentimiento explícito y por escrito del usuario. No obstante, en la práctica, las redes sociales a menudo

omiten este requisito, sus políticas de cookies suelen ignorar principios como el de finalidad e información, y el simple clic en un botón no puede considerarse un consentimiento válido (Herrera, 2016).

De acuerdo con un estudio, el 95% de los estudiantes utiliza funciones de privacidad para controlar quién accede a su perfil, compartiéndolo solo con contactos cercanos (92%). El 90% es consciente de los riesgos asociados con su identidad digital y evita revelar información privada en la red. También consideran necesario mantener un nivel de privacidad, especialmente en redes sociales, para protegerse de la suplantación de identidad, estafas o robos de datos (89%). Algunos gestionan varias identidades digitales para controlar mejor su información y extreman precauciones al compartir datos personales sensibles, como dirección, edad o datos bancarios, salvo que la aplicación lo requiera (Castillejos *et al.*, 2016).

Las tecnologías de la información y comunicación son una herramienta muy útil que facilita la comunicación y el acceso rápido a la información en todo el mundo; sin embargo, su uso irresponsable representa un gran riesgo para la privacidad y seguridad de los usuarios, las amenazas más comunes destacan el ciberacoso, la suplantación de identidad y la exposición no autorizada de datos personales, problemas que se agravan con las vulnerabilidades en los sistemas de seguridad, la recopilación masiva de datos por parte de empresas y las frecuentes fugas de información. Además, el uso de herramientas de inteligencia artificial que manejan datos sin el consentimiento adecuado de los titulares puede comprometer aún más la privacidad, lo que subraya la necesidad de adoptar medidas de protección adecuadas.

Es preocupante que en países como Ecuador y, en general, en América Latina, muchas personas hayan sido víctimas de ciberacoso o robo de información, evidenciando la falta de seguridad en línea, problema que se agrava porque en muchos casos, los usuarios desconocen los riesgos y las medidas de seguridad que pueden implementar para reducir estas amenazas en las redes sociales. Por esta razón, el gobierno ecuatoriano ha impulsado algunas iniciativas para enfrentar estos riesgos, al mismo tiempo que se promueven recomendaciones para que los usuarios sepan cómo protegerse mejor y evitar convertirse en víctimas de ciberataques.

Aun así, la falta de transparencia por parte de algunas empresas y plataformas digitales genera desconfianza en el entorno digital, añadiendo el hecho de que los usuarios no siempre saben cómo se utilizan o cómo

proteger sus datos. Esto hace urgente que tanto los gobiernos como las empresas implementen políticas de protección de datos que fortalezcan la seguridad digital y permitan a los usuarios navegar con confianza, especialmente a los menores de edad, que son los más vulnerables en estas plataformas.

3. Marco Jurídico de la privacidad y la protección de los datos personales

El derecho a la protección de los datos personales tiene su origen en el derecho a la privacidad y, por consiguiente, en el derecho a la intimidad, los cuales enfrentan constantes desafíos debido al avance tecnológico que modifica las formas de almacenamiento y distribución de información. En este contexto, es esencial establecer marcos legales y políticas públicas que regulen el ejercicio de la libertad individual, con el propósito de aprovechar los avances tecnológicos para el beneficio colectivo y de alcanzar un equilibrio entre los derechos individuales y los de los demás, siempre en concordancia con los principios fundamentales de la sociedad (Villalba, 2017).

Asimismo, la regulación de protección de datos es esencial para garantizar la seguridad de los menores, especialmente frente a la difusión de imágenes ilegales, como contenido que promueva la violencia contra las mujeres o la pornografía infantil; así como la distribución de información personal sensible sin consentimiento, en tanto las redes sociales son utilizadas como espacios de intercambio, a veces se infringen normas relacionadas con la propiedad (Brosh, 2018, citado en Gonzalez et al., 2022).

Por otra parte, en la legislación de Estados Unidos y Canadá, la privacidad en el ámbito público está protegida como un derecho constitucional aplicable a las comunicaciones electrónicas, incluyendo Internet, y esta protección se extiende a las instituciones gubernamentales. En Estados Unidos, la *Electronic Communications Privacy Act*, y en Canadá, el *Criminal Code*, son leyes que resguardan el derecho a la privacidad en este contexto al exigir autorizaciones para las comunicaciones electrónicas, lo que implica que la policía no puede interceptar correos electrónicos ni realizar transferencias mediante FTP o Telnet sin una orden judicial (Castillo, 1998).

Los Estados asignan la responsabilidad de garantizar los derechos previstos en las leyes de protección de datos personales a distintas instituciones. En la Unión Europea, el Reglamento 2016/679 delega esta tarea a cada

país miembro; en España, se designa a una autoridad de protección de datos como un organismo público independiente, mientras que en Perú, dicha responsabilidad está a cargo del Ministerio de Justicia, a través de la Dirección Nacional de Justicia (Enríquez, 2017).

De hecho, la República Dominicana cuenta con la Ley 172-13, promulgada el 15 de diciembre de 2013, con el propósito de proteger de manera integral los datos personales almacenados en archivos, registros públicos, bancos de datos u otros medios, sean estos públicos o privados. Aunque busca garantizar derechos como el acceso, rectificación, actualización y eliminación de datos personales, ya sean digitales o manuales, la ley presenta deficiencias al no establecer un órgano regulador específico, salvo en el caso de la información financiera, donde se supone que la supervisión corresponde a la Superintendencia de Bancos (Barinas, 2019).

Asimismo, en América Latina, la protección de la vida privada ha sido reconocida como un derecho de rango constitucional. En Ecuador, este reconocimiento se reforzó en 2010 con la promulgación de la Ley del Sistema Nacional de Registro de Datos Públicos (LSNRDP), la cual regula el registro y acceso a los datos públicos con el propósito de organizar y transparentar la información almacenada por instituciones públicas y privadas sobre las personas. En esta normativa, el artículo 6 define los datos confidenciales y establece que su acceso solo será permitido al titular o mediante mandato legal. Sin embargo, no contempla mecanismos específicos para garantizar una protección efectiva de los datos personales (Estrada et al., 2015).

En 2008, Uruguay aprobó una ley general de protección de datos con el propósito de adecuarse a los estándares europeos en esta materia, la Ley 18.331, que define en su articulado las fuentes de acceso público, considerándolas como aquellas bases de datos disponibles para cualquier persona, salvo que exista una norma restrictiva o que su acceso requiera el pago de una contraprestación. Además, en el artículo 9, inciso tercero, se establece que no será necesario obtener consentimiento para el uso de datos cuando estos provengan de fuentes accesibles al público, como registros oficiales o publicaciones en medios de comunicación masiva (Alvarado, 2014).

En Chile, el derecho a la vida privada se encuentra consagrado en la garantía establecida en el numeral 4° del artículo 19 de la Constitución Política, tal precepto asegura a todas las personas “el respeto y protección

a la vida privada”. Además, este derecho adquiere una dimensión específica en relación con la inviolabilidad del hogar, las comunicaciones y los documentos privados, lo que está regulado en el numeral 5° del mismo artículo, reforzando la protección en estos ámbitos esenciales de la privacidad individual (Álvarez, 2016).

En esta línea, Chile se convirtió en el primer país de Iberoamérica en aprobar una legislación específica sobre la protección de la privacidad, incorporando principios fundamentales en materia de datos personales, Ley 19.628 conocida como Ley sobre Protección de la Vida Privada, la cual establece en su artículo 4 que el tratamiento de datos personales solo es permitido cuando cuenta con autorización expresa de esta ley, de otras disposiciones legales o del consentimiento explícito del titular. Además, exige que el titular sea debidamente informado sobre el propósito del almacenamiento de sus datos y la posibilidad de que estos sean divulgados al público (Chen, 2010).

A diferencia de otros marcos normativos, la legislación peruana de protección de datos establece una distinción clara entre seguridad y confidencialidad, mas en cuanto a la seguridad en el tratamiento de datos personales, es el responsable del banco de datos quien debe implementar medidas técnicas, organizativas y legales que garanticen la protección de la información, evitando su alteración, pérdida, tratamiento o acceso no autorizado. Además, está prohibido procesar datos personales en bancos de datos que no cumplan con los estándares de seguridad exigidos, sin embargo, respecto a la confidencialidad, tanto el responsable del banco como el encargado y cualquier persona involucrada en el tratamiento de datos están obligados a preservar la reserva de la información y sus antecedentes (Enríquez, 2017).

En el Estado peruano ha destacado una situación peculiar que, a pesar de contar con una regulación constitucional orientada a proteger la intimidad de las personas, presenta limitaciones en su aplicación debido a factores como la frecuente falta de organización, planificación, presupuesto, prevención y atención a las víctimas, lo que ha llevado a analizar uno de los casos más representativos, donde se observa la actuación del Estado como regulador y sancionador, la participación de la empresa privada y la afectación sufrida por la víctima (Galvis y Pesca, 2020).

En definitiva, la protección de la privacidad en el ámbito digital ha experimentado un avance significativo, ajustándose a los desafíos que

plantea el desarrollo tecnológico y los riesgos emergentes en el manejo de información personal. En países como Estados Unidos y Canadá. En América Latina, la legislación sobre privacidad y protección de datos avanza de manera heterogénea, con diferencias marcadas entre países que han logrado desarrollar marcos regulatorios sólidos y aquellos que enfrentan rezagos significativos. Uruguay y Chile son ejemplos destacados con leyes como la Ley 18.331 y la Ley 19.628, que garantizan principios fundamentales como el consentimiento informado y la transparencia en el acceso a bases de datos públicos.

Las normativas no solo aseguran un control efectivo sobre los datos personales, sino que también establecen mecanismos para que las personas puedan conocer y decidir sobre el uso de su información. En contraste, países como Ecuador muestran deficiencias, limitándose a regulaciones parciales como la Ley del Sistema Nacional de Registro de Datos Públicos, que no incluyen medidas específicas para proteger la información personal frente a usos indebidos. República Dominicana, por su parte, cuenta con la Ley 172-13 que regula la protección de datos, pero carece de un órgano regulador específico, lo que limita su capacidad de supervisión y ejecución, especialmente fuera del ámbito financiero.

En Perú, la legislación en materia de datos personales presenta una clara distinción entre seguridad y confidencialidad, lo que permite abordar estos aspectos desde perspectivas complementarias. En términos de seguridad, se exige que los responsables de bases de datos adopten técnicas, organizativas y legales que previenen alteraciones, pérdidas, accesos no medidas autorizadas o tratamientos indebidos de la información personal almacenada. Este enfoque técnico busca garantizar que las bases de datos operen bajo estándares que minimicen los riesgos asociados al manejo de información sensible.

4. Importancia de la Protección de datos y la Privacidad

El derecho a la protección de datos personales es fundamental e inherente a cada individuo para garantizar su desarrollo en un entorno adecuado, aunque el vasto alcance de Internet y el ejercicio pleno de la libertad de expresión han generado limitaciones a esta protección, especialmente en el caso de los menores, quienes, conforme a la normativa nacional e internacional, requieren una protección prioritaria debido a su mayor vulnerabilidad frente a posibles vulneraciones (Ordóñez y Calva, 2020).

Los datos reflejan hechos, conceptos y dimensiones, forma parte esencial del lenguaje y la gestión; además de facilitar la creación de relaciones para analizar comportamientos en diversos procesos, permiten generar, distribuir y utilizar información (Nieves-Lahaba y Ponjuan-Dante, 2021). La Ley de Protección de los Datos Personales también abarca la información relacionada con personas jurídicas, incluyendo los datos procesados de forma electrónica o automatizada, considerando tanto los propios datos como la infraestructura utilizada para su tratamiento y el factor humano que participa en su gestión (Lo Giudice, 2017).

Esto significa que, la protección de datos personales y la seguridad de la información, aunque estrechamente relacionadas, están vinculadas a principios como la confidencialidad, integridad y disponibilidad, debido a los numerosos incidentes de fugas de información que se originan en portales creados para diversos propósitos. Esta nueva realidad virtual ha facilitado el acceso a datos personales, exigiendo a empresas y organizaciones una atención rigurosa a la seguridad de la información y la privacidad de los usuarios (Paluma y De Moura, 2019).

En cuanto a la protección de la información personal, se reconoce la presencia de varios principios generales, garantías y excepciones. Estos principios son fundamentales para asegurar, de manera directa, la protección adecuada de los datos personales y de manera indirecta, para proteger derechos como la privacidad, el honor, la reputación y la libertad de expresión, entre otros. Todo esto se logra mediante la creación de un marco jurídico adecuado que permita la efectiva realización de estos derechos y garantías fundamentales (Chen, 2010).

Asimismo, el análisis de la importancia y protección de los datos personales resalta el papel fundamental que estos juegan en la sociedad moderna, especialmente con el avance de la tecnología y la expansión de internet. Los datos no solo son una representación de hechos, conceptos o dimensiones, sino que también sirven como base para la creación de relaciones que permiten analizar comportamientos humanos, lo que es crucial tanto en el ámbito comercial como en el político. El uso creciente de los datos electrónicos, su intercambio masivo y el volumen cada vez mayor de información recopilada requieren, de manera urgente, políticas y marcos legales que garanticen su protección (Cerde, 2006).

La privacidad está vinculada a la dimensión política de las tecnologías y ha sido un tema central en los debates de las últimas décadas, especialmente

en lo que respecta a la relación entre ética, política y tecnología. Además, recuperar el control sobre la privacidad resulta esencial para hacer frente a un sistema de vigilancia que pone en riesgo la libertad, la igualdad y la autonomía. En este sentido, la privacidad no solo protege la información personal, sino que también proporciona herramientas para fomentar una conciencia crítica sobre el impacto del desarrollo tecnológico (López, 2022).

En 2008, Uruguay promulgó una ley general de protección de datos con el objetivo de alinearse con los estándares europeos en esta materia. La Ley 18.331 incluye en su articulado una definición de fuentes de acceso público, describiéndolas como aquellas bases de datos cuya consulta está disponible para cualquier persona, siempre que no exista una norma restrictiva o que únicamente requiera, en su caso, el pago de una contraprestación. Esta disposición refleja un enfoque amplio respecto al concepto de fuente de acceso público, sin restricciones específicas sobre la naturaleza de los datos que pueden recopilarse ni las bases de datos que podrían incluirse en esta categoría (Nieves, 2007).

Por último, la seguridad informática, de naturaleza técnica, se basa en aplicar buenas prácticas para reducir riesgos y corregir vulnerabilidades relacionadas con la gestión de la información, las redes y el software. En contraste, la confidencialidad se refiere a la confianza depositada en quien administra los datos, asegurando que no se divulga información protegida sin el consentimiento del titular. Esta distinción entre seguridad y confidencialidad es crucial para asignar responsabilidades civiles y penales, especialmente ante el aumento de ataques informáticos, la vigilancia masiva por parte de algunos gobiernos y el manejo negligente de datos personales por institución (Enríquez, 2017).

Está marcado por la expansión de las nuevas tecnologías de la información y la comunicación, se hace indispensable abordar el concepto de intimidad o privacidad y su protección jurídica. Aunque definir y delimitar los límites de la intimidad resulta un desafío en la actualidad, es fundamental trabajar en un concepto que, aunque no sea plenamente satisfactorio, permita enfrentar los desafíos que surgen del avance de la informática y de los sistemas tecnológicos, cuya influencia en la vida cotidiana es cada vez más significativa (Lucena, 2012).

La protección de los datos personales se enfrenta a profundas contradicciones, evidenciando una compleja dualidad en el ámbito social,

político e institucional, mientras crece la conciencia de su relevancia tanto para la privacidad como para la libertad individual, pero al mismo tiempo, su preservación se complica debido a las demandas de seguridad, los intereses del mercado y la reorganización de las administraciones públicas, que tienden a reducir las garantías (Rodotá, 2006).

En relación con la protección de datos personales, resulta fundamental analizar las condiciones y términos de uso de las herramientas y páginas digitales disponibles en Internet considerando la importancia de crear conciencia sobre el resguardo de información personal, como textos, imágenes y videos, con el fin de prevenir riesgos como amenazas, fraudes o ciberacoso, que son frecuentes en la actualidad, además de que este aspecto también implica respetar la privacidad de los demás, evidenciándose, por ejemplo, en redes sociales donde es común etiquetar contactos en imágenes publicadas en los muros (Lee, 2014, citado por Castillejos *et al.*, 2016).

En algunos países iberoamericanos, el derecho a la protección de datos personales se ha definido, tanto legislativa como jurisprudencialmente, como un derecho autónomo con una naturaleza distinta a los derechos vinculados a la vida privada y familiar, la intimidad, el honor y el buen nombre, cuyo propósito es garantizar el control y la disposición que cada individuo tiene sobre la información que le concierne, especialmente ante el uso de las tecnologías de la información y la comunicación, resaltando que al proteger este derecho se resguardan también otros derechos humanos considerados indivisibles e interdependientes entre sí, los cuales pueden verse vulnerados por intrusiones ilegales o arbitrarias, incluso relacionadas con el tratamiento de datos personales (Porcelli, 2020).

El análisis sobre la protección de datos personales no es reciente, aunque ha cobrado mayor relevancia con el avance de la informática debido a la capacidad de las computadoras para almacenar grandes volúmenes de información, lo que permite la creación de perfiles personales que pueden afectar la imagen social de las personas o generar perjuicios en su vida cotidiana, que hace referencia al riesgo de una contaminación de las libertades, siendo esta amenaza para el derecho a la intimidad, lo que demanda acciones desde las estructuras jurídicas para evitar que el flujo de datos indispensable en la sociedad de la información, donde la información representa poder, termine convirtiéndose en una amenaza para los derechos y libertades fundamentales del ciudadano (Porven *et al.*, 2021).

Todo documento que contenga información única y personal de un ciudadano debe ser resguardado y protegido por quienes lo gestionan, un aspecto regulado dentro del marco de la protección de datos personales. Esto es especialmente relevante en el manejo de bases de datos, soportes o ficheros electrónicos, dado que están estrechamente vinculados con derechos de la personalidad como el honor, la vida privada, la intimidad y la propia imagen. Dicha información representa elementos clave de identidad personal, por lo que su robo o uso indebido no solo afecta directamente al individuo, sino que también puede tener un impacto negativo en su entorno social (Meraz, 2018).

La creciente circulación y divulgación de datos personales, gustos y preferencias en internet, ya sea de manera voluntaria o involuntaria, se ha convertido en una realidad que puede resultar abrumadora, debido a que el desarrollo tecnológico ofrece importantes beneficios en cuanto al acceso al conocimiento y la información, también conlleva riesgos significativos para quienes son titulares de esos datos, los cuales suelen difundirse sin un control adecuado, afectando gravemente la protección de su privacidad y su capacidad de autodeterminación informativa (Muñoz, 2015).

El Internet no ha generado novedades respecto al conflicto de intereses mencionado, pero ha permitido la difusión ilimitada en tiempo y espacio de información que está vaciando de contenido la protección de derechos fundamentales reconocidos en todas las legislaciones, mientras los usuarios comparten archivos, expedientes o correos electrónicos con datos personales protegibles, ya sea relacionados con autoridades públicas o entre particulares (Castillo, 1998).

La importancia de los datos personales, al estar ligados a la identidad de la persona, hace que su manejo sea un tema delicado, pues la exposición o el uso inapropiado de esta información puede tener consecuencias graves como la discriminación o el control social; aunque existan medidas de protección de los datos personales debe ser vista como la defensa de un derecho humano esencial, pues estos datos no solo permiten identificar a una persona, sino también forman parte integral de su dignidad, honor, intimidad y libertad individual. En este contexto, el tratamiento de datos personales por terceros puede ser peligroso, debido a que la manipulación de estos datos puede influir en las decisiones políticas y comerciales de los individuos, lo que refuerza la necesidad de una legislación sólida que proteja estos derechos fundamentales.

La protección de datos personales es crucial en la sociedad moderna, donde el avance tecnológico y la digitalización han aumentado la recolección y el uso de la información personal. Estos datos son esenciales para analizar comportamientos en distintos ámbitos, destacándose su valor en contextos comerciales y políticos. La privacidad no solo busca restringir el acceso a la información, sino también otorgar a las personas el control sobre qué datos comparten, cómo se utilizan y con quién. Este control refuerza la protección de derechos fundamentales como la dignidad, la libertad y la intimidad, evitando su vulneración en un entorno cada vez más expuesto a riesgos.

CONCLUSIONES

- Por lo tanto, se reafirma que el tema abordado destaca que el derecho a la privacidad ha sido clave desde el siglo XIX al considerarse un derecho separado de la libertad, un concepto que se fortaleció con leyes internacionales como la Declaración Universal de Derechos Humanos y otros acuerdos. A lo largo del tiempo, la privacidad se ha ampliado para incluir el control sobre los datos personales, especialmente debido al avance de las nuevas tecnologías. La protección de la privacidad ha impulsado la creación de leyes que establecen responsabilidades sobre el manejo de la información personal.
- En conclusión, es evidente que la protección de datos personales es clave en la era digital porque con tanta información recopilada se necesita cuidar la privacidad y los derechos de las personas los datos personales y se debe tener control sobre esta información para evitar abusos y discriminaciones en un mundo con tecnologías avanzadas que pueden invadir la vida privada por eso es importante tener leyes que protejan estos derechos.
- En definitiva, queda claro que la protección de la privacidad y los datos personales ha avanzado para enfrentar los retos del entorno digital con normativas que buscan controlar la información individual. En Estados Unidos y Canadá se requiere autorización judicial para acceder a comunicaciones electrónicas; América Latina, Uruguay y Chile se caracteriza por sus regulaciones fuertes, mientras que países como Ecuador y República Dominicana enfrentan falta de leyes claras.
- En conclusión, el tema abordado destaca la importancia de que el derecho a la privacidad es clave para proteger la dignidad y libertad

de las personas, ganando relevancia en el entorno digital. Asimismo, los retos del manejo de datos en internet requieren leyes actualizadas y una visión global que garantice una protección efectiva, equilibrando innovación tecnológica y respeto a la privacidad.

REFERENCIAS BIBLIOGRÁFICAS

- Alvarado, F. (2014). Las fuentes de acceso público a datos personales. *Revista Chilena de Derecho y Tecnología*, 3(2), Article 2. <https://doi.org/10.5354/0719-2584.2014.33276>
- Álvarez, D. (2016). Acceso a La Información Pública Y Protección De Datos Personales. ¿Puede El Consejo Para La Transparencia Ser La Autoridad De Control En Materia De Protección De Datos? *Revista de Derecho - Universidad Católica del Norte*, 23(1), 51-79. <https://www.redalyc.org/articulo.oa?id=371046600003>
- Barinas, D. (2019). Protección de datos personales y cibercriminalidad. *Saber y Justicia*, 1(15), 48-53. <https://dialnet.unirioja.es/servlet/articulo?codigo=8500569>
- Castillejos, B., Torres, C., y Lagunes, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura*, 8(2), 54-69. <https://www.redalyc.org/journal/688/68848010004/>
- Castillo, C. (1998). Protección de la intimidad en Internet. *Informática y derecho: Revista iberoamericana de derecho informático*, 27, 461-468. <https://dialnet.unirioja.es/servlet/articulo?codigo=248216>
- Castro, K. (2008). El derecho fundamental a la protección de datos personales: Aportes para su desarrollo en el Perú. *IUS ET VERITAS*, 37, 260-276. <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/12229>
- Cerda, A. (2006). Mecanismos de Control en la Protección de Datos en Europa. *Ius et Praxis*, 12(2), 221-251. <https://www.redalyc.org/articulo.oa?id=19712209>
- Chen, S. (2010). Privacidad y protección de datos: Un análisis de legislación comparada. *Diálogos Revista Electrónica*, 11(1), 115. <https://doi.org/10.15517/dre.v11i1.6111>

- Dermizaky, P. (2000). El Derecho a la Intimidad. *IUS ET PRAXIS*, 6, 177-193.
- Enríquez, L. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Foro, Revista de Derecho*, 27, 43-61. <https://www.redalyc.org/articulo.oa?id=90075911003>
- Estrada, J., Estrada, J., Rodríguez, A., y Tipantuña, C. (2015). Ecuador y la privacidad en Internet: Una Aproximación Inicial. *Revista Politécnica*, 36(1). <https://www.redalyc.org/articulo.oa?id=688773649010>
- Galvis, L., y Pesca, D. (2020). Límites del tratamiento de los datos personales en el ámbito laboral frente al uso de las tecnologías de la información y la comunicación en la era digital. *Iusta*, 52, 51-76. <https://www.redalyc.org/journal/5603/560365773003/html/>
- González, A. (2017). Amenazas a la seguridad y privacidad: La dificultad del equilibrio perfecto. *Revista europea de derechos fundamentales, Extra 29*, 267-294. <https://dialnet.unirioja.es/servlet/articulo?codigo=6144011>
- González, M., Dans, I., Muñoz, P., y Estévez, I. (2022). Adolescencia y privacidad digital. *Revista mexicana de investigación educativa*, 27(93), 583-603. <https://www.redalyc.org/journal/140/14071512011/>
- Lo Giudice, M. (2017). Datos empresarios, protección en la actual sociedad de la información: Una visión argentina. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, 17, 8. <https://dialnet.unirioja.es/servlet/articulo?codigo=7499164>
- Lopez, C. (2022). Privacidad es poder. *Revista Iberoamericana de Ciencia, Tecnología y Sociedad - CTS*, 17(49), 279-283. <https://www.redalyc.org/journal/924/92472613016/>
- López-Torres, J. (2014). Antecedentes internacionales en materia de privacidad y protección de datos personales. *Ejil - EAFIT Journal of International Law*, 5(2), Article 2. <https://publicaciones.eafit.edu.co>
- Lucena, I. (2012). La protección de la intimidad en la era tecnológica: Hacia una reconceptualización. *Revista Internacional de Pensamiento Político*, 7, 117-144. <https://www.upo.es/revistas/index.php/ripp/article/view/3683>

- Macías, C., Maynard, G., Massó, E., Hernández, J., Soto, Y., Borges, Y., y Figueras, M. (2007). Consideraciones Teórico-Filosóficas que sustentan la investigación científica Psicosocial Y Educacional. *Revista Información Científica*, 56(4). <https://www.redalyc.org/articulo.oa?id=551757327018>
- Mendoza, O. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, 15(48), 179-207. <https://www.redalyc.org/journal/2932/293270311009/>
- Meraz, A. (2018). Empresa y privacidad: El cuidado de la información y los datos personales en medios digitales. *Revista IUS*, 12(41), 293-310. <https://www.redalyc.org/journal/2932/293258387016/>
- Moreno, I., y Olmeda, M. (2021). Derecho a la privacidad en la sociedad de la información. *Advocatus*, 37, 1-19. <https://dialnet.unirioja.es/servlet/articulo?codigo=8453176>
- Muñoz, A. (2015). Eliminación de datos personales en internet: El reconocimiento del derecho al olvido. *Revista Chilena de Derecho y Tecnología*, 4(2), Article 2. <https://doi.org/10.5354/0719-2584.2015.37426>
- Nahabetián, L. (2015). Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información. *Revista de la Facultad de Derecho*, 39, 199-225. <https://www.redalyc.org/articulo.oa?id=568160375009>
- Nieves, M. (2007). La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de la información personal en los Estados Unidos. *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*, 9(18), 85-115. <https://www.redalyc.org/articulo.oa?id=28291805>
- Nieves, M. (2012). *La génesis de la protección de la privacidad en el Sistema Constitucional Norteamericano: El centenario legado de Warren y Brandeis*.
- Ordóñez, L., y Calva, S. (2020). Amenazas a la privacidad de los menores de edad a partir del Sharenting. *Revista Chilena de Derecho y Tecnología*, 9(2), Article 2. <https://doi.org/10.5354/0719-2584.2020.55333>

- Orellana, C. (2017). De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales. *Foro, Revista de Derecho*, 27, 5-21. <https://www.redalyc.org/articulo.oa?id=90075911001>
- Paluma, T., y De Moura, J. (2019). Aspectos regulatorios de la protección jurídica de la privacidad y de los datos personales en Brasil. *Revista Justicia & Derecho*, 2(1), Article 1. <https://doi.org/10.32457/rjyd.v2i1.269>
- Porcelli, A. (2020). La protección de los datos personales en el entorno digital. Los estándares de protección de datos en los países Iberoamericanos. *REVISTA QUAESTIO IURIS*, 12(2), Article 2. <https://doi.org/10.12957/rqi.2019.40175>
- Porven, Y., Morejón, R., y Pérez, A. (2021). La protección de datos personales. Presupuestos constitucionales para su protección en los procesos judiciales en cuba. *REVISTA CIENTÍFICA ECOCIENCIA*, 8, 126-161. <https://doi.org/10.21855/ecociencia.80.644>
- Robles, A. (2021). El derecho a la privacidad y la protección de datos personales transfronterizos. *Revista Eurolatinoamericana de Derecho Administrativo*, 8(1), 35-60. <https://www.redalyc.org/journal/6559/655969720001/>
- Rodotà, S. (2006). La conservación de los datos de tráfico en las comunicaciones electrónicas. *IDP. Revista de Internet, Derecho y Política*, 3, 53-60. <https://www.redalyc.org/articulo.oa?id=78800310>
- Sabater, C. (2010). Comunicación: El debate en torno a la autorregulación y la cancelación de datos personales en internet. *RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, 1(1), Article 1. <https://www.ride.org.mx/index.php/RIDE/article/view/20>
- Sánchez, M. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, 10(1). <https://www.redalyc.org/journal/6559/655977607008/>
- Soto, Y. (2017). Datos masivos con privacidad y no contra privacidad. *Revista de Bioética y Derecho*, 40, 101-114. <https://www.redalyc.org/journal/783/78351101008/>

- Trujano, P., Dorantes, J., y Tovilla, V. (2009). Violencia en Internet: Nuevas víctimas, nuevos retos. *Liberabit. Revista Peruana de Psicología*, 15(1), 7-19. <https://www.redalyc.org/articulo.oa?id=68611923002>
- 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, 23-42. <https://www.redalyc.org/articulo.oa?id=90075911002>

INSTRUCCIONES PARA PUBLICAR EN DERECHO Y PODER

1. Los artículos son originales e inéditos, enviados por correo electrónico, escritos en tipo de letra Times New Roman, tamaño 12, en español con letras de color negro, en formato Word, tablas en Excel, tamaño A4, interlineado de 1.15.
2. La extensión máxima de los textos, incluyendo imágenes, tablas y bibliografía, es de veinticinco (25) páginas.
3. Los títulos no exceden de veinte palabras, en cada idioma. En caso necesario, los autores utilizan subtítulos, en forma tal que expliquen o amplíen la idea del título y que no se contabilizan dentro de ese límite.
4. Los artículos, después del título en español e inglés, nombre y apellidos del autor o autores, comprende, al menos, las siguientes partes: resumen y palabras clave, abstract y key words, introducción, material y métodos, resultados, discusión, conclusiones y referencias bibliográficas. Las palabras clave no exceden de cinco.
5. La tipología de textos es la siguiente:
 - a) Artículos de investigación científica: textos que presentan, de manera detallada, los resultados de una investigación cualitativa, cuantitativa o mixta, cuya estructura incluye: resumen y palabras clave, abstract y key words, introducción, metodología, resultados, discusión, conclusiones y referencias bibliográficas.
 - b) Artículos de revisión: textos sobre una investigación en los cuales se analizan, sistematizan e integran los resultados de otros trabajos de investigación sobre un determinado campo de la ciencia, tecnología o humanidades, con el propósito de dar cuenta del desarrollo de dichos campos.

- c) Artículos de reflexión: textos que presentan resultados de una investigación sobre un tema específico desde una perspectiva analítica, interpretativa, crítica o reflexiva.
- d) Ensayos: textos en los cuales el autor expone un tema en forma libre, según su manera personal de concebirlo; implica reflexión, opinión o criterios propios, propuesta y defensa de ideas; tienen carácter argumentativo. Por lo general, en ellos se distingue: resumen, introducción, desarrollo o cuerpo central y conclusión.
6. Según el tipo de investigación o naturaleza del tema, caben las adaptaciones en la estructura del artículo por parte de los autores. Se tiene en cuenta, por ejemplo, que material y métodos, resultados y discusión aluden al desarrollo de los contenidos del problema tratado, sobre todo cuando se utiliza alguna variante de la investigación cualitativa.
 7. En nota de pie de la primera página del artículo, se indican los siguientes datos del autor: título profesional, grado o condición académica, filiación institucional, algún otro dato relevante y correo electrónico.
 8. El resumen se presenta en trescientas palabras como máximo; en él se debe aludir al objetivo, la relevancia, la metodología y las conclusiones.
 9. Para las citas y referencias bibliográficas, se utiliza el sistema APA.
 10. Los títulos y subtítulos se escriben en negrita. Los resaltados se presentan en *itálicas* (cursivas), no en negrita ni en letras mayúsculas, tampoco subrayadas o en colores.
 11. Los cuadros o tablas, gráficos y otras ilustraciones, con sus títulos y leyendas respectivos, son numerados correlativamente. En la leyenda se cita la fuente, incluso si la elaboración es del autor. Todas las imágenes, a colores o en blanco y negro, son enviadas en formato JPG de alta resolución, y ubicadas en el lugar que deben ocupar dentro del texto.

12. Las unidades de medida se escriben según el Sistema Internacional de Medidas; las cifras deben agruparse en tríos a la derecha e izquierda de la coma decimal y separadas entre sí por un espacio simple.
13. Cada texto es acompañado de una página previa en la cual el autor registra lo siguiente: nombre, lugar de trabajo, dirección, correo electrónico, teléfono, título profesional, principales publicaciones y resumen de su hoja de vida.
14. Los autores llenan y firman un formato mediante el cual autorizan la publicación de su artículo.
15. Presentado el texto para su publicación, no se envía, al mismo tiempo, a otras revistas.
16. Cada autor recibe tres ejemplares del número en el que aparece su artículo, si se trata de una versión impresa de la revista, y el libre acceso a tres ejemplares del artículo si se trata de una edición electrónica.
17. Los artículos expresan el pensamiento personal de sus autores, no de la institución.
18. Todos los textos remitidos son sometidos a evaluación, según lo estipulado en la sección sistema de arbitraje.



UPAO

FONDO EDITORIAL