Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

USO DE REDES SOCIALES Y VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN ESTUDIANTES DE LA INSTITUCIÓN EDUCATIVA N°1138 “JOSÉ ABELARDO QUIÑONES”, 2024

Línea de investigación:

Gobernabilidad, Derechos Humanos e Inclusión Social

Tesis para optar el Título Profesional de Abogada

Autora

Guzman Meza, Karen Jazmin

Asesora

Leandro Martín, Mauro Florencio

Codigo ORCID 0009-0006-1235-0691

Jurado:

Gonzales Loli, Martha Rocío

Ambrosio Bejarano, Hugo Ramiro

Moscoso Torres, Víctor Juber

Lima - Perú

2025

Guzman Meza, Karen.docx

INFORME DE ORIGINALIDAD

21%	17%	17%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	6%
2	Zamudio Salinas, Maria de Lourdes. "El Derecho a la Proteccion de Datos Personales de los Trabajadores Frente al Control Laboral a Traves del Sistema de Geolocalizacion GPS. Limites y Propuestas", Pontificia Universidad Catolica del Peru - CENTRUM Catolica (Peru) Publicación	2%
3	izai.org.mx Fuente de Internet	2%
4	Submitted to Universidad Andina del Cusco Trabajo del estudiante	2%
5	www.informatica-juridica.com Fuente de Internet	1%
6	Durán Cardo, Ana Belén, Universitat Autònoma de Barcelona. Departament de Ciència Política i de Dret Públic. "La Figura del responsable en el derecho a la protección de datos : génesis y evolución normativa ante el	1%

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

USO DE REDES SOCIALES Y VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN ESTUDIANTES DE LA INSTITUCIÓN EDUCATIVA N°1138 "JOSÉ ABELARDO QUIÑONES", 2024

Línea de Investigación:
Gobernabilidad, Derechos Humanos e Inclusión Social

Tesis para optar el Título Profesional de Abogada

Autor:
Guzman Meza, Karen Jazmin

Asesor:
Leandro Martín, Mauro Florencio
(ORCID: 0009-0006-1235-0691)

Jurado:
Gonzales Loli, Martha Rocío
Ambrosio Bejarano, Hugo Ramiro
Moscoso Torres, Víctor Juber

Lima – Perú
2025

Dedicatoria

Mis esfuerzos serán dedicados siempre a mi madre por haber sido mi soporte emocional en los días más difíciles, por ser el más grande ejemplo de superación y valentía. Esto no sería posible sin ti. Te amo.

Agradecimientos

Al Altísimo Dios, por su gracia y misericordia eterna; por todo, gracias Señor.

Con gratitud de mi corazón, agradezco a mi madre por su amor inagotable, por tomar mi mano en cada uno de mis desafíos. Eres la única persona que nunca me ha dejado sola, sabemos todo lo que nos costó. ¡Gracias por velar por mí!

Hoy también tengo la bendición de poder escribir: ¡Gracias por estar aquí presente apoyándome, papá!

De igual manera, agradezco a mi abuela que ya no comparte la vida con nosotros, pero que mientras estuvo presente me enseñó con gran ejemplo el camino de la bondad y el amor al prójimo.

Además, agradecimientos especiales a mis dos grandes amigos, por su paciencia y orientación académica en este proyecto, pero sobre todo porque a su lado conocí el verdadero valor de la amistad.

Finalmente, al director y subdirector de la Institución Educativa N° 1138 José Abelardo Quiñones, por las facilidades que me brindaron para realizar la recolección de datos de esta investigación dentro de las aulas abelardinas.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

El presente trabajo de investigación tuvo por objetivo determinar la relación existente entre el uso de redes sociales y la vulneración del Derecho a la Protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024. Para ello se empleó el diseño de investigación no experimental, de tipo cuantitativo con alcance correlacional. La técnica de investigación que se utilizó fue la encuesta cuyo instrumento consistió en un cuestionario aplicado a 187 estudiantes matriculados en el 4to y 5to grado del nivel secundaria. La técnica de análisis incluyó herramientas de estadística descriptiva e inferencial. Los resultados evidenciaron la existencia de una relación significativa entre las variables uso de redes sociales y vulneración del derecho a la protección de datos personales, ya que el coeficiente de correlación de Spearman devolvió un valor de 0.909, lo que sugirió la existencia de una relación positiva muy fuerte y significativa entre las variables de estudio, concluyéndose que altas vulneraciones del derecho a la protección de datos personales de los estudiantes se asocian con el uso de redes sociales.

Palabras clave: derecho a la protección de datos personales, redes sociales, adolescentes, datos personales.

Abstract

The purpose of this research was to examine the relationship between social network use and the violation of the Right to Data Protection in students at the Educational Institution N°1138 José Abelardo Quiñones in 2024. To achieve this, a non-experimental research design was employed, characterized by a quantitative approach with a correlational scope. Data were collected through a survey administered to 187 students enrolled in the 4th and 5th levels of secondary education, using a questionnaire as the primary research instrument. The analysis involved both descriptive and inferential statistical tools. The findings revealed a significant relationship between social network use and the violation of the right to data protection, as evidenced by a Spearman correlation coefficient of 0.909. This indicates a very strong and significant positive relationship between the two variables. Consequently, it can be concluded that a considerable portion of the violations of students' right to data protection can be attributed to their engagement with social media.

Keywords: right to the protection of personal data, social networks, teenagers, personal data

I.INTRODUCCIÓN

El avance de las tecnologías de la información y su enorme capacidad de almacenamiento, procesamiento e intercambio de información personal representa un beneficio significativo para la sociedad moderna plenamente informatizada; sin embargo, supone también la desafiante tarea de unir esfuerzos para asumir las amenazas que conlleva, especialmente en relación al disfrute efectivo de los derechos fundamentales.

Las redes sociales en línea son espacios de interacción social cuyo principal insumo es la información personal de los usuarios. El acceso a estas plataformas no es realmente gratuito como se suele pensar. La realidad es que se alimentan primordialmente de la información personal que reciben de los usuarios, la misma que es sometida a diversos tratamientos con fines que generalmente se identifican con la obtención de ganancias económicas para el gestor de la red social. No obstante, el universo de las redes sociales es tan grande y accesible que cualquier persona puede realizar tratamientos de datos personales con fines no siempre lícitos.

Ante esta realidad, cabe preguntarnos si ¿Los usuarios realmente advierten las consecuencias de su participación en esta forma de comunicación en lo que respecta a la protección de sus datos personales? Creemos que la respuesta es negativa. Probablemente, podría argumentarse que los riesgos son asumidos por voluntad propia de los usuarios; no obstante, el razonamiento no es tan simple cuando se trata de usuarios menores de edad. Son dos las razones que sustentan lo anterior: i) El menor se encuentra en proceso de desarrollo, y ii) El deber del Estado de proteger de manera especial a los menores.

Es claro que los menores participan activamente en estos espacios y que la mayoría de ellos no está en la capacidad de realizar la custodia y supervisión del flujo de su información personal, lo que repercute en la facultad de control de sus datos personales. Los menores no cuentan con las herramientas necesarias para gestionar de manera adecuada su información personal en redes sociales. Esto conlleva a un uso inadecuado de estas plataformas.

Esta situación nos revela la necesidad de determinar el alcance de estos entornos digitales en relación a la situación humana, concretamente en el ámbito del derecho a la protección de los datos personales de los menores de edad, ello a fin de advertir las principales vulnerabilidades que se derivan de su uso y fortalecer un oportuno control y eficacia del citado derecho fundamental. Determinar la relación que existe entre el uso de las redes sociales y la vulneración del derecho a la protección de datos personales resulta sustancial ya que permitirá advertir cómo la vulnerabilidad de los usuarios menores de edad repercute en el núcleo esencial del derecho a la autodeterminación informativa.

La presente investigación se refiere a la relación que existe entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, para ello se toma como referencia la regulación jurídica del derecho fundamental a la protección de datos personales en el marco de las redes sociales.

El propósito central consiste en probar la hipótesis que relacione el uso de redes sociales y la vulneración del derecho a la protección de datos personales, ya que, desde la perspectiva de esta investigación, el uso de redes sociales está asociado con niveles altos de vulneración del derecho antes mencionado. Para ello, se lleva a cabo un estudio basado en el enfoque cuantitativo de alcance correlacional y se emplea un cuestionario como instrumento para medir las variables de investigación en una determinada población estudiantil de la Institución Educativa N°1138 José Abelardo Quiñones.

En el primer capítulo, se describe y formula el problema de investigación; asimismo, se señala las antecedentes internacionales y nacionales que permitirán ubicar el estado actual de la investigación.

En el segundo capítulo, se estudian las bases teóricas de la investigación, desarrollando con amplitud las teorías existentes en relación al problema de investigación para así proveer un marco referencial que informe el estudio; en ese sentido, se desarrollan las variables y sus

dimensiones (redes sociales y derecho a la protección de datos personales), así como, los fundamentos teóricos del enfoque adoptado para sustentar el problema planteado.

El tercer capítulo abarca la estructura metodológica de la investigación, consignándose el diseño y el enfoque de investigación; así como, la técnica y el instrumento para la recolección de datos.

El cuarto y quinto capítulo comprenden los resultados y la discusión de resultados, respectivamente, los cuales han sido obtenidos a partir de la aplicación del cuestionario. Finalmente, en el sexto y sétimo capítulo se abordan las conclusiones y recomendaciones, respectivamente.

1.1. Descripción y formulación del problema

La era digital ha traído consigo la proliferación de las redes sociales en línea que ha supuesto un impacto positivo para la sociedad conectando usuarios y facilitando el intercambio de información. No obstante sus ventajas, el uso de estas plataformas digitales supone también el surgimiento de diversas amenazas para los derechos fundamentales que obliga abordar una respuesta jurídica.

En los últimos tiempos, las redes sociales han incrementado su presencia en las actividades del ser humano. Según el Global Digital Report 2024 elaborado por We Are Social en alianza con Meltwater existen más de 5,037 millones de usuarios registrados en redes sociales, lo que equivale al 62,3% de la población mundial; mientras que, a inicios del año 2024, el Perú cuenta con 24,05 millones de usuarios activos en redes sociales, lo que equivale al 69,7 % de la población total.

En este contexto, la garantía del derecho a la protección de datos personales se ha convertido en un desafío significativo que merece una atención especial en su análisis. En primer lugar, el contenido que se comparte en redes sociales revela una gran cantidad de datos personales tales como las características personales o físicas que terminan registrados en una

nube digital. En segundo lugar, la posibilidad que ofrece a sus usuarios de transmitir y difundir datos personales de manera intuitiva- con un solo clic-y de acceder a ellos con gran facilidad. En tercer lugar, la dificultad de los usuarios de redes sociales de comprender el mecanismo utilizado para recopilar y utilizar sus datos personales.

Las redes sociales son empleados por un alto porcentaje de menores de edad quienes han ingresado prematuramente al ciberespacio, por lo que su acceso representa un riesgo significativo para la protección de sus datos personales derivado de su propia condición de «nativos digitales» que suelen exponer de manera peligrosa su información personal sin el conocimiento de los alcances que implica dicha actividad. De esta manera, en su interacción en las redes sociales se encuentran constantemente expuestos a la pérdida del control de sus datos de carácter personal y, por ende, a la vulneración de su derecho a la protección de datos personales.

En el Perú, la Ley N°29733, Ley de protección de datos personales y su Reglamento representan esfuerzos significativos a fin de responder a este desafío. No obstante, el rápido avance de la tecnología y el acceso de los menores a la red, cada vez más frecuente, ha superado la capacidad de estas normativas para responder a esta problemática.

Se plantea que la forma en la que los menores hacen uso de estas plataformas digitales se encuentra asociada a la vulneración del derecho a la protección de los datos personales, ya que no suelen tener plena consciencia de los riesgos inherentes al uso de estos medios, incorporándose a ellas desconociendo sus reglamentaciones y funcionamiento sin tener elementos que les permitan identificar las amenazas que implica el tratamiento indebido de sus datos personales, lo cual constituye un problema medular en relación a la efectividad de este derecho.

Pese a ello, estos usuarios no son protegidos de manera especial conforme lo exige el principio del interés superior del niño y del adolescente, que supone una mayor intervención

en el ámbito preventivo y proteccionista en cuanto al control de sus datos personales, por ser una situación que puede afectar su desarrollo. En general, la legislación existente no responde de manera eficaz a este planteamiento.

Se entiende que esta problemática se debe fundamentalmente a la ausencia de una cultura de protección de datos personales; asimismo, a la carencia de la integración de la educación en asuntos relacionados a la ciberseguridad como un componente esencial en los niveles de aprendizaje, y en general, a la ausencia de un marco jurídico eficaz que provea verdaderos mecanismos de protección de los menores de edad.

Es importante reconocer que el uso de redes sociales trae aparejada afectaciones derivados de la sobreexposición de la información personal por parte de los adolescentes, lo que a su vez puede traer consigo riesgos físicos, mentales y económicos para los usuarios e incluso a sus personas más cercanas, riesgos que pueden materializarse en *ciberbullyng*, racismo, *sexting*, *grooming*, exposición al *phishing*, ejercicio abusivo del *profiling*, suplantación de identidad, extorsión digital y afectaciones a otros derechos fundamentales como la intimidad, el honor o la imagen.

En virtud al contexto anteriormente referido, la relevancia de esta investigación radica en la necesidad de garantizar una efectividad real del derecho a la protección de datos personales de los menores en el ámbito de las redes sociales, así como proponer iniciativas preventivas y proteccionistas que minimicen las repercusiones del uso de redes sociales y fomenten un entorno digital que promueva su uso responsable.

1.1.1. Problema General

PG: ¿Qué relación existe entre el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024?

1.1.2. Problemas Específicos

PE 1: ¿Qué relación existe entre el uso de la red social Facebook y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024?

PE 2: ¿Qué relación existe entre el uso de la red social TikTok y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024?

1.2. Antecedentes

1.2.1. Antecedentes Internacionales

Ordóñez (2021), en su tesis doctoral titulada "*El derecho fundamental a la protección de datos personales en Ecuador"* de la Universidad de Cádiz. En relación a su metodología, se empleó el enfoque cualitativo de tipo descriptivo. La presente investigación tuvo por objetivo estudiar el desarrollo del derecho a la protección de datos personales en Ecuador, así como, analizar su Ley Orgánica de Protección de Datos Personales. En ese sentido, el referido trabajo de investigación concluyó que la Ley de protección de datos personales de Ecuador pretende promover un marco jurídico compatible que facilite el intercambio de datos personales y a la vez respete y proteja los derechos humanos; asimismo, en relación a la protección de datos de los menores de edad, concluyó que la falta de concientización sobre los peligros que supone el acceso a medios informáticos constituye un problema medular en relación al respeto del derecho a la protección de datos personales, por lo que se requiere que su garantía suponga la

adopción de mecanismos especiales de tutela, resultando destacable el desarrollo del derecho a la educación digital previsto en la Ley de protección de datos personales.

Rodríguez (2021), en su tesis para obtener el grado de Magíster, titulada "*Las formas discursivas y la protección de datos personales en las redes sociales. Facebook Inc. ¿Consentimiento informado? Sí&Acepto"* de la Universidad de San Andrés de Buenos Aires. En relación a su metodología, se empleó el enfoque cualitativo de tipo descriptivo y analítico. La investigación tuvo por objetivo verificar en el entorno online la adecuación de la empresa Facebook a la normativa vigente en Europa desde el 25 de mayo de 2018 en materia de protección de datos personales. En ese sentido, se concluyó sosteniendo que debido a su extensión y complejidad, los documentos que forman parte del contrato de Facebook no aseguran una privacidad amigable, por lo que resulta imperioso seguir estudiando el modo en que Facebook emplea los datos personales; asimismo, señaló que la acumulación de datos es el bien principal del activo patrimonial de las redes sociales y que el exceso de la información compartida y la falta de conciencia sobre el valor de los datos propicia que terceras personas usen la información con fines ilícitos; finalmente, sostuvo que resulta imperioso educar a la población en relación a la privacidad en línea.

Mayorga-Veloz et al. (2024) en su artículo de investigación titulado *"Las redes sociales y la violación al derecho a la intimidad"* publicado en la Revista Verdad y Derecho. En cuanto al método, el estudio se desarrolló mediante una metodología descriptiva documental, con enfoque comparativo. La investigación tuvo por objetivo analizar las redes sociales y la violación al derecho a la intimidad. En el estudio, los autores concluyeron que existe un insuficiente marco normativo para garantizar una protección efectiva de los datos personales y la privacidad en la era digital, por lo que se requiere la implementación de reformas legislativas que aborden la responsabilidad de las plataformas y los derechos individuales, con especial atención en la regulación del uso indebido de la información.

Galvis (2019), en su tesis presentada para optar por el título de Doctor en Derecho, titulada "*Protección de datos personales de Niños, Niñas y Adolescentes. En el marco de juridificación y prevención del riesgo digital en Colombia*" de la Universidad Santo Tomas- Bogotá. En relación a su metodología, acoge el tipo de investigación socio-jurídica, basado en el método sistémico, empleando el proceso cualitativo y descriptivo de las variables. La investigación tuvo por objetivo analizar el régimen de protección de datos personales de niños, niñas y adolescentes de Colombia frente a los Estándares de Protección de Datos Personales para los Estados Iberoamericanos; de tal forma que, se estableció como conclusión que el ejercicio de derechos por parte de los niños, niñas y adolescentes como usuarios de redes sociales y la falta de mecanismos efectivos de tutela de los derechos ARCO en el ámbito digital requiere de la implementación de un Sistema global de Protección de la Privacidad e Información de niños, niñas y adolescentes en la era digital adecuado a los estándares internacionales de privacidad y tratamiento de datos personales a nivel proteccionista y preventivo; además, sostuvo que se requiere incorporar al ordenamiento jurídico los Estándares de Protección de Datos Personales de los Estado Iberoamericanos y un modelo de gestión de riesgos de seguridad digital para los menores.

Manzano y Galarza (2020), en su tesis para la obtención del grado de Magíster en Derecho Constitucional, titulada "*El Estado como garante del derecho a la protección de datos personales y el derecho a la intimidad de adolescentes inmersos en las redes sociales en el Ecuador*" de la Universidad de Otavalo. En relación a su metodología, se empleó el enfoque mixto de tipo descriptivo. La investigación tuvo por objetivo analizar el cumplimiento de la intimidad y la protección de datos personales de los adolescentes inmersos en las redes sociales para la efectiva protección de los referidos derechos constitucionales. En ese sentido, la investigación concluyó estableciendo que Ecuador cumple de manera parcial con la obligación de garantizar de forma integral los derechos a la intimidad y protección de datos personales de

los adolescentes inmersos en las redes sociales; asimismo, concluyó estableciendo que los adolescentes exponen de manera voluntaria y libre sus datos personales en las redes sociales, desconociendo la magnitud del riesgo al que se exponen, por lo que este grupo etario constituye un grupo vulnerable en relación al cumplimiento de sus derechos. Ante ello, sostienen que se requiere de una atención especial por parte del Estado para apoyar el ejercicio de su derecho a la protección de datos personales.

1.2.2. Antecedentes Nacionales

Hidalgo (2020), en su tesis para obtener el título de abogado intitulado *"El paradigma del derecho global para la protección de datos personales en redes sociales*" de la Universidad Católica Santo Toribio de Mogrovejo. En cuanto al aspecto metodológico, se empleó el enfoque cualitativo de tipo descriptivo. La investigación tuvo por objetivos establecer un mecanismo jurídico idóneo para evitar el uso abusivo de datos personales en redes sociales desde la perspectiva del derecho global y determinar la influencia de las redes sociales en el ámbito de las relaciones personales y en el manejo de la intimidad; en ese sentido, se concluyó que las redes sociales tienen un gran impacto en la sociedad al modificar sus relaciones personales permitiendo que la comunicación sea más fluida; sin embargo, también resultan ser un escenario en el que terceros pueden acceder a la información de los usuarios debido a la sobreexposición de información en la plataforma, de manera que se presenta una vulneración a la intimidad; asimismo, se concluyó que los mecanismos de protección autorregulados por las redes sociales, en especial Facebook, no cumplen con la finalidad del derecho a la protección de datos personales y que resulta conveniente una regulación de la protección de datos personales de alcance global que sea aplicable a todos los Estados con la finalidad de cubrir los vacíos de las legislaciones existentes.

Zevallos (2021), en su tesis para obtener el grado de Doctor en Derecho, titulada "*Redes sociales y su incidencia en la vulneración del derecho a la intimidad en los habitantes de*

Trujillo, 2020", en la Universidad César Vallejo. En cuanto a su metodología, se empleó el enfoque cuantitativo de tipo básica y diseño correlacional causal. La investigación tuvo por objetivo analizar la incidencia de las redes sociales en la vulneración del derecho a la intimidad en los habitantes de Trujillo, así como relacionar las redes sociales con la vulneración al derecho a la intimidad en sus diferentes dimensiones, en los habitantes de Trujillo, 2020. Entre las conclusiones a las que se arribaron figura que existe incidencia muy significativa de las redes sociales en la vulneración del derecho a la intimidad de los habitantes de Trujillo, en la medida que a mayor exposición a las redes sociales mayor es la vulneración del derecho a la intimidad; asimismo, se determinó que la relación entre las redes sociales y la dimensión de derecho a la protección de las comunicaciones privadas del derecho a la intimidad es altamente significativa, en el mismo sentido, la relación entre las redes sociales y la dimensión derecho a la salvaguardia de los datos personales del derecho a la intimidad es altamente significativa, lo que demostró que las redes sociales repercuten directa y muy significativamente en la vulneración del derecho a la salvaguardia de los datos personales; así, a mayor exposición en las redes sociales mayor es la vulneración del derecho a la salvaguarda de los datos personales; finalmente, respecto a la relación entre las redes sociales y la dimensión vulneración de los derechos sexuales se determinó que las redes sociales repercuten directa y muy significativamente en la vulneración de los derechos sexuales.

Jauregui y Maldonado (2023), en su tesis presentada para obtener el título de abogado, titulada *"Los datos personales y su tratamiento como activo para la publicidad de Facebook",* en la Universidad Católica San Pablo. En relación a su metodología, se empleó el enfoque cualitativo y el tipo dogmático-jurídico. La investigación tuvo por objetivo determinar si los datos personales y su tratamiento son un activo para la publicidad de Facebook, en ese sentido, se concluyó que Facebook se constituye en una plataforma atractiva para la publicidad y dado que esta requiere conocer al usuario previamente, lo importante para Facebook es el

conocimiento obtenido de los datos personales, lo que se hace posible mediante su tratamiento, por lo que los datos personales y su tratamiento constituyen un activo para la publicidad de Facebook; asimismo, se estableció que resulta importante conocer el trasfondo y consecuencias del uso de plataformas digitales como Facebook ya que pueden ocasionar vulneraciones a la intimidad.

Terrones(2021) en su tesis para obtener el grado de Maestro en Derecho Constitucional, titulada "*Derechos fundamentales de los niños y adolescentes en redes sociales*" en la Universidad Nacional Federico Villarreal. En cuanto a su metodología, se empleó el enfoque cuantitativo de nivel descriptivo – explicativo. La investigación tuvo por objetivo establecer los motivos por los cuales la protección legal de los derechos fundamentales de los menores y adolescentes en las redes sociales es ineficaz. El estudio concluyó sosteniendo que si bien los menores de edad cuentan con acciones legales para salvaguardar sus derechos como la intimidad y la forma en que se emplean sus datos personales, ninguna de ellas logra un restablecimiento absoluto de estos dado que los contenidos subidos al internet nunca pueden desaparecer; asimismo, se logró establecer que el derecho de protección de datos personales es ineficaz por cuanto el plazo transcurrido entre la solicitud al operador de la red, la tutela administrativa y el hábeas data, no permite la restauración del derecho de manera inmediata; finalmente, se llegó a concluir que la protección de los datos personales de los niños y adolescentes resulta trascendental porque los encargados de los Bancos de datos los comercializan sin tomar en cuenta el fin para el que son empleados.

Chávez (2022), en su tesis para obtener el título de Abogada, titulada "*Las redes sociales y el derecho fundamental a la intimidad de los niños, niñas y adolescentes en el Perú*" en la Universidad Nacional Santiago Antúnez de Mayolo. En relación a su metodología, se realizó bajo el tipo de investigación jurídica teórica o dogmática y diseño descriptivo. La investigación tuvo por objetivo analizar de qué forma las redes sociales viene afectando el

derecho fundamental a la intimidad de los niños, niñas y adolescentes, se llegó a la conclusión que las violaciones a los derechos fundamentales más frecuentes se centran en las redes de ocio y se relacionan con intromisiones ilegítimas en el honor, intimidad, derecho de la imagen, a lo que se suman cuestiones derivadas de la protección de datos de carácter personal de los niños y adolescentes, la protección de consumidores, el ejercicio abusivo de la libertad de expresión, entre otros aspectos; asimismo, se estableció que existe un preocupación por la alta participación de los niños, niñas y adolescentes en redes sociales, quienes sin ser conscientes de las consecuencias publican todo tipo de información sobre ellos y otros usuarios, lo que trae como consecuencia la afectación de la esfera integral de protección del menor.

1.3. Objetivos

1.3.1.Objetivo General

OG: Determinar la relación existente entre el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024.

1.3.2.Objetivos Específicos

OE 1: Determinar la relación existente entre el uso de la red social Facebook y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024.

OE 2: Determinar la relación existente entre el uso de la red social TikTok y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024.

1.4. Justificación

1.4.1.Justificación teórica

La investigación planteada se justifica teóricamente porque abordará un tema escasamente estudiado en el campo jurídico, como es la vinculación del uso de las redes sociales con el derecho a la protección de datos personales. Asimismo, contribuirá a desarrollar la compresión sobre cómo las redes sociales se asocian con el desenvolvimiento social de los menores y el control de su información personal, núcleo esencial del derecho a la protección de datos personales.

La investigación permitirá incrementar el conocimiento respecto de la regulación jurídica de las redes sociales y los derechos digitales.

1.4.2.Justificación práctica

Los resultados de este estudio permitirán alertar a los actores sociales respecto de la problemática planteada, ofreciendo la posibilidad que se adopten mecanismos jurídicos especiales con un enfoque claramente preventivo que busque la protección integral de los estudiantes que hacen uso de redes sociales de manera que se garantice la efectiva tutela de los datos personales de los menores de edad. Asimismo, será de utilidad práctica para que las instituciones educativas fomenten contenidos pedagógicos para padres, educadores y estudiantes sobre temas relacionados a la ciberseguridad y así promover hábitos responsables en el mundo digital.

1.4.3.Justificación metodológica

El presente estudio se justifica metodológicamente porque sigue los procedimientos del método científico utilizando un enfoque cuantitativo orientado a determinar la validez de las hipótesis planteadas. Para la investigación, se elaboró un cuestionario basado en la revisión de la literatura, instrumento que se aplicó a una muestra de estudiantes con el fin de recolectar datos confiables sobre la manera en la que los estudiantes hacen uso de las redes sociales y su

relación con la vulneración del derecho a la protección de datos personales. El estudio permite sugerir herramientas cuantitativas para futuras investigaciones en el campo jurídico.

1.4.4.Justificación social

La presente investigación se justifica socialmente porque busca entender de qué manera el uso de redes sociales puede incidir en la esfera integral de los menores de edad, lo que puede contribuir a crear mayor conciencia en los padres sobre la importancia de proteger la información personal de sus hijos y promover el uso de herramientas de control parental en las redes sociales.

1.5. Hipótesis

1.5.1.Hipótesis General

HG: Existe una relación significativa entre el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones 2024.

1.5.2.Hipótesis Específicas

H1: Existe una relación significativa entre el uso de la red social Facebook y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024.

H2: Existe una relación significativa entre el uso de la red social TikTok y la vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024.

II.MARCO TEÓRICO

2.1. Bases teóricas sobre el tema de investigación

2.1.1.Redes sociales

2.1.1.1.Definición

Las redes sociales han logrado incorporarse en la vida diaria de las personas al convertirse en parte fundamental de la interacción social con otros individuos, logrando con ello la transformación de la estructura social y la forma de vida de las personas, en donde los límites geográficos no representan un obstáculo.

Los investigadores Boyd y Ellison (2008) definen las redes sociales en línea como servicios en la web que permiten a las personas: 1) construir un perfil público o semipúblico dentro de un sistema limitado, 2) articular una lista de otros usuarios con quienes comparten una conexión y 3) ver y rastrear su lista de conexiones y las realizadas por otros dentro del sistema.

Por su parte, el profesor Orihuela (2008) define a la red social como un servicio basado en la web que permite al usuario relacionarse y compartir información, en donde se construye una identidad online.

En síntesis, las redes sociales digitales se constituyen en espacios virtuales que permiten al usuario configurar un perfil virtual con el cual interactúa, se conecta e intercambia contenidos con una mayor cantidad de personas.

El núcleo esencial de las redes sociales radica en la creación de un «perfil» con el cual el usuario se presenta ante la comunidad. El Instituto Nacional de Ciberseguridad (2019) destaca esta característica al definir a la red social como “un servicio en línea donde cada usuario/a tiene un perfil con sus datos personales”. (Sección segunda). En el mismo sentido, Blasco (2021) refiere que “las redes sociales nos permiten mostrar ‘un perfil con sus datos

personales’”. (p.99). En otras palabras, el atractivo principal de estas plataformas radica en la posibilidad del usuario de crear un perfil digital conformado por sus datos personales.

Profundizando en la importancia y el atractivo de la idea de «construir un perfil», Aguilar y Said (2010) han advertido que la construcción de un perfil en dichas redes virtuales facilita al usuario organizar los rasgos de la identidad que desea mostrar.

En ese sentido, la red social virtual es una comunidad en la que cada usuario comparte parte de su individualidad para construir una identidad según su conveniencia, perfil que le permite presentarse ante el resto de usuarios con el objeto de interactuar y comunicarse con otras personas.

Quizá una de las razones de su éxito radica en su facilidad para conectar personas pues supone una forma de comunicación horizontal y rápida (Díaz, 2011).

Estas plataformas han fomentado la participación activa de los usuarios, por lo que se les identifica con el desarrollo de la denominada Web 2.0, nuevo modelo de participación y comunicación en el que el usuario deja el papel de consumidor pasivo para convertirse en un suministrador de contenidos y datos que contribuye a la formación de conocimiento en la red de redes. Siendo así, las redes sociales online se caracterizan también por ser espacios en el que el usuario no solo consume, sino también colabora y coopera, particularmente con su información personal logrando así la máxima interacción entre los usuarios. Como consecuencia de ello, el control de la información y los contenidos pasa a los usuarios.

En general, se desprende que las características fundamentales de una red social están referidos a la posibilidad de construcción de un perfil conformado por datos personales del usuario, el favorecimiento de la comunicación y la generación de comunidades de usuarios en donde el intercambio de información en tiempo real es una ventaja de grandes dimensiones.

Son plataformas que favorecen la integración del mundo físico y el mundo virtual, de tal forma que ambos espacios se retroalimentan. De este modo, lo que sucede en el espacio virtual puede trascender al mundo físico y viceversa.

2.1.1.2.Facebook

Facebook es unas de las redes sociales digitales más populares e importantes en todo el mundo. En la actualidad, pertenece a la empresa matriz de Meta Platforms, por lo que la empresa Facebook ahora se llama Meta y la forma en la que Facebook recoge, usa, comparte, conserva y transfiere los datos se rige a la fecha de la presente investigación por la Política de privacidad de Meta (versión 26 de junio de 2024). La sede de la empresa se encuentra en Menlo Park, California.

Fue creado por Mark Zuckerberg en el año 2004 como una web para estar en contacto con sus compañeros de la universidad; posteriormente, en el año 2006 la red alcanzó a expandirse mundialmente. Con el paso del tiempo, Facebook fue creciendo y se convirtió en la red social más grande del mundo. Según el Global Digital Report 2024, Facebook es la red social con más usuarios activos globales, respaldado por 3,049 millones de usuarios activos mensuales, lo que representa un 37.7% de la población total mundial.

El modelo de negocio de esta plataforma se encuentra basado en brindar acceso gratuito a la plataforma, recaudando ganancias a partir de los anuncios publicitarios personalizados que se muestran y consumen en la red. El sitio permite a sus usuarios crear un perfil, acumular amigos/seguidores, interactuar y establecer una comunicación a nivel global.

Como ya se señaló anteriormente, la plataforma en teoría es gratuita; sin embargo, para el registro y el posterior uso el interesado tiene que facilitar obligatoriamente una serie de datos personales, tales como su edad, género, correo electrónico o número de teléfono; luego, durante la interacción en la plataforma el usuario también presta información sobre sus gustos y/o actividades, los mismos que son sometidos a diversos tratamientos por el operador de la red

social con la finalidad de utilizarlos como insumo para la personalización de los anuncios que se muestran en la web.

Durante el proceso de registro, la plataforma proporciona un mensaje indicando: "*Al hacer clic en Registrarte, aceptas las Condiciones, la Política de privacidad y la Política de cookies. Es posible que enviemos notificaciones por SMS, que podrás desactivar cuando quieras".* Las palabras subrayadas son enlaces que dirigen a los documentos que señala. Además, en la parte inferior de la ventana aparece un botón verde que indica la acción «Registrarte», pudiendo el interesado dar clic en este último sin necesidad de acceder a cualquiera de los enlaces señalados previamente para hacer uso de los servicios de la red social.

De lo anterior, es posible sostener que la red social no resalta lo suficiente los documentos mediante los cuales se brinda la información necesaria al interesado respecto al tratamiento de sus datos personales (Política de Privacidad); elemento indispensable para la emisión de un consentimiento informado e inequívoco como lo requiere la normativa, en particular si se trata de menores de edad.

En relación a este último aspecto, Garduño y Magaña (2023) afirman que un diseño como el referido – presentar el aviso de privacidad en forma de hipervínculo- impediría al usuario conocer plenamente los usos que se dan a los datos personales y, por ende, vulneraría la autodeterminación informativa.

En igual sentido, la Agencia Española de Protección de Datos Personales en un procedimiento sancionador instruido a Facebook. INC hizo la advertencia al gestor de esta red social respecto a la manera en la que se obtenía el consentimiento para el tratamiento de los datos personales puntualizando en que "se hace obligado que en la práctica el procedimiento para la obtención del oportuno consentimiento informado no se lleve a cabo con un simple clic, como ocurre en el presente caso concreto con un recuadro con una expresión 'Terminado'".

(Resolución R/01870/2017, del 21 de agosto de 2017, p.81). Pese ello, es fácil advertir que la versión peruana de la plataforma persiste con la misma práctica.

Por otro lado, de la lectura que se hace de las «Condiciones del servicio» (versión 26 de julio de 2022) se desprende que Facebook está disponible para mayores de 13 años, es decir, permite que un menor de edad de 13 años pueda crear una cuenta, lo que implica proporcionar alguno de sus datos personales y autorizar su tratamiento, sin que se habiliten opciones para el consentimiento de los padres o tutores. Al respecto, cabe precisar que la normativa peruana de protección de datos personales establece que solo los mayores de 14 años pueden emitir un consentimiento válido para el tratamiento de sus datos personales; siendo así, resulta evidente que las «Condiciones de servicio» que la plataforma pone a disposición para su lectura se encuentra en contradicción con lo establecido en nuestra legislación, ya que permite que quienes tengan 13 años brinden «consentimiento» para el tratamiento de sus datos personales, cuando la norma es clara al establecer que para este grupo de menores es indispensable el consentimiento de los titulares de la patria potestad o tutores.

Aunado a lo anterior, la plataforma adolece del defecto común en la mayoría de las redes sociales, esto es, no cuenta con mecanismos efectivos de comprobación de la edad, generando que los menores puedan crear cuentas usando edades falsas y sean desprotegidos de las protecciones especiales que se hayan habilitado al efecto para las cuentas de menores de edad.

Facebook recopila varios datos personales de los usuarios que le llega a través de diversos canales, los mismos que son tratados por la plataforma a fin de proporcionar anuncios personalizados. Es decir, a cambio del servicio, el usuario otorga a la empresa la facultad de tratar sus datos personales con fines económicos. Esto se desprende del apartado «Cómo se financian nuestros servicios» de las Condiciones de servicio, documento en el cual se describe lo siguiente: "*En lugar de pagar por usar Facebook…aceptas que podemos mostrarte anuncios*

personalizados y contenido comercial y publicitario de otro tipo de empresas y organizaciones que nos pagan por promocionarse dentro y fuera de los Productos de las empresas de Meta". Continúa indicando lo siguiente: "*Usamos tus datos personales, como la información sobre tu actividad y tus intereses, para mostrarte el contenido publicitario y los anuncios personalizados*".

Dentro del universo de datos personales que recaba la plataforma, singular atención merece lo establecido en relación a la categoría de datos especialmente protegidos, pues la Política de privacidad indica que la red social puede recopilar información sobres las creencias religiosas, ideología política, origen étnico o racial, así como datos relacionados con la salud y la pertenencia a sindicatos; sin embargo, no señala en ningún apartado que para ello deberá recabarse un consentimiento que ha de ser expreso y escrito, conforme lo requiere la normativa. El único registro que realiza el usuario para que Facebook inicie el tratamiento de estos datos especialmente protegidos es pulsar el botón «Registrarte», sin que se recabe un consentimiento específico en forma escrita para el tratamiento de sus datos personales sensibles.

Ahora bien, en relación a la fuente de los datos personales, la Política de Privacidad establece que se recopila información que el usuario proporciona voluntariamente cuando se registra en la Plataforma y crea un perfil (su dirección de correo electrónico, teléfono o foto de perfil) y cuando realiza determinadas acciones como rellenar formularios; también se recopila información sobre la actividad que realiza el usuario en la plataforma (contenido que crea, mensajes que envía y recibe, incluso el contenido de los mismos, también aplicaciones y funciones que usa, compras u otras transacciones que realiza, tipos de contenido que ve y cómo interactúa, hora, frecuencia y duración de la actividades que realiza); información sobre sus amigos, seguidores, grupos, cuentas, páginas de Facebook y otros usuarios y comunidades con las que interactúa, incluye la forma en la que se interactúa con ellos; por otro lado, información relativa al dispositivo en el que se haga uso del servicio (p. ej., de qué tipo de dispositivo se

trata, cómo se usa el dispositivo, señales GPS y de Bluetooth del dispositivo, puntos de accesos a redes Wifi cercanas al dispositivo, datos relacionados con la ubicación, incluso si los servicios de ubicación están desactivados, información sobre la red a la que conecta su dispositivo y su conexión, incluida la dirección IP, información que se comparte con la plataforma a través de la configuración del dispositivo); información procedente de socios, proveedores y otros terceros relativa a la información y acciones que el usuario lleva a cabo tanto dentro como fuera de la Plataforma (p. ej., información de su dispositivo, sitios web a los que accede, aplicaciones que usa, datos demográficos sobre el usuario, anuncios que ve); asimismo, información sobre el usuario en función de la actividad de terceros (se recopila y deduce datos basado en la actividad de otras personas); finalmente, recopila información de cookies y tecnologías similares.

En cuanto a los fines del tratamiento y a la modalidad de tratamiento, en la Política de privacidad se indica que la información se recopila y asocia con el usuario y otros usuarios de manera automática a fin de personalizar la plataforma. De esta manera, se recaba información del usuario para proporcionar, personalizar y mejorar la red social, para promover la seguridad, la integridad y la protección en los productos Meta, para ofrecer servicios empresariales y de medición y de análisis, para comunicarse con el usuario, para identificar al usuario y personalizar los anuncios que se muestran a través de Meta Audience Network cuando visite otras aplicaciones, para realizar investigaciones e innovar en beneficio del bienestar social, para transferir, conservar o tratar la información de los usuarios en otros países, finalmente, para compartir información con terceros, como fuerzas de seguridad y responder requerimientos jurídicos.

En cuanto a la cesión de los datos, se señala que se comparte información con las otras Empresas de Meta que ofrecen Productos de Meta como WhatsApp, Marketplace, Instagram,

entre otros; asimismo, con otras empresas de Meta, con socios, proveedores de medición y marketing, proveedores de servicios y otros terceros.

Finalmente, en cuanto a la posibilidad del ejercicio de los derechos que forman parte de la protección de datos personales se establece la garantía del derecho a acceder a la información que Meta tiene sobre el usuario; asimismo, el derecho a la portabilidad, así como el derecho a la supresión de datos personales.

2.1.1.3.TikTok

TikTok es una red social de origen chino cuyas actividades de funcionamiento iniciaron en el año 2016. Es propiedad de la empresa China *ByteDance.*

Esta plataforma digital permite a sus usuarios crear, editar, compartir y descubrir videos de diferentes temáticas. Al igual que otras redes sociales, los usuarios pueden crear un perfil y «seguir» a otros usuarios, dar «me gusta», interactuar y comentar los videos. Se caracteriza por ofrecer contenidos de consumo rápido destinados al entretenimiento, con funcionalidades de fácil acceso. Además, la plataforma incluye la posibilidad de enviar mensajes, tener una lista de «amigos» y un sistema de seguidores y seguidos.

Debido a su sencillez basado en la presentación de videos verticales de corta duración, la plataforma ha logrado incorporarse de forma exitosa en el mercado de redes sociales en línea. Según el Global Digital Report 2024, TikTok tuvo el promedio de tiempo por usuarios en Android más alto de todas las plataformas sociales en el mundo, alcanzando entre el mes de julio y setiembre de 2023, 34 horas al mes – más de una hora al día- en la plataforma. Actualmente, cuenta con 1,562 millones de usuarios activos en todo el mundo. Sin duda, desde su incorporación en el mercado es una plataforma que ha tenido un crecimiento sumamente veloz.

Se sabe que una de las razones de su incomparable éxito consiste en ofrecer a sus usuarios contenido personalizado en función de sus intereses y preferencias. Sin embargo,

detrás de esta curiosa funcionalidad se encuentra la actividad de tratamiento de una gran cantidad de datos personales de sus usuarios que incluso se inicia antes del registro en la Plataforma, dado que desde el acceso a la aplicación la plataforma presenta opciones en las cuales se ofrece al usuario la posibilidad de seleccionar sus intereses.

Dado lo anterior, TikTok ha sido cuestionada por temas referidos a la seguridad de la información personal. Así, luego de un estudio riguroso, Perkins (2022) a través de la organización líder en seguridad cibernética denominada Internet 2.0 ha afirmado que esta red social solicita demasiados permisos en el dispositivo y recopila excesivos datos, mucho más de los que necesita para que la aplicación funcione. A modo ilustrativo, el autor refiere que la plataforma recopila información detallada sobre nuestros dispositivos y las aplicaciones instaladas, así como historial de transacciones y compras.

Para poder interactuar y disfrutar de los servicios ofrecidos por esta red social digital es necesario que el usuario se registre con un correo electrónico o un número de teléfono; o, asocie su cuenta con otra red social como Facebook o cuenta Google. El proceso de registro implica proporcionar cualquiera de los elementos señalados; así como, la fecha de nacimiento; luego, se establece un nombre de usuario y una clave. A continuación, la plataforma presenta una ventana emergente que señala: “Al pulsar «Aceptar y continuar», aceptas nuestros Términos del servicio y confirmas haber leído nuestra Política de privacidad para saber cómo recopilamos, utilizamos y compartimos tus datos”. Las palabras subrayadas aparecen marcadas en negrita y son enlaces que conducen a los Términos del servicio y a la Política de privacidad. Debajo del párrafo, aparece un botón etiquetado como «Aceptar y continuar». Desde un servidor web peruano, se ha podido verificar que no es obligatorio acceder a la Política de privacidad para empezar con el uso del servicio, por lo que adolece del mismo defecto señalado respecto a la red social Facebook.

De acuerdo a los Términos del Servicio (versión de febrero de 2021 disponible a la fecha de la presente investigación) los servicios prestados son para personas que tengan 13 años de edad en adelante (con límites adicionales que se podrían establecer en los «Términos Complementarios»); sin embargo, en el citado apartado no se reconocen las disposiciones que en materia de consentimiento rigen en la legislación peruana. De esta manera, las condiciones de TikTok relativas a la edad mínima requerida para hacer uso del servicio no son compatibles con la normativa peruana que establece que la edad mínima de los menores de edad para prestar el consentimiento por sí solos es a partir de los 14 años. Asimismo, en relación al acceso a esta plataforma, se repite el inconveniente consistente en la ausencia de medidas adicionales que garanticen la identidad y edad de la persona que se está registrando.

En cuanto a la fuente de los datos, la Política de privacidad (versión del 02 de enero de 2024 disponible a la fecha de la presente investigación) establece las siguientes fuentes: i) Datos proporcionados por el usuario, ii) Información recopilada automáticamente e iii) Información proveniente de otras fuentes.

En relación a la información proporcionada por el usuario, se trata usualmente de información que se brinda al momento del registro en la Plataforma (nombre de usuario, fecha de nacimiento, dirección de correo electrónico, número de teléfono, fotografía o video de perfil), o durante el uso del servicio (contenido que el usuario genera en la plataforma como fotos y videos, contenido de los mensajes y su información, información de compra, información de contactos móviles o redes sociales).

En lo que respecta a la información recopilada automáticamente, estos incluyen, información de uso de la Plataforma (anuncios, videos, contenido que le gusta al usuario, historial de navegación, búsqueda, entre otros.), información inferida (inferencia de intereses, atributos, rango de edad a fin de personalizar el servicio), información técnica del usuario (el dispositivo que usa, aplicaciones, operador móvil, tipo de red, etc.), información de ubicación

aproximada, información de imagen y audio (la existencia y la ubicación dentro de una imagen de las características y atributos de la cara y el cuerpo, la naturaleza del audio y el texto de las palabras que se hablan en el Contenido del usuario); y, cookies (empleada para analizar cómo se utiliza la Plataforma, incluidas las páginas que ve el usuario con mayor frecuencia y cómo interactúa con el contenido).

Frente a la información de otras fuentes, se incluye información proveniente de otras cuentas de redes sociales o servicios – cuando se utilice la plataforma con datos de esas cuentas; asimismo, información que brindan los anunciantes, socios de medición y otros socios sobre actividades llevadas a cabo fuera de la plataforma; también se recaba información del usuario brindada por entidades de su grupo corporativo; información proveniente de comerciantes y procesadores de pagos; finalmente, información sobre el usuario proveniente de otras personas y de fuentes disponibles públicamente.

Sobre las finalidades del tratamiento de datos, la plataforma señala que la información recopilada es utilizada principalmente para i) Mejorar, brindar asistencia y administrar la plataforma, ii) Usar sus funcionalidades y iii) Cumplir y hacer cumplir los Términos del servicio. Agrega a estos fines, los relacionados a la personalización del contenido que se ve, promoción de la plataforma y personalización de publicidad. Al respecto, resulta cuestionable que en la redacción de los fines se utilicen términos como los siguientes: "*Por lo general, usamos la información…*" o "*Podemos usar la información para, entre otras cosas*…"; ya que es obligación del responsable del tratamiento cumplir con especificar de manera concreta todos los fines del tratamiento de datos (artículo 6° de la Ley N°29733, Ley de Protección de datos personales), lo que significa la prohibición de usar términos indeterminados como los señalados.

En cuanto a las operaciones de tratamiento de datos, se realizan tratamientos consistentes principalmente en la recopilación, análisis y cesión de datos. En cuanto a este

último, se señala que la información recopilada por la plataforma puede ser compartida con Socios Comerciales, Proveedores de servicios que brindan asistencia a la Plataforma, anunciantes, redes publicitarias y socios de medición, investigadores independientes, con el grupo corporativo de la empresa y comerciantes, proveedores de procesamiento de pagos y otros proveedores de servicios.

Finalmente, en cuanto al ejercicio de los derechos que forman parte de la protección de datos personales se establece que se puede solicitar el derecho a acceder, eliminar, actualizar o rectificar los datos, a ser informado del tratamiento de los datos y otros derechos, según la ley aplicable al caso.

2.1.2.Derecho fundamental a la protección de datos personales

2.1.2.1.Antecedentes históricos

El derecho a la protección de datos personales nace como una respuesta a la necesidad de regular el tratamiento automatizado de la información personal a través del uso de las tecnologías de la información y su potencial poder de vigilancia.

En la evolución y consolidación del derecho a la protección de datos personales, la figura de la privacidad ha constituido un elemento decisivo pues es a partir de su contenido que el derecho a la protección de datos personales ha ido adquiriendo autonomía propia.

De esta manera, es posible sostener que su nacimiento se enmarca en el ámbito norteamericano en donde se gesta la construcción jurídica del derecho a la intimidad (*right to privacy*), cuando Samuel Warren y Louis Brandeis publicaron en 1890 su conocido artículo intitulado "*The Right to Privacy*" en la Harvard *Law Review*. En el referido ensayo, Warren y Brandeis (1890) sostuvieron que los avances de la civilización expresado en los nuevos inventos han dado lugar a que el hombre sea más vulnerable frente a la posibilidad invasiva de la tecnología, de tal forma que la intimidad se convierte en un valor estimado de la persona que

de ser invadida puede causar un sufrimiento espiritual. Ante este riesgo, estos autores expresan la necesidad de configurar un principio fundamentado en la personalidad inviolable que garantice el control sobre aquella información personal que pueda afectar la integridad psicológica de la persona.

Así, la *privacy* fue la respuesta de los norteamericanos al acelerado crecimiento de las tecnologías de la información y su capacidad invasiva en la vida privada de las personas. Desde aquel entonces, la cuestión de la privacidad fue un asunto imparable en la conquista de las sociedades democráticas. A través del tiempo, el derecho a la vida privada adquirió mayor relevancia en la legislación internacional y en la jurisprudencia de los tribunales internacionales y constitucionales.

Por su parte, la tradición jurídica europea emprendió las primeras manifestaciones del derecho a la protección de datos personales sobre la base de los derechos a la intimidad, el honor y la imagen, así como, sobre la idea de la «vida privada». De esta forma, encontramos que en el año 1970 fue aprobada en Alemania la primera Ley de protección de datos personales. Se trata de una normativa histórica dictada en el Land de Hesse, limitada a su territorio y a los centros de información electrónicos manejados por autoridades públicas.

Posteriormente, a principios de los años 80 surgieron algunos instrumentos normativos que pusieron especial interés en el tratamiento de los datos personales, como el documento denominado “Directrices relativas a la Protección de la Intimidad y de la circulación transfronteriza de datos personales”(1980) expedido por la Organización para la Cooperación y Desarrollo Económico (OCDE), en el cual se recomendó a los países la adopción de criterios mínimos para el tratamiento de datos personales que impliquen peligros para la intimidad. Este documento constituye el primer instrumento supranacional que aborda el tema de la protección de datos personales.

Asimismo, el Convenio 108 del Consejo de Europa sobre la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (1981) constituye un antecedente fundamental en el desarrollo del derecho a la protección de datos personales, ya que es el primer instrumento jurídicamente vinculante a nivel de Europa en el que se establecen los principios básicos de la protección de datos personales. A partir de su gestación, el derecho a la privacidad adquiere una connotación distinta al entender los actores políticos que este último ya no aporta una protección suficiente frente a la aparición de las primeras bases de datos gestionados por grandes industrias. De conformidad con el referido Convenio, los Estados debían adoptar medidas pertinentes para hacer efectivas ciertas pautas en relación al tratamiento de datos personales, pautas expresadas en los principios de equidad, legalidad, proporcionalidad, confidencialidad, información, así como, en los derechos de acceso y rectificación.

Especial atención merece el aporte que realiza Alemania en la formulación de este derecho al que reconoció como «autodeterminación informativa». Pese a que ya contaba con una ley que la regulaba parcialmente (Ley Federal sobre protección de datos de 1977), la consolidación de esta figura fue expresada en la sentencia de la Primera Sala del 15 de diciembre de 1983 sobre el caso Censo de la Población, en el cual el Tribunal Constitucional Federal Alemán estableció lo siguiente:

> Quien no pueda estimar con suficiente seguridad, qué informaciones sobre sí mismo son conocidas en determinadas esferas de su medio social … puede verse restringido esencialmente en su libertad para plantear o decidir con base en su propia autodeterminación. Un ordenamiento social y un orden global en el que los ciudadanos no pudieran conocer *quiénes, cuándo* y *en qué circunstancias* saben *qué* sobre ellos, sería incompatible con el derecho a la autodeterminación de la información. (Huber, 2009, p.96)

De esta forma, sobre la base del derecho a la dignidad y el libre desarrollo de la personalidad, el Tribunal Constitucional Alemán formuló el derecho autónomo a la autodeterminación informativa ampliada a una dimensión activa basada en el control, decisión y vigilancia por parte del titular de datos personales, desligada del fundamento del derecho a la intimidad.

Con el tiempo, ante la revelación del valor económico de los datos personales y su importancia en la economía del mercado, la Unión Europea se preocupó por garantizar su libre circulación con pleno respeto de los derechos fundamentales, por lo que se gestó una normativa de garantías mínimas a la que debían sujetarse sus Estados Miembros, se trata de la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta Directiva impuso obligaciones al responsable del tratamiento de datos personales ante la necesidad de velar por el respeto de los derechos fundamentales, especialmente el respeto a la intimidad. Asimismo, convocó a sus Estados miembros a crear un organismo cuya función principal sea supervisar las operaciones de tratamiento de datos personales.

A partir de estos elementos históricos, la protección de datos personales ha tenido una evolución normativa constante hasta consolidarse como un derecho fundamental autónomo e independiente del derecho a la intimidad. Dicha consolidación se atribuye a la Carta de Derechos Fundamentales de la Unión Europea proclamada en el año 2000, la misma que le reconoció tal naturaleza de forma expresa.

Durante el trayecto normativo del derecho a la protección de datos personales puede afirmarse que es en la Unión Europea en donde el tema ha venido desarrollándose con mayor interés constituyéndose en un modelo para otras regulaciones del mundo, siendo el principal referente el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril

de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE.

2.1.2.2.Delimitación conceptual

Antes de ingresar al desarrollo de su definición y naturaleza, es preciso puntualiza que este derecho ha sido denominado indistintamente como derecho a la autodeterminación informativa o derecho a la protección de datos personales. En nuestro país, se ha seguido la tendencia legislativa mayoritaria de Iberoamérica que lo reconoce como derecho a la protección de datos personales.

En cuanto a su naturaleza, es considerado por diversas regulaciones normativas como un derecho fundamental autónomo y un principio o norma de valor.

El reconocido constitucionalista peruano Landa (2017) afirma que el derecho a la protección de datos personales "faculta a su titular a ejercer control sobre la información que sea recolectada, registrada o almacenada en base de datos, archivos o registros de cualquier tipo bajo gestión o administración de entidades públicas o privadas" (p.75).

En consonancia con ello, Landa (2017) también refiere que existe una doble vertiente de la institución, al señalar que como derecho subjetivo supone el ejercicio del control de la información personal; mientras que, como principio, impone obligaciones al Estado o instituciones privadas que almacenan datos personales.

En un sentido similar, nuestro Tribunal Constitucional lo define estableciendo que "consiste en la serie de facultades que tiene toda persona para ejercer el control sobre la información personal que le concierne, contenidos en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos" (Exp. N° 04739-2007-PHD/TC, de fecha 15 de octubre de 2007, F.J.2).

De manera que, el derecho a la protección de datos personales se constituye como un derecho en sí mismo cuya principal característica radica en el poder de control que tiene la persona respecto a su información personal contenida en cualquier soporte.

En el ámbito extranjero, la jurista mexicana Román (2023) sostiene que es un "derecho fundamental que se traduce en la potestad de las personas para decidir sobre el uso que se hace de sus datos personales" (p.360-361). Donoso y Reusser (2021) sostienen que "es el derecho del individuo de controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos las condiciones en que dichas operaciones pueden llevarse a cabo" (p.20).

Sin perjuicio de su autonomía como derecho fundamental, en la delimitación conceptual de este derecho resulta importante resaltar su carácter instrumental, por el cual se constituye en una garantía al servicio de otros derechos constitucionales que pueden resultar afectados por el tratamiento indebido de los datos personales, tales como el honor, la imagen personal o la intimidad.

En suma, el derecho a la protección de datos personales constituye un elemento primordial en la configuración de la autonomía individual, dado que una sociedad no puede garantizar debidamente la soberanía de la persona sobre sí misma si no garantiza que la persona pueda ejercer un control real del flujo de su información personal, especialmente cuando se realizan tratamientos automatizados en el marco de la comunicación en internet.

2.1.3.Normativa peruana en materia de protección de datos personales

En cuanto a la legislación interna, debemos partir por establecer que la Constitución Política del Perú no contempla de manera específica el derecho a la protección de datos personales. El numeral 6 del artículo 2° señala de manera muy laxa que toda persona tendrá derecho "*A que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecten la intimidad personal y familiar*." De lo anterior se

evidencia una regulación sesgada del derecho a la protección de datos personales al establecer su interdependencia con el derecho a la intimidad y limitar su ejercicio únicamente frente a los servicios informáticos (Castro, 2008).

La Constitución Política solo prevé una limitación a los servicios informáticos cuya finalidad se circunscribe a proteger el derecho a la intimidad personal y familiar y no hace referencia concreta al derecho a la protección de datos personales como un derecho autónomo desligado de su antecedente y con posibilidad de proteger derechos fundamentales distintos a la intimidad. Asimismo, reconoce únicamente el derecho a impedir el suministro de datos personales, dejando de lado la precisión de sus otros contenidos. Pese a estas deficiencias en su redacción, se ha entendido que el contenido constitucional del derecho a la protección de datos personales no se limita a dicha facultad constitucionalizada expresamente, sino que deben ser consideradas todas aquellas facultades destinadas a ejercer un control real de los datos personales (Linares, 2020).

Por otro lado, la Constitución Política prevé en su artículo 200° una garantía procesal constitucional específica y autónoma que procede ante cualquier hecho u omisión que vulnere o amenace el derecho a la protección de datos personales, se trata del denominado proceso de «Hábeas Data». Consiste en un proceso de naturaleza constitucional que tiene por objeto la protección de los derechos establecidos en los incisos 5 y 6 del artículo 2° de la Carta Política, estos son, el derecho a la autodeterminación informativa y el derecho de acceso a la información pública.

El desarrollo legislativo del derecho a la protección de datos personales se encuentra en la Ley N°29733, Ley de Protección de Datos Personales, de fecha 02 de julio de 2011 (en adelante la Ley) norma nacional básica en materia de protección de datos personales que reconoce el derecho fundamental a la protección de datos personales y establece una serie de aspectos sustantivos y adjetivos a fin de garantizarlo. Tiene por objeto la protección integral de

los datos de carácter personal contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y administración privada cuyo tratamiento se realice en el territorio nacional.

Aunado a la regulación anterior, el Reglamento de la Ley Protección de Datos Personales aprobado a través del Decreto Supremo N° 003-2013-JUS, de fecha 21 de marzo de 2013 (en adelante el Reglamento) es un instrumento legal importante que busca garantizar el cumplimiento de las obligaciones asociadas al derecho a la protección de datos personales.

Con la finalidad de garantizar un marco jurídico regulador efectivo, la Ley dispuso la creación de la Autoridad Nacional de Protección de Datos Personales, una autoridad de control independiente y responsable de supervisar la observancia de la legislación sobre protección de datos personales. Depende jerárquicamente del Ministerio de Justicia.

Frente al vertiginoso avance de la tecnología en los últimos años y su consiguiente impacto en la protección de los datos personales, diversos ordenamientos jurídicos han actualizado sus normativas en la materia a fin de responder a los desafíos que plantea esta nueva realidad. Basta señalar la adopción del Reglamento Europeo de Protección de Datos (en adelante, Reglamento (UE) 2016/679) que entró en vigor el 25 de mayo de 2018 para advertir que el nuevo contexto regulatorio internacional ha cambiado. En el mismo sentido, son ejemplos de cambios recientes las legislaciones de Uruguay y Argentina. Cabe agregar que las legislaciones regionales han optado por receptar el Reglamento (UE) 2016/679 en sus normas internas sobre la materia.

Actualmente, en nuestro país se encuentra en marcha esfuerzos legislativos a fin de contar con un nuevo Reglamento de desarrollo de la Ley en los próximos meses. La iniciativa se encuentra bajo la dirección del Ministerio de Justicia para lo cual se ha constituido una Comisión que ya ha logrado publicar el Proyecto del Nuevo Reglamento de la Ley de Protección de Datos Personales (en adelante el proyecto del nuevo Reglamento). Sin duda, la

aprobación de esta normativa significará un paso decisivo en la conformación de una cultura de protección de datos ya que sigue los lineamientos más modernos en la materia.

Por cuanto al tiempo de redacción de esta investigación no encontramos bibliografía especializada que estudie de forma profunda la Ley y su Reglamento, se tomará gran parte de la información proveniente de obras de la comunidad europea a fin de interpretar la normativa de protección de datos.

2.1.4.La regulación del dato personal

La noción de lo que constituye dato personal es muy extensa. Se trata de *"Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados"* (art .2.4 de la Ley). En otras palabras, se entiende por dato personal toda aquella información sobre una persona «identificada» o «identificable».

Sobre la categoría «persona identificada», Polo (2020) sostiene que se trata de una información que "indica directamente a esa persona sin necesidad de utilizar un conjunto de medios para poder averiguar su identidad (DNI, pasaporte, etc.)" (p.180). Es decir, la información permite diferenciar por sí sola a la persona respecto de los demás.

Ahora bien, en cuanto al término «persona identificable» la normativa peruana actual no la define. Sin embargo, el proyecto del nuevo Reglamento considera que nos encontramos ante una persona identificable cuando "*se puede verificar la identidad de la persona de manera directa o indirectamente*" (numeral 4 del artículo II). Por consiguiente, lo relevante es que se trate de un dato que permita identificar – a través de medios razonablemente utilizados- a la persona que todavía no ha sido identificada.

Polo (2021) explica que nos encontramos en un supuesto de persona identificable cuando se trata de un dato que por sí solo no aporta información acerca de la persona, ni la identifica, pero sí suministra información suficiente para poder descubrir su identidad.

Conforme se ha señalado, dicha identificación puede realizarse de manera «directa» o «indirecta». El Dictamen 4/2007 sobre concepto de datos personales elaborado por el Grupo de Trabajo del Artículo 29 (2007) considera que una persona puede ser identificable directamente por sus nombres y apellidos, debido a que estos son los identificadores más comunes a través de los cuales la información original se asocia con una persona física que puede ser distinguida de otros individuos. Por otra parte, se habla de una persona identificable indirectamente cuando se puede lograr su identificación a través de la combinación del identificador disponible con otros datos; estos son, uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social, los cuales permitirán distinguir a una persona de otra.

El referido Dictamen cita como ejemplos de información que hace identificable indirectamente a una persona el número de teléfono, el número de pasaporte, la matrícula de automóvil o una combinación de criterios significativos (edad, empleo, domicilio, etc.).

De esta forma, en el ámbito europeo la categoría de «persona identificable» se encuentra delimitado por los «identificadores» disponibles». Al respecto, la consideración de que un determinado identificador puede ser suficiente para distinguir una persona de otra dependerá del medio utilizado y de las circunstancias concretas del caso. Así lo ha establecido el Reglamento (UE) 2016/ 679 en cuyo considerando 26 se establece que para determinar si una persona física es identificable deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona. Además, para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesario para la identificación, teniendo en cuenta la tecnología disponible en el momento del tratamiento.

En cuanto a los medios de identificación nuestra legislación establece que se considerarán aquellos que razonablemente puedan ser utilizados para lograr identificar a una persona, esto significa que si no existe una posibilidad real y plausible de lograrlo la información no se considerará dato personal.

De esta forma, la información que puede catalogarse como dato personal es diversa pudiendo consistir en cualquier información referida a la identidad personal, física, psicológica, social, cultural, académica, económica que se vincule de manera directa o indirecta a una persona natural. Polo (2021) menciona algunos ejemplos que pueden llegar a constituir datos personales, estos son, el identificador de una cookie o el identificador de la publicidad del teléfono, la dirección del correo electrónico (cuando incluya el nombre de la persona), el ADN, el iris del ojo, las respuestas escritas de un aspirante a un examen, las comunicaciones, grabaciones de sonidos, entre otros.

De la misma manera, se ha llegado a la consideración de que las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso y en tanto permiten identificar al usuario constituyen datos de carácter personal. En igual sentido, los perfiles creados en las redes sociales son considerados datos de carácter personal (Véase la Sentencia del Tribunal de Justicia de la Unión Europea, del 16 de febrero de 2012, asunto C-360/10, caso SABAM, ap. 49).

Lo que la normativa pretende proteger son aquellos datos que permitan identificar a la persona y que tal vez aisladamente no tenga importancia, pero que en conjunto pueden afectar el espacio más íntimo del ser humano. De esta manera, la Ley y el Reglamento son aplicables únicamente a los datos personales; es más, no cualquier dato personal, sino solamente datos de las personas naturales, excluyéndose así los datos pertenecientes a las personas jurídicas.

Dentro del género de datos personales se encuentra la figura de los «datos sensibles», los mismos que se refieren a aquellos datos que revelan la esfera más íntima de la persona y

que por tanto requieren de un régimen especial de protección. Se consideran dentro de esta categoría aquellos que revelan el origen racial y étnico, los ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; información relacionada con la salud o la vida sexual, así como los datos biométricos que por sí mismos pueden identificar al titular. La normativa dispone que el consentimiento para el tratamiento de esta categoría de datos debe ser otorgado por escrito.

En cuanto a la forma de presentarse los datos personales, la Autoridad Nacional de Protección de Datos Personales ha señalado que el tratamiento de datos que no estén contenidos en bancos de datos personales también debería efectuarse conforme a los lineamientos establecidos en la Ley y el Reglamento, por lo que el responsable del tratamiento es el titular del banco de datos cuando se trata de datos contenidos en un banco de datos y también puede ser quien decide sobre el tratamiento cuando los datos no se encuentren en un banco de datos personales (Opinión Consultiva N° 43-2020-JUS/DGTAIPD, de fecha 09 de octubre de 2020). De esta manera, la garantía de protección alcanza también a aquellos datos personales que no se encuentren contenidos en un banco de datos personales.

2.1.5.El concepto de tratamiento de datos personales en el marco de las redes sociales

El entendimiento de lo que constituye un «tratamiento de datos personales» es elemental por cuanto definirá el ámbito de aplicación de la normativa de protección de datos personales. Así, el Reglamento señala que la normativa se aplicará a "*toda modalidad de tratamiento de datos personales"* (art.3°). Por su parte, la Ley define al tratamiento como "*Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales*". (art.2.19). De esta forma, el concepto

de tratamiento estará determinado por una concreta «operación» sobre los datos de carácter personal.

De lo anterior se desprende que cualquier tipo de operación con datos personales y realizados en los términos que señala la Ley constituye un tratamiento, sin importar la modalidad de tratamiento, el agente que realice la operación o el soporte en el que se encuentre.

La Autoridad Nacional de Protección de Datos Personales ha interpretado el significado de «tratamiento de datos» dándole un sentido extenso. Así, por ejemplo,, refiriéndose al ámbito del internet, ha considerado que las actividades desarrolladas por los motores de búsqueda constituyen actividades de tratamiento de datos personales dado que indexan información contenida en diversos links poniéndola a disposición de los internautas con una mera indagación nominal a través de sus buscadores. (Resolución Directoral N° 2377 -2018-JUS/DGTAIPD-DPDP, del 24 de setiembre de 2018).

Sin perjuicio de lo anterior, el Reglamento excluye de su ámbito de aplicación el tratamiento de datos personales realizado por personas naturales para fines exclusivamente personales, domésticos o relacionados con su vida privada o familiar.

Se sostiene que se presenta una actividad personal “cuando los datos tratados afectan a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos” (Véase la Sentencia 3077/2006 de la Sección Primera de la Sala de lo Contencioso -Administrativo de la Audiencia Nacional de España, del 15 de junio de 2006, F.D. Tercero). En el ámbito local, los especialistas Iriarte y Bolaños (2024) sostienen que para aplicar la exención deben presentarse dos requisitos, estos son, que el tratamiento sea realizado por una o más personas naturales y que el fin sea estrictamente doméstico, personal y/o relacionado con su vida privada o familiar. Son ejemplos de estos supuestos la agenda de direcciones de amigos, el tratamiento que se realiza para cursar invitaciones a una boda, entre otros.

Se sostiene que no procederá considerar que una actividad es exclusivamente personal o doméstica cuanto tenga por objeto permitir a un número indeterminado de personas el acceso a datos personales o cuando la actividad se extienda, aunque sea en parte, al espacio público y esté dirigida hacia el exterior de la esfera privada de la persona que procede al tratamiento de los datos personales (Sentencia del Tribunal de Justicia de la Unión Europea del 10 de julio de 2018, asunto C-25/17, apartado 42).

La excepción doméstica resulta importante en relación a las actividades que se despliegan dentro de las redes sociales digitales. Como se sabe, es habitual que los usuarios de estas plataformas incluyan contenidos de otras personas en sus respectivos perfiles, lo que sin duda constituye un tratamiento de datos personales; sin embargo, generalmente estos tratamientos se encuentran excluidos del cumplimiento de la normativa de protección de datos personales al ser amparados por la llamada excepción doméstica, lo que supone la inaplicación de las disposiciones sobre protección de datos personales. A modo de ejemplo, podría considerarse tratamiento de datos con fines domésticos cuando un usuario publica una fotografía grupal en el perfil de una determinada red social para un número limitado de amigos.

Pese a lo anterior, se considera que en el ámbito de las redes sociales los usuarios efectúan también determinados tratamientos de datos de carácter personal que no pueden ampararse en la referida excepción y que por ello deberán regirse por la normativa de protección de datos, cuestión que se encuentra pendiente de definir en el ámbito jurídico peruano, pero que ya ha sido materia de pronunciamiento en el ámbito europeo por parte del Grupo de Trabajo del artículo 29 que ha definido tres actividades desarrolladas en el entorno de las redes sociales que no pueden ser cobijados en el supuesto de excepción. En estos casos se entiende que el usuario es responsable del tratamiento de datos personales de otras personas que fueron publicados en su perfil.

2.1.6. El responsable del tratamiento de datos personales en las redes sociales digitales

Entender el concepto de «responsable del tratamiento» resulta fundamental a fin de determinar quién responderá por el cumplimiento de la normativa de protección de datos. El numeral 14 del artículo 2° del Reglamento conceptualiza la figura del responsable del tratamiento señalando que es aquella persona que decide sobre el tratamiento de datos de carácter personal. La Autoridad Nacional de Protección de Datos Personales ha señalado que el responsable del tratamiento es "aquella persona natural o jurídica que define los fines o medios a través de los cuales se llevará a cabo el mismo" (Resolución Directoral N° 2377 -2018-JUS/DGTAIPD-DPDP, de fecha del 24 de setiembre de 2018, p.9).

Con una técnica similar, el Comité Europeo de Protección de Datos (2021) ha afirmado que la determinación de los fines y medios implica que el responsable de tratamiento defina el por qué tiene lugar el tratamiento y cómo se alcanzará ese objetivo.

Según se encuentra redactado en las Condiciones de servicio de las diferentes plataformas de redes sociales, los usuarios proporcionan un sinfín de datos personales durante el uso del servicio en donde los fines de la recopilación de estos datos son definidos por el gestor de la red social, quien además presta los medios para su registro, conservación y supresión; por tanto, es innegable que los proveedores de estos servicios deban ser considerados responsables del tratamiento de datos personales de los usuarios y cumplir con la normativa peruana de protección de datos personales. En igual sentido, se considerarán responsables del tratamiento de datos personales aquellos usuarios que realicen operaciones con datos personales de otros usuarios en la medida que deciden sobre la finalidad y uso de los datos recopilados.

Lo anterior quedó establecido en el Dictamen 5/2009, sobre redes sociales en línea, adoptado el 12 de junio de 2009 por el por el Grupo de Trabajo del Artículo 29 (2009) al

sostener que los proveedores de servicios de redes sociales son responsables del tratamiento porque brindan los medios para tratar los datos de los usuarios y porque determinan la forma en la que los datos de sus usuarios pueden emplearse con fines comerciales.

Conforme se mencionó en el apartado anterior, en determinados casos los usuarios también pueden ser considerados responsables del tratamiento de datos personales de sujetos que pueden ser o no miembros de la red social. En el Dictamen mencionado supra el Grupo de Trabajo del artículo 29 (2009) ha establecido tres supuestos en los cuales un usuario podría ser calificado como «responsable del tratamiento». Así, en primer lugar, cuando el usuario actúa en nombre de una empresa o de una asociación o utiliza la red social principalmente como una plataforma con fines comerciales, políticos o sociales; en segundo lugar, cuando el usuario adquiere un gran número de contactos terceros y no conoce a alguno de ellos para quienes el acceso a los datos está disponible; finalmente, cuando el usuario permite el acceso a la información del perfil más allá de los contactos elegidos, en particular, cuando los datos pueden ser indexeables por los motores de búsqueda o cuando todos los miembros que pertenecen a la red social puede acceder al perfil; o, cuando el usuario decide ampliar el acceso más allá de los «amigos» elegidos.

En consonancia con lo anterior, los autores peruanos Iriarte y Bolaños (2024) reproducen los mismos supuestos de aplicación de la normativa de protección de datos personales afirmando que un usuario de redes sociales podría ser considerado responsable del tratamiento de datos personales respecto del banco de datos personales que constituye su cuenta de usuario.

En los mencionados supuestos se entiende que no se presenta un tratamiento de datos con fines domésticos o personales ya que se presenta una cesión indiscriminada de datos donde se pierde el control de la información personal (Troncoso, 2012). En general, las actividades desarrolladas por los usuarios de redes sociales serán consideradas como parte de la excepción

doméstica siempre que mantengan dicha actividad en la esfera de su lista de contactos al círculo más cercano.

Debe tenerse presente que cuando el usuario de la red social se convierte en responsable del tratamiento de datos personales le serán exigibles las obligaciones legales establecidas en la Ley y el Reglamento. En líneas generales, deberá cumplir con garantizar el deber de información previo a la solicitud de consentimiento para el tratamiento de datos personales, solicitar autorización para enviar comunicaciones comerciales; así como, atender los requerimientos planteados en virtud del ejercicio de los derechos establecidos en la normativa.

Ahora bien, habiéndose señalado que los gestores de redes sociales realizan actividades de tratamiento de datos personales y que por tanto son responsables del tratamiento, cabe enfatizar en que estas plataformas pese a que sus centros de operaciones se encuentren en otros países les es aplicable la normativa peruana de protección de datos personales en virtud del numeral 4 del artículo 5° del Reglamento que señala que será de aplicación a todo tratamiento de datos cuando el titular del banco de datos personales o quien resulte responsable no se encuentre establecido en territorio peruano, pero utilice medios situados en este territorio para efectuar el tratamiento.

Estas plataformas digitales si bien no tienen un establecimiento físico ubicado en el territorio peruano, emplean medios establecidos en nuestro país a fin de efectuar los tratamientos de datos que requiere la prestación del servicio. Dichos medios podrían ser, a modo ejemplo, cookies que dirigen la publicidad a los consumidores que se encuentran en nuestro país.

2.1.7.Principios rectores para el tratamiento de datos personales

Son entendidos como normas de carácter general y fundamental que tienen como finalidad ser el soporte del desarrollo y aplicación de todo el sistema de protección de datos personales; además, operan como un conjunto de obligaciones que se deben cumplir en el

tratamiento de datos personales que garantice la protección efectiva de los derechos y libertades de las personas. Asimismo, se constituyen en elementos normativos que funcionan como criterios interpretativos e integradores en la aplicación de la Ley y el Reglamento.

Se describirán lo más nucleares en la configuración del derecho a la protección de datos personales.

2.1.7.1.Principio de legalidad

Este principio implica el reconocimiento del tratamiento de datos personales como una actividad reglada por el ordenamiento jurídico que debe sujetarse a lo establecido en la normativa pertinente. Supone la exigencia dirigida a todos los implicados en el tratamiento de datos personales de acomodar sus actividades a lo que establece el sistema de protección de datos personales, excluyéndose todo tratamiento arbitrario desde su recopilación hasta su cancelación.

El informe de la Asamblea General de las Naciones Unidas (2022) enfatiza en que la legalidad supone la necesidad de que el procesamiento de datos personales tenga como fundamento la configuración de alguna de las causales legitimantes para el tratamiento previstas en la normativa correspondiente de cada país. Atendiendo a ello, en nuestro ordenamiento jurídico el tratamiento de datos de carácter personal debe encontrarse basado en el consentimiento del titular de datos personales; o, en su defecto, en alguna de las excepciones al consentimiento previstas en el artículo 14° de la Ley.

2.1.7.2. Principio de consentimiento

El consentimiento se erige como la principal fuente de legitimación del tratamiento de datos personales ya que es una clara expresión de la facultad de «autodeterminación» de su titular.

La Ley entiende por consentimiento la manifestación de voluntad del titular de datos personales por la que acepta las operaciones de tratamiento de sus datos, es decir, es un acto

constitutivo a través del cual se autoriza una determinada actividad sin el cual no podría realizarse o si se realizase sería ilícito. En virtud de lo anterior, en la mayor parte de las actividades de tratamiento de datos personales el consentimiento debe prestarse antes de que el responsable emprenda cualquiera de las actividades previstas como tratamiento de datos de carácter personal.

Esta declaración de voluntad no obliga al interesado en el sentido de una irreversibilidad, ya que conforme al artículo 16° de la Ley el consentimiento puede ser revocado en cualquier momento, sin justificación previa, por cuanto el titular de datos sigue manteniendo cierto grado de control. La revocación tiene efectos *ex nunc*.

El consentimiento no consiste únicamente en una simple declaración, sino en una que cumpla con los requisitos estrictos establecidos en la normativa. Así, el artículo 7° del Reglamento establece que el consentimiento debe ser libre, previo, expreso, informado e inequívoco.

El consentimiento será libre cuando se otorgue sin que medio error, mala fe, violencia o dolo que puedan afectar una elección real del interesado. En estos supuestos que invalidan el consentimiento se trata de evitar que se ejerza cualquier presión o influencia sobre el titular de datos personales que impida que este ejerza su libre voluntad.

En la cuestión de si un consentimiento es o no libre resulta interesante lo contemplado en el Reglamento (UE) 2016/679 en cuyo considerado 43 se indica que no es posible hablar de un consentimiento verdaderamente libre en aquellos casos en los que existe un claro desequilibrio de poder entre el interesado y el responsable del tratamiento de datos personales. En este supuesto, se asume que se presenta una asimetría de poder que podría significar una falta de libertad implícita. Por ejemplo, se considera que determinados tratamientos de datos personales emprendidos por los empleadores o las autoridades públicas grafican esta situación,

por lo que se sostiene que en estos casos el consentimiento no debería ser una causa legitimadora del tratamiento.

En nuestro país, el proyecto del nuevo Reglamento con mejor técnica legislativa que la Ley y el Reglamento, introduce algunos supuestos que por las circunstancias en que se presentan conllevarían a invalidar el consentimiento por falta de libertad en su otorgamiento. Se trata del artículo que dispone que "*el consentimiento no será libre si el titular del dato personal no puede elegir, denegar o retirar su manifestación de voluntad sin que ello le genere algún perjuicio*". Constituye una circunstancia en la que el consentimiento se invalida por el temor del titular a sufrir un agravio real y concreto. En este caso, el responsable del tratamiento de datos debe demostrar que la retirada del consentimiento no supondrá un coste para el interesado.

Asimismo, tampoco será libre si se supedita la prestación de un servicio o la entrega de un bien o la firma de un contrato a la prestación del consentimiento para el tratamiento de los datos personales que no son necesarios para ello.

Respecto a este último supuesto de condicionalidad del servicio, el Comité Europeo de Protección de Datos (2020) explica que otorgar el consentimiento para un tratamiento de datos personales innecesario para la ejecución del contrato no puede considerarse como un requisito obligatorio para la prestación de un servicio, por lo que si la ejecución del contrato está supeditado a la prestación de un consentimiento que acepte un tratamiento de datos que no se encuentre vinculado directa y objetivamente con la ejecución del contrato, se entenderá que no hay un ejercicio libre del consentimiento. Además, si un responsable desea realizar un tratamiento de datos personales que sí es fundamental para la ejecución de un contrato el consentimiento no será el fundamento jurídico apropiado, es decir, no se aplica el consentimiento. La Comisión concluye indicando que, en cualquier caso, la carga de la prueba del consentimiento libre recae sobre el responsable del tratamiento y en tal caso se evalúa que

este responsable ofrezca un servicio equivalente – otro servicio- que no implique prestar el consentimiento para el uso de los datos con fines adicionales, debiendo ambos servicios ser realmente equivalentes.

Lo señalado por el Comité Europeo de Protección de Datos se puede entender con un ejemplo: una aplicación móvil de lectura de libros digitales solicita acceder al micrófono del celular como condición necesaria para hacer uso de la aplicación, de tal forma que, si no presta consentimiento para el tratamiento de esos datos, no se podrá hacer uso del servicio. En dichas circunstancias, si el interesado otorga su consentimiento para la recopilación de datos vinculados a su voz a través del micrófono se considerará que aquel no ha sido dado en condiciones de libertad pues el acceso al micrófono y la consiguiente obtención de ese tipo de datos no son necesarios para prestar el servicio básico ofrecido.

Siendo así, consideramos que la inclusión en nuestro ordenamiento jurídico de este supuesto de anulación del consentimiento- que tiene su antecedente en la legislación europea-es acertada, ya que hoy en día muchos proveedores de servicios digitales, interesados en cumplir con sus fines notoriamente económicos pretenden recabar más datos personales de los que realmente requieren para la prestación del servicio.

El consentimiento informado implica la obligación del responsable del tratamiento de datos personales de proporcionar información accesible al titular de datos personales antes de obtener su consentimiento, de tal forma que el titular ejerza un control real de su información personal como consecuencia de una decisión debidamente informada. La información que brinde el responsable del tratamiento consiste en una serie de elementos mínimos establecidos en el artículo 12° del Reglamento, como son la identidad de los que son o pueden ser los destinatarios, la transferencia de los datos que se efectúe, la existencia del banco de datos personales, entre otros. La previsión de un consentimiento verdaderamente informado obliga a

considerar como ilícitos aquellos consentimientos obtenidos con omisión de algunas de las informaciones listadas en el referido artículo.

Además, el cumplimiento de este requisito requiere que la comunicación de estas informaciones se realice de forma clara y empleando un lenguaje sencillo, de forma que "el mensaje debe ser comprensible para un ciudadano medio y no únicamente para juristas". (Comité Europeo de Protección de Datos, 2020, p.15).

En esta línea, la Agencia Española de Protección de Datos resalta la importancia de la información previa al consentimiento como un elemento esencial para el usuario de tal forma que si no se proporciona información clara y accesible el control del usuario sería ficticio (Resolución del Procedimiento Sancionador Nº: PS/00070/2019, de fecha 18 de noviembre de 2020).

En cuanto a la forma de otorgar el consentimiento la normativa peruana establece que debe ser expreso e inequívoco. Al respecto, cabe establecer que el actual Reglamento de la Ley no hace una distinción clara de los términos «expreso» e «inequívoco»; sin embargo, el proyecto del nuevo Reglamento establece su diferencia estableciendo que el consentimiento será expreso cuando se exteriorice a través de una acción que demuestre una aceptación concreta, directa y explícita; mientras que el consentimiento será inequívoco cuando se pueda apreciar que los actos materiales por parte del titular de datos personales manifiestan la aceptación indubitable, sin ninguna posibilidad de duda o equivocación, respecto a un determinado tratamiento de sus datos personales. En ese sentido, el consentimiento debe consistir en una clara y evidente acción o declaración afirmativa, no admitiéndose supuestos de consentimiento tácito.

Para cumplir con lo anterior, el consentimiento puede recabarse mediante una declaración verbal o escrita; así también, mediante medios digitales cuando se firma un documento a través de medios electrónicos o digitales, o cualquier otro mecanismo electrónico,

incluso mediante una manifestación consistente en “hacer clic”, dar un “toque”, “touch” o “pad” u otros similares que generalmente se presentan en el entorno digital. En todas estas formas de prestar el consentimiento el responsable del tratamiento debe garantizar que la acción de consentir se distinga de otras acciones relacionadas al tratamiento de datos personales evitando en todo momento cualquier situación de ambigüedad.

Con arreglo al Reglamento (UE) 2016/679 se tiene claro que el uso de las casillas de aceptación ya marcadas por defecto para recabar el consentimiento no es válido, así como tampoco será válido el silencio o la inactividad del interesado, o la continuación del uso del servicio.

En el caso de las redes sociales, el gestor de la plataforma generalmente recaba el consentimiento de sus usuarios mediante la aceptación de las Políticas de Privacidad; o, mediante el ajuste voluntario de los parámetros técnicos del servicio.

Sin duda, la figura del consentimiento constituye la piedra angular de todo el sistema de protección de datos personales que se regula en nuestro país. Como bien se afirma, a través de un sistema de declaración de voluntad del consentimiento el titular de datos personales tendrá la posibilidad de conocer las condiciones en las que se realizará el tratamiento antes de consentirlo (García- Ripoll, 2020).

Sin perjuicio de lo anterior, existen casos en los cuales el tratamiento de datos personales no requerirá el consentimiento del titular de datos personales, toda vez que confluyen causas que por sí solas legitimarán el tratamiento; se trata de las llamadas limitaciones al consentimiento que se encuentran listadas en el artículo 14° de la Ley.

En relación a estos supuestos, la Autoridad Nacional de Protección de Datos Personales ha precisado que estas excepciones no implican desconocer las demás obligaciones señaladas en la Ley y el Reglamento, por lo que el responsable del tratamiento de datos personales

igualmente deberá cumplirlas (Opinión Consultiva N°19-2019-JUS/DGTAIPD, de fecha 07 de marzo de 2019).

2.1.7.3.Principio de finalidad

Este principio se configura en dos vertientes, a saber: las características de la finalidad para lo cual se recopilan los datos personales y la obligación de que el tratamiento de datos personales se realice sin extenderse a una finalidad distinta a la establecida al momento de la citada recopilación.

En cuanto al primer aspecto, la Ley indica que la finalidad del tratamiento de datos personales debe ser determinada, explícita y lícita. La finalidad será determinada cuando se haya establecido de manera específica sin generalidades de ningún tipo; asimismo, será explícita cuando sea definida de manera clara y sin lugar a ambigüedades; finalmente, será lícita cuando los datos sean recopilados a través de medios lícitos establecidos en la Ley y el Reglamento.

El segundo aspecto de este principio consiste en la prohibición de realizar tratamientos de datos personales para una finalidad diferente a la previamente especificada, de forma que cualquier nuevo tratamiento con otros fines requerirá un nuevo fundamento jurídico. En otras palabras, el tratamiento de datos que se efectúe se encuentra limitado por la finalidad para la cual fueron recopilados.

De esta forma, todo tratamiento de datos de carácter personal con fines indefinidos o sin una finalidad concreta es ilícita (Agencia de los Derechos Fundamentales de la Unión Europea & Consejo de Europa, 2019).

Es una garantía que permite al interesado y en su caso a las autoridades de control verificar si un tratamiento de datos personales responde a la finalidad para lo cual se recabó el consentimiento.

2.1.7.4.Principio de proporcionalidad

Este principio constituye una garantía en función al cual el tratamiento de datos personales debe guardar una relación razonable con la finalidad para la que estos han sido recogidos. En tal sentido, el tratamiento de datos debe ser adecuado, relevante y no excesivo a sus fines.

En virtud de este principio, el responsable del tratamiento deberá realizar los esfuerzos pertinentes para que los datos personales sean tratados al mínimo necesario. Se trata del deber de "recabar solo la información necesaria para el cumplimiento de sus fines" (Hidalgo, 2018, p.35). A dicho deber, se agrega el deber de elegir el tratamiento de datos menos invasivo a la esfera personal, según la finalidad autorizada (Zamudio, 2021).

Por ejemplo, una aplicación de celular cuya finalidad es la edición de músicas intenta acceder a nuestra ubicación personal. En este caso, el tratamiento de datos de la ubicación del usuario será excesivo y desproporcionado en relación a la finalidad que el encargado de tratamiento busca cumplir, pues es más que obvio que para la edición de músicas no se requiere la información de la posición geográfica del equipo terminal de un usuario

2.1.7.5.Principio de calidad

Este principio establece obligaciones vinculadas a la exactitud y fidelidad de los datos que vayan a ser materia de tratamiento, exigiendo que el responsable del tratamiento de datos adopte las medidas pertinentes para mantener la veracidad de los datos. De manera complementaria a la citada obligación, la ley establece que - "en la medida de lo posible"- los datos sean actualizados, necesarios, pertinentes y adecuados en relación a la finalidad para la que fueron recopilados. En este segundo aspecto, la norma sugiere que el responsable establezca procedimientos de revisión y actualización que garanticen la exactitud total de los datos.

Respecto a los atributos que deberían poseer los datos personales que sean objeto de tratamiento, Donoso y Reusser (2021) afirman que la veracidad y la exactitud dependen de la actualidad, por lo cual el dato que vaya a ser sometido a una operación de tratamiento debe ir modificándose para adecuarse a cada situación personal. Asimismo, la Autoridad Nacional de Protección de Datos Personales señala que en virtud de este principio los datos personales deben ser revisados durante todo el tiempo en que se produce el tratamiento (Resolución Directoral N° 2377-2018-JUS/DGTAIPD-DPDP, del 24 de setiembre de 2018).

La importancia de este principio radica en evitar que se produzcan afectaciones a la dignidad de la persona por causa de decisiones que se tomen en virtud de un tratamiento de datos personales inexactos.

Respecto a la idea de la adecuación de los datos personales a su finalidad se prevé que no se recopilen más datos de los necesarios para cumplir la finalidad del tratamiento. A modo de ejemplo, si una determinada institución educativa tiene como finalidad establecer una base de datos para contactar a los responsables legales de los estudiantes en caso de presentarse una emergencia, sería innecesario que se recopilen datos referidos a los ingresos económicos de los padres, bastando únicamente los datos de contacto.

2.1.7.6.Principio de seguridad

El principio de seguridad se encuentra regulado en el artículo 9° de la Ley como una obligación dirigida al titular del banco de datos personales y al encargado del tratamiento de tomar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos de carácter personal.

Este principio implica la implementación de medidas de protección tendientes a propiciar un espacio confiable y controlado para evitar que los datos sean perdidos, alterados, adulterados, usados de manera ilícita o sujetos a un tratamiento no autorizado. Se trata de un principio que busca resguardar el carácter reservado de los datos personales.

La Autoridad Nacional de Protección de Datos Personales ha sostenido que el artículo 16° de la Ley que regula la seguridad del tratamiento de datos personales establece un objetivo general dirigido a garantizar la seguridad de los datos personales y un objetivo específico dirigido a la adopción de medidas para concretar la garantía antes señalada (Resolución Directoral N° 1114-2022-JUS/DGTAIPD-DPDP, de fecha 17 de marzo del 2022).

En el marco del Reglamento (UE) 2016/679 se considera que las medidas apropiadas para garantizar un nivel de seguridad adecuado serían aquellas que incluyan la seudonimización y el cifrado de datos personales; así como, un proceso de verificación de la eficacia de las medidas para garantizar la seguridad de la operación de tratamiento.

En el campo de las redes sociales es especialmente relevante como medida técnica apropiada la limitación de acceso a las cuentas personales mediante sistemas de inicio de sesión que consten de varios niveles. Por ejemplo, Facebook proporciona una herramienta que permite a los usuarios agregar un nivel adicional de seguridad de los datos mediante la autentificación en dos niveles.

2.1.7.7.Principio de transparencia

Este principio constituye otra de las novedades que pretender introducir el proyecto del nuevo Reglamento de la Ley. Pese a su importancia en el tratamiento de datos personales, sobre todo de los menores inmersos en las redes sociales, la normativa actual no lo contempla. Según lo establecido en el citado proyecto, quien resulte responsable del tratamiento de datos personales debe informar el tratamiento de datos personales de manera clara, fácil de entender y accesible al titular de los datos personales.

Siendo así, la información relativa al tratamiento de datos personales que ponga en conocimiento el responsable del tratamiento de datos personales debe cumplir con las siguientes exigencias:

i.) Ser clara. – Esto alude a que la información pueda ser entendida de forma evidente, sin ambigüedades.

ii.) Fácil de entender. – La información debe ser comprensible para las personas a quienes se dirige.

iii.) Accesible. – Relativo a que la información se encuentre al alcance de los titulares a través de procedimientos sencillos.

Este artículo prevé que los titulares de datos personales tengan las herramientas necesarias para emitir o en su caso, restringir o revocar el consentimiento en cualquier momento. En general, es condición necesaria para que el titular de datos personales pueda emitir una decisión debidamente fundamentada, y en ese sentido, supone también la obligación del responsable del tratamiento de proporcionar información respecto a los riesgos, el ejercicio de los derechos y los medios previstos para ello, así como, la finalidad, los destinatarios, la transferencia de datos personales y las consecuencias de proporcionarlos.

Este principio debe informar toda actividad de tratamiento, para lo cual se puede adoptar un modelo de información por capas o niveles. Según la Agencia Española de Protección de Datos et al. (2017b) este modelo consiste en (i) una información básica de un primer nivel en que se presenta la información de forma resumida en el mismo medio y (ii) una información adicional de segundo nivel en que se remite información de los detalles de la información resumida e información adicional.

Dado que los menores merecen una protección específica y reforzada, “la transparencia y la información previa se convierten en los pilares de la validez del consentimiento del interesado”. (García, 2020, p.191). Así también se encuentra establecido en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos al señalar que debe tenerse

especial atención cuando la información va dirigida a los menores pues supone la obligación de emplear un lenguaje de fácil comprensión para ellos. (art. 16.3.).

2.1.7.8.Principio de responsabilidad proactiva

La aplicación de este principio importa una continua revisión y prevención de los riesgos y efectos negativos de las actividades de tratamiento que realice una determinada entidad. Es decir, requiere la evaluación de las consecuencias del riesgo de tratamiento y la posterior implantación y utilización de medidas adecuadas para contrarrestarlo y poder demostrar que el tratamiento de datos personales que se realiza es el adecuado, atendiendo a su naturaleza, ámbito, contexto y finalidad. Sin duda, el fin es que se implementen los procedimientos adecuados para prevenir un impacto negativo en los derechos de las personas.

La Agencia Española de Protección de Datos Personales et al. (2017a) realiza una explicación didáctica del contenido de este principio indicando que en virtud de este principio las organizaciones deben analizar qué datos tratan, con qué finalidades y qué tipo de operaciones de tratamiento emprenden; luego, con dicho conocimiento deben determinar la forma en que se aplicarán las medidas adecuadas para cumplir la normativa, asegurándose de que dichas medidas puedan demostrarse ante los interesados.

Por su lado, Aparicio (2019) sostiene que son expresiones concretas de la aplicación de este principio las figuras denominadas «privacidad desde el diseño» y «privacidad por defecto»; que implican, respectivamente, tomar en consideración la protección de datos personales desde el inicio de un proyecto tecnológico y restringir por defecto la publicidad de los datos de los usuarios de un servicio, siendo estos últimos los encargados de establecer qué datos pueden o no ser públicos. A modo de ejemplo, este autor refiere que la aplicación de la privacidad por defecto en el campo de las redes sociales consistirá en la obligación del prestador del servicio de brindar a la cuenta nueva un nivel alto de privacidad, en donde por defecto solo sean públicos los menores datos posibles. En consecuencia, en virtud de la

aplicación de este principio las redes sociales en línea deben establecer configuraciones estrictas de privacidad y permitir que sea el usuario quien opte por reducir los niveles de seguridad, especialmente si trata de menores de edad.

En síntesis, se trata de una obligación a cargo del responsable del tratamiento consistente en la rendición de cuentas sobre cómo se efectúa el tratamiento, probando que se ha adoptado una política de protección de datos, por ejemplo, estableciendo códigos de conductas y mecanismos de revisión periódicos (Barrón, 2019).

2.1.8.Derechos del titular de datos personales

El derecho de protección de datos personales engloba un haz de facultades destinadas a que el titular de los datos personales ejerza el control del tratamiento de sus datos personales realizado por terceros, siendo estas las herramientas esenciales para hacer efectivo los intereses jurídicos que componen el derecho a la protección de datos personales. Se considera que forman parte de su contenido esencial (Zamudio, 2022). La regulación de estos derechos en favor de los titulares de datos expresa que el ejercicio del derecho no se refiere a la mera protección de los datos, sino al control efectivo sobre su uso o destino.

El proveedor de servicios de la red social en su calidad de responsable del tratamiento de datos personales está obligado a proporcionar un medio adecuado para ejercer estos derechos y responder a cada uno de los requerimientos que sus usuarios realicen en su ejercicio; y, para el caso específico de los menores, estos derechos se concretarán mediante sus representantes legales conforme se encuentra establecido en el artículo 49° del Reglamento.

Cabe señalar que el ejercicio de estos derechos no se encuentra limitado a los usuarios de la plataforma, sino que corresponde a cualquier persona cuyos datos se traten en estos espacios digitales.

2.1.8.1.Derecho de información

Como regla ineludible, el titular de datos personales tiene derecho a que el responsable del tratamiento de datos personales le informe previamente a su recopilación, sobre la finalidad para la cual sus datos serán tratados, los destinatarios de los datos personales, la existencia de un banco de datos personales así como la identidad y domicilio de su titular, el carácter obligatorio o facultativo de sus respuestas, la transferencia de los datos personales, los efectos de proporcionar sus datos personales y de su negativa de hacerlo, el plazo de conservación de los datos, la opción de ejercer los derechos que la ley concede y los medios previstos para ello.

A diferencia de los demás derechos, este no requiere que el titular presente una solicitud concreta, sino que el responsable del tratamiento debe cumplirla de manera proactiva. Así lo ha expresado la Autoridad Nacional de Protección de Datos Personales al señalar que este derecho requiere de una acción del responsable del tratamiento de datos personales que permita el ejercicio del derecho, antes de la recopilación (Resolución Directoral N° 1114-2022-JUS/DGTAIPD-DPDP, de fecha 17 de marzo del 2022).

En virtud a la naturaleza de los servicios y contenidos brindados por las redes sociales, la práctica más extendida consiste en brindar dicha información en las Políticas de Privacidad, por consiguiente, el tratamiento de datos personales solo será lícito si el usuario ha brindado su consentimiento expreso en el que acepte los términos de la política de privacidad que contenga la información que establece el artículo 18° de la Ley, el cual reconoce este medio de información, pero además dispone que estas deben ser «fácilmente accesibles e identificables».

Sobre esta última cuestión, Pérez (2018) sostiene que generalmente las redes sociales no destacan lo suficiente estas políticas en las páginas de inicio o fase de registro, por lo que son pocos los usuarios que las leen, lo cual conlleva a que realmente no exista un consentimiento informado.

Dado que no brindar la información pertinente previa a la recopilación de los datos impide el ejercicio real del derecho a la información y los otros derechos señalados en la Ley, su incumplimiento por parte del responsable del tratamiento conlleva la configuración de una infracción grave de acuerdo a lo establecido en el literal a) del numeral 2 del artículo 132° del Reglamento.

2.1.8.2.Derecho de acceso

Este derecho consiste en la obtención por parte del titular de los datos de: i.) la información que sobre sí mismo sea objeto de tratamiento, ii.) la forma en la que los datos fueron recopilados, iii.) las razones que motivaron su recopilación iv.) la entidad o persona que solicitó la recopilación y v) las transferencias realizadas o que se prevén realizar.

Permite verificar la licitud de las actividades del tratamiento que realice un responsable y para ello, dicha información deberá ser proporcionada en un lenguaje accesible al conocimiento medio de la población, es decir, la información debe ser lo suficientemente clara para un usuario de conocimiento medio evitando caer en ambigüedades que provoquen incertidumbre en el solicitante. Asimismo, el responsable se encuentra en la obligación de proporcionar un acceso directo y permanente a los datos, de tal forma que el acceso a esta información deba ser en formato claro, legible e inteligible.

Para Moralejo (2023) el usuario de la red social no necesitaría ejercer este derecho cuando se trata de datos que hubiera facilitado voluntariamente en la plataforma bastando que acceda a su perfil; en cambio, sí podría tener interés en conocer los datos personales que hubieran sido objeto de colecta secundaria por la plataforma de la red social como por ejemplo su historial de navegación o aquellos datos cuyo tratamiento no esté basado en su consentimiento.

Este derecho se constituye en un pilar fundamental para el ejercicio de los demás contenidos en la Ley, en tanto el titular de los datos puede ejercer, por ejemplo, el derecho a la

actualización, cuando previamente haya conocido los datos personales que se encuentren en posesión de terceros.

2.1.8.3.Derecho de actualización, inclusión, rectificación y supresión

La rectificación está referida a la facultad de solicitar al responsable del tratamiento la corrección de sus datos personales cuando estos no se ajusten a la verdad. Por otro lado, se solicitará la actualización cuando los datos personales no se correspondan con la realidad a la fecha del ejercicio del derecho, que, si bien en algún momento fueron reales, estos ya no se encuentran vigentes. El derecho de inclusión se refiere a la facultad del titular de datos personales de solicitar que ciertos datos sean incluidos en un banco de datos o que se incorpore al tratamiento de sus datos cierta información faltante que hace que los datos sean incompletos, omitidos o eliminados en función a su relevancia para dicho tratamiento. Finalmente, el derecho de supresión supone la facultad del interesado de solicitar la eliminación de sus datos bajo ciertas circunstancias que se detallarán más adelante.

En el ámbito de las redes sociales, las citadas facultades normalmente pueden hacerse efectivas por el propio usuario quien a través de la opción de ajustes puede realizar modificaciones a sus datos personales; sin embargo, cuando se trate de datos personales que figuran en los perfiles de otros usuarios resulta necesario realizar la solicitud pertinente.

Particular atención merece el derecho de supresión o cancelación, pues la norma establece que este se puede ejercer solo cuando se presenten cualquiera de las siguientes circunstancias: i) Los datos ya no sean necesarios para los fines para los cuales fueron recogidos, ii). Vencimiento del plazo establecido para su tratamiento, iii). Revocación del consentimiento para el tratamiento, iv.) Tratamientos de datos al margen de la Ley y el Reglamento.

En el ámbito de las redes sociales online, los datos dejan de ser necesarios para los fines para los que fueron recogidos cuando, por ejemplo, un usuario de una red social solicita la baja

del servicio o cuando haya inactividad del usuario por un determinado plazo conforme lo ha establecido el Grupo de Trabajo del Artículo 29 (2009) en su Dictamen 5/2009 sobre las redes sociales en línea al señalar que constituye una obligación de los servicios de redes sociales establecer plazos máximos de conservación de los datos de los usuarios inactivos, así como suprimir las cuentas abandonadas.

La revocación del consentimiento se extiende a la posibilidad de solicitar la supresión de datos cuando un determinado usuario realice tratamiento de datos personales de otros usuarios fuera del ámbito de las excepciones domésticas. Por ejemplo, se puede solicitar la supresión de una foto personal que aparezca en el perfil de un usuario con el que ya no se tiene alguna vinculación saludable y la foto haya sido compartido públicamente.

En la regulación europea el derecho de supresión ha sido ampliado al supuesto en el cual los datos hayan sido obtenidos en relación con la oferta de servicios de la sociedad de la información, específicamente cuando se trata de un tratamiento de datos en el marco de una oferta directa de servicios de la sociedad de la información dirigida a niños. De esta forma se garantiza que se pueda solicitar la supresión de aquellos datos concernientes a menores que hayan sido obtenidos en el ámbito de los servicios digitales como los navegadores web o las redes sociales en línea.

Aunado a ello, el Reglamento (UE) 2016/679 ampara la supresión de datos si el interesado dio su consentimiento siendo niño, sin ser plenamente consciente de los riesgos que implica el tratamiento y más tarde quiere suprimir tales datos personales, especialmente en internet, incluso cuando haya dejado de ser menor de edad. Estas previsiones son importantes por cuanto reconocen que los usuarios menores de edad son especialmente vulnerables en los entornos digitales en los cuales se suelen recopilar sus datos personales cuyo tratamiento podría resultar perjudicial para su desarrollo futuro.

Suele considerarse al derecho de supresión como un «derecho al olvido». En nuestro país, se han presentado diversos pronunciamientos de la Autoridad Nacional de Protección de Datos Personales en los que se ha tratado a este último como una manifestación del derecho de supresión entendido como aquel que puede ejercerse frente a los motores de búsqueda a fin de evitar la hipervisibilización de la información de la persona buscando la limitación respecto de su información al buscarla por su nombre en los motores de búsqueda. Se sostiene además que el denominado derecho al olvido tiene como factor decisivo el paso del tiempo (Resolución Directoral N° 2377-2018-JUS/DGTAIPD-DPDP, del 24 de setiembre de 2018).

En el Manual de Protección de Datos Personales elaborado por la Defensoría del Pueblo (2019) se sostiene que el derecho al olvido es "una vertiente del derecho a la protección de datos personales, que busca la supresión de datos contenidos en diversas fuentes de información". (p.19).

Así también, Merino (2023) sostiene que el derecho al olvido permite la eliminación o cancelación de datos de una persona que ya no sean necesarios para el fin que fueron tratados, que sean negativos sobre su pasado o que impliquen un agravio.

El Tribunal Constitucional del Perú considera que el derecho al olvido tiene por finalidad evitar que, por efecto del tiempo, se lesione el ejercicio de derechos fundamentales esenciales para desarrollar una vida digna como consecuencia de la exhibición o difusión de información de carácter personal a través de sistemas informáticos (Sentencia del Tribunal Constitucional de fecha 22 de agosto de 2022, Exp. N.° 02839-2021-PHD/TC).

Los alcances de este derecho en el ámbito digital han sido atendidos en la normativa española a través de la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el mismo que en su artículo 94° regula el ejercicio del derecho al olvido en los servicios de redes sociales y servicios equivalentes, estableciendo que cuando se trate de datos que el usuario hubiese facilitado para su publicación

por las redes sociales se podrá solicitar su supresión sin expresión de causa más que la simple solicitud; por el contrario, cuando se trate de datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por las redes sociales, la solicitud de supresión solo procederá si dichos datos fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieran devenido como tales por el transcurso del tiempo. En igual sentido, la supresión será atendida cuando las circunstancias personales que invoque el afectado evidenciase la prevalencia de sus derechos sobre el mantenimiento de los datos. No obstante, cuando se trate de datos facilitados por el usuario o por terceros, durante su minoría de edad, el responsable del tratamiento deberá proceder a su supresión por su simple solicitud, no siendo necesarios las dos circunstancias antes mencionadas. Importante previsión en relación a la situación concreta de los menores.

Lo anterior evidencia un claro y completo derecho a "ser olvidado" en la Red como consecuencia de una situación en la que, si bien los datos son exactos, estos pueden devenir con el tiempo en incompatibles con la normativa porque dejaron de ser necesarios para los fines por los cuales se recopilaron o trataron en su momento.

En nuestro ordenamiento jurídico, este derecho encuentra limitaciones a su ejercicio cuando se trata de datos que deban ser conservados por razones históricas, estadísticas o científicas; o en su caso, en las relaciones contractuales entre el responsable y el titular de los datos personales que justifiquen el tratamiento de los mismos.

A manera de reflexión, resulta necesario subrayar que, pese a la garantía del derecho de supresión en las redes sociales, "se plantea la dificultad de que, en este ámbito concreto, pueda conseguirse realmente una desaparición de todos los datos del usuario de la red" (Moralejo, 2023, p.302). Lo anterior se debe principalmente a su naturaleza compleja que permite el almacenamiento de datos por los propios usuarios de la red, de ahí la importancia de

una normativa que prevea una protección eficaz de los menores que interactúan en estos espacios.

2.1.8.4.Derecho de impedir el suministro

Es un derecho a través cual el titular de los datos personales tiene la potestad de decidir que sus datos personales no sean suministrados a terceros, especialmente si su manipulación puede afectar sus derechos fundamentales.

De esta manera, el titular evita el uso irregular de sus datos personales que amenace el ejercicio de sus derechos. El Tribunal Constitucional ha identificado este derecho con el Hábeas Data Cautelar que tiene por objeto "impedir la manipulación o publicación del dato en el marco de un proceso, a fin de asegurar la eficacia del derecho a protegerse" (Sentencia del Tribunal Constitucional, de fecha 29 de agosto de 2013, Exp. N°04387-2011-PHD/TC, F.J. 6). Por lo que se entiende que su marco de aplicación está destinado a la protección de ciertos intereses que pudieran verse afectados como consecuencia del suministro de datos personales a terceros.

2.1.8.5.Derecho de oposición

Este derecho está referido al poder del titular de datos personales de oponerse, en cualquier momento, al tratamiento de sus datos personales en dos supuestos:

i). Cuando no se haya prestado su consentimiento para su recopilación por haber sido tomados de fuente de acceso al público.

ii). Aun cuando se haya prestado el consentimiento, si se acredita la existencia de motivos fundados y legítimos relativos a su concreta situación personal.

Se trata de un derecho consistente en la expresión de negativa a la continuación de un determinado tratamiento. En el primer supuesto se considerarán fuentes accesibles al público las establecidas en el artículo 17° del Reglamento, siendo definidas como bancos de datos

personales que pueden ser consultados por cualquier persona. Por otra parte, cuando el titular de datos haya otorgado su consentimiento se requiere que el interesado en impedir que sus datos continúen recibiendo un determinado tratamiento logre acreditar razones que sean fundadas y legítimas; y que, además, estas razones se relacionen con la situación particular del interesado.

La Autoridad Nacional de Protección de Datos Personales explica el derecho de oposición sosteniendo que para que proceda es necesario que concurra: a) La existencia de un motivo legítimo y fundado, b) El motivo se refiera a una concreta situación personal; c) El motivo justifique el derecho de oposición (Resolución Directoral N°925-2018-JUS/DGTAIPD-DPDP, del 02 de mayo del 2018 y la Resolución Directoral N° 2377 -2018-JUS/DGTAIPD-DPDP, del 24 de setiembre de 2018).

Ejercida la solicitud de oposición, la norma impone la carga de la prueba en el responsable del tratamiento, quien deberá decidir y fundamentar si la oposición resulta justificada o no.

Por cuanto su regulación actual es limitada en comparación con la legislación comparada, el proyecto del nuevo Reglamento amplía los alcances de este derecho al establecer la facultad de ejercerlo, en todo momento, cuando además los datos personales sean tratados para fines de prospección comercial y publicidad (art. 79°, inciso 4).

2.1.9.Tratamiento de datos personales de menores de edad en las redes sociales

Cuando se trate de menores de edad, además de regir las disposiciones antes desarrolladas se deben tomar en cuenta otras disposiciones específicas determinadas por la especial situación del menor. Aunque la Ley no establece un apartado concreto que regule de manera exhaustiva la cuestión del tratamiento de datos personales de los menores, en el capítulo titulado *"Tratamientos especiales de datos personales"* contenido en el Reglamento establece importantes alcances.

Nuestra legislación ha optado por el criterio cronológico al regular el consentimiento de los menores para el tratamiento de datos personales, ya que se considera que el mayor de 14 años tiene capacidad para consentir por sí mismo el tratamiento de sus datos personales, mientras que el menor de 14 requerirá que el consentimiento sea prestado por sus representantes legales. Esta previsión tiene como objetivo proporcionar seguridad jurídica al tratamiento de datos personales. Además del criterio cronológico, la norma señala una condición para que el mayor de 14 años pueda consentir de manera válida, esto es, la necesidad de que la información que se brinde al menor se exprese en un lenguaje sencillo adaptado a su nivel de compresión.

En el proyecto del nuevo Reglamento se establecen los mismos requisitos que deben cumplirse; además de ello, se ha previsto un apartado destinado a regular el tratamiento de sus datos en internet en el cual se regula la obligación del responsable del tratamiento de garantizar el interés superior del niño y sus derechos fundamentales en los espacios digitales.

En cuanto a la prueba del consentimiento, consideramos que las medidas aún siguen siendo muy laxas ya que no se establece la obligación del responsable del tratamiento de verificar de modo efectivo la edad y la autenticidad del consentimiento prestado por los padres o tutores, como se encuentra regulado, por ejemplo, en el ordenamiento jurídico español a través del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 diciembre, de protección de datos de carácter personal.

Al respecto, Toral (2020) sostiene que es necesario avanzar en el proceso de verificación de la edad propiciando mecanismos que garanticen la comprobación efectiva de la edad del menor así como la autenticidad del consentimiento prestado por sus representantes legales, lo que supone la implementación de sistemas electrónicos de certificación de edad y

control parental como podría ser exigir el DNI, tarjetas de identificación electrónica, firma electrónica de los padres u otros mecanismos análogos.

Como ya se explicó, resulta especialmente relevante el deber de información y transparencia previstos en la Ley cuando se trata de menores de edad, puesto que se dirige a una persona en pleno desarrollado, lo que justifica que la información debe ser adecuada a su edad.

Cabe precisar que la normativa establece que el consentimiento prestado por el menor mayor de 14 años únicamente será válido para el tratamiento de datos que le conciernen, no pudiendo ampliarse a la información relativa a su grupo familiar.

2.1.10.El consentimiento del menor para el tratamiento de datos personales como contraprestación por el suministro de servicios digitales

En el análisis de la relación entre las redes sociales y la protección de datos personales es preciso expresar algunas ideas respecto a la naturaleza del acceso de las personas a las redes sociales. Como primer punto, se debe reconocer que ese acceso – el uso del servicio- se presenta a través de la celebración de un contrato.

La normativa de la comunidad europea regula diversos aspectos de estos contratos a través de la Directiva 2019/770, del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales. El objeto de este instrumento jurídico comunitario consiste en armonizar aspectos relativos a los citados contratos celebrados entre empresarios y consumidores, partiendo de la base de un alto nivel de protección de estos últimos con la finalidad de consolidar un mercado único digital (Considerando 3 de la Directiva 2019/770).

Según el artículo 2° de la mencionada normativa, los servicios digitales que puede ser objeto de estos contratos son de dos tipos: a.) Un servicio que permite crear, tratar, almacenar o consultar datos en formato digital, por ejemplo, los servicios de *cloud computing* ofrecidos

por One Drive, Dropbox; o, b) Un servicio que permite compartir datos en formato digital cargados o creados por el consumidor u otros usuarios de ese servicio, o interactuar de cualquier otra forma con dichos datos; como pueden ser los servicios de redes sociales prestados por Instagram, TikTok, Facebook, entre otros.

Las redes sociales son servicios gestionadas por grandes empresas tecnológicas en donde el acceso al servicio está sujeto a la celebración de un contrato que posee carácter oneroso, por cuanto dichas empresas suministran o se comprometen a suministrar contenidos o servicios digitales al consumidor y este último paga o se compromete a pagar un precio. Al respecto, la citada Directiva entiende que el precio puede consistir en que el consumidor facilite o se comprometa a facilitar datos personales, salvo cuando los datos personales facilitados por el consumidor sean tratados exclusivamente por el empresario con el fin de suministrar los contenidos o servicios digitales o para permitir que el empresario cumpla los requisitos legales a los que se encuentra obligado, y el empresario no trate esos datos para otros fines (art. 3°). De esta manera, la normativa europea advierte que el acceso a las redes sociales constituye un modelo de negocio que podría configurar un verdadero contrato a través del cual el consumidor (titular de los datos personales) facilita o se compromete a facilitar datos de carácter personal (precio) a cambio del suministro de contenidos o servicios digitales por parte del empresario titular de la red social (Considerando 24 y 25).

Otro aspecto interesante de la normativa especial antes mencionada es relativo a la aplicación del Reglamento (UE) 2016/679 a los datos personales tratados en virtud de este contrato; pues, se señala que las normas sobre la protección de datos personales se aplicarán a cualquier dato personal tratado en virtud de los contratos contemplados en el apartado 1 de la Directiva. (art.3.8). Siendo así, el tratamiento de dichos datos debe regirse por principios y derechos aplicables a la protección de datos personales.

Asimismo, se prevé que el derecho del consumidor de retirar su consentimiento para el tratamiento de sus datos personales supondrá que el gestor de la red social quede facultado para resolver el contrato, toda vez que, el modelo de negocio de estos contratos se basa principalmente en el tratamiento de datos personales.

La doctrina también se ha pronunciado a favor de considerar el acceso a las redes sociales como un verdadero contrato. Así, por ejemplo, Moralejo (2023) reconoce que se trata de un contrato de suministro de servicios de redes sociales en donde el usuario permite la colecta de sus datos con diversos fines.

De la misma forma, Sánchez y Romero (2021) sostienen que el acceso a las redes sociales supone el establecimiento de una relación jurídica contractual entre el usuario y el gestor de la red social, la misma que puede calificarse como contrato de prestación de servicios en la cual la prestación del usuario consistirá en una licencia que otorga respecto a la información y contenido que facilita. Asimismo, Ayllón (2022) refiriéndose a la red social TikTok sostiene que se trata de un contrato en el cual la contraprestación consiste en datos de carácter personal a cambio de servicios que la plataforma ofrece.

Sin duda, el esquema normativo y doctrinal desarrollado denota un gran avance a efectos de regular la actuación de las empresas cuyos modelos de negocios se basan fundamentalmente en el tratamiento de datos personales, como pueden ser las redes sociales digitales. Lamentablemente, en nuestra región aún no se ha regulado por completo este esquema de tratamiento dejando así un vacío importante en la protección de datos personales que constituyen contraprestación del consumidor del servicio.

Es más, a diferencia de la normativa española en la que se establece la capacidad legal de los mayores de catorce años para celebrar contratos relativos a servicios ordinarios de la vida corriente propios de su edad con arreglo a los usos sociales, de forma que el consentimiento contractual del menor para acceder a las redes sociales resultaría

completamente válido en virtud a la citada disposición; en nuestro país, con las modificatorias introducidas al Código Civil por el Decreto Legislativo N° 1384, de fecha 04 de setiembre de 2018, se eliminó una previsión normativa similar que reconocía la plena de validez de los contratos celebrados por los menores con discernimiento para la realización de actividades relacionados a sus necesidades ordinarias (antiguo artículo 1358° del Código Civil).

Por el contrario, la interpretación de la normativa vigente relativa a esta cuestión entiende que se presenta la anulabilidad de los contratos celebrados por los mayores de dieciséis y menores de dieciocho años (artículo 221° del Código Civil) y la nulidad de los contratos celebrados por los menores de dieciséis años (artículo V del título Preliminar, 43°, 219° y 140° del código Civil). Así lo ha expresado el reconocido civilista Chipana (2019) para quien desde la modificación que sufrió el Código Civil a partir del Decreto Legislativo N° 1384 los contratos celebrados por menores de dieciséis años son nulos, pues se ha derogado el artículo 1358° que los salvaba de esa nulidad.

De lo anterior se desprende que en el ordenamiento jurídico peruano no hay claridad respecto a si los menores de dieciséis años cuentan con capacidad legal para celebrar contratos cuyo objeto sea el suministro de servicios o contenidos como puede ser el acceso a redes sociales, por lo que permitir que menores de edad accedan a estos servicios y presten sus datos personales resulta cuestionable.

2.1.11.La relación entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales de los menores de edad

Es innegable que el acceso de los menores a los servicios de redes sociales es cada vez más frecuente. En estas plataformas digitales los usuarios menores de edad suelen prestar sus datos personales tales como sus nombres y fechas de nacimiento, al momento de registrarse; asimismo, durante el uso del servicio, suben a sus perfiles fotos y videos de ellos o de los integrantes de su círculo familiar y amical; luego, es habitual ver en sus perfiles información

respecto a sus gustos, aficiones y actividades. Siendo estos solo algunos datos que se suele visualizar en el entorno de las redes sociales digitales, pues como se ha podido desarrollar precedentemente las plataformas de redes sociales como Facebook y TikTok recopilan muchos más datos que los mencionados.

De esta manera, el uso de las redes sociales por parte de los menores implica reconocer en ellas diversos tratamientos de datos personales. Moralejo (2023) explica dicho tratamiento sosteniendo que se produce una *colecta primaria* de datos personales cuando el usuario los facilita activamente al titular de la plataforma que gestiona la red social en el momento de registrarse o durante el uso del servicio; y, existe una c*olecta secundaria* cuando los datos personales son recogidos de manera indirecta por la propia plataforma o terceras empresas que colaboran con ella, a través de herramientas tecnológicas que les permiten recopilar información sobre el uso de los productos, acciones que el usuario lleva a cabo, las personas con las que interactúa, contenido que visualiza, entre otros. Aunado a la colecta primaria y secundaria, la citada autora manifiesta que el tratamiento de datos puede darse también cuando terceros (otros usuarios) incluyen nuestros datos personales en sus perfiles de redes sociales.

En la actualidad, la excesiva recopilación de los datos personales y el modo en que estos son tratados por parte de los gestores de las plataformas de redes sociales es un tema que forma parte del debate jurídico, por cuanto se suele argumentar que estas actividades colisionan con diversos principios de la normativa de protección de datos personales, situación que se agrava cuando se trata de datos personales que conciernen a menores de edad.

La principal preocupación se deriva de la forma de obtención del consentimiento de los usuarios. Las redes sociales como Facebook o TikTok recaban en bloque todos los consentimientos necesarios mediante una única fórmula global consistente en dar clik a un botón que señala haber leído las Políticas de Privacidad y aceptarlas. Respecto a esta práctica, se sostiene que no es una fórmula correcta para la recopilación de datos personales de los

menores porque no facilita la comprensión de los alcances de la autorización que el usuario está realizando; más bien, lo que propicia es la aceptación de la cesión de datos sin la lectura de las cláusulas del contrato (Barrón, 2019).

Aunado a ello, respecto a la naturaleza de las Políticas de Privacidad se sostiene que se caracterizan por ser documentos muy técnicos y poco explícitos que no garantizan un consentimiento verdaderamente libre e informado.

Por otro lado, se cuestiona también la falta de incorporación de herramientas de comprobación de la edad pues resulta fácil evidenciar que menores que no tienen la edad permitida para acceder a las plataformas suelen estar integrados en las redes sociales. Así, Toral (2020) enfatiza en que los mecanismos técnicos de verificación de la edad en las redes sociales no son realmente eficaces.

Respecto a estos aspectos, Ayllón (2022) refiriéndose a la red social TikTok sostiene que el consentimiento prestado por los menores de edad para el tratamiento de sus datos personales es contrario a la ley, al considerar que la plataforma permite registrarse como usuario por sí solo al menor de 13 años cuando la normativa establece en 14 años la edad mínima para brindar un consentimiento válido; además, considera que el consentimiento brindado por estos últimos para el tratamiento de sus datos no es inequívoco porque cuando se registra no se tiene que hacer una acción positiva concreta para autorizar el tratamiento, de igual forma, el consentimiento tampoco es específico para cada tratamiento de datos personales que hace la plataforma.

Los mecanismos que estas plataformas incorporan en sus sistemas a fin de perfilar a sus usuarios y así ofrecerles servicios y productos personalizados también es un aspecto que ha recibido críticas por parte de la doctrina. La personalización de los servicios es un elemento especialmente relevante en las redes sociales que se encuentra basada en la recopilación de

datos personales para ajustar los servicios a las preferencias, necesidades y capacidades de los usuarios y así incrementar sus beneficios.

Este tratamiento de datos es explicado por Donoso y Reuser (2021) quienes afirman que las redes sociales asocian la información que los usuarios suben a la red vinculándolos a los datos que proporcionaron ellos al momento de registrarse o terceros que forman parte de su interacción social a través de la propia red, todo lo cual deriva en la construcción de un perfil del usuario que es utilizado para beneficiarse económicamente.

Los datos personales nutren los sistemas de personalización que implementan los gestores de redes sociales para poder sostener su actividad económica, por lo que estos deberían respetar los principios establecidos para el tratamiento de datos personales; sin embargo, ha sido cuestionado la falta de transparencia de los algoritmos empleados por las plataformas de redes sociales ya que estas no dicen nada respecto a los datos que emplea y los factores que determinan un resultado.

Respecto al uso de estos sistemas de perfilado, Piñar (2020) afirma que son prácticas comerciales que integran a los usuarios en determinados estamentos a partir del tratamiento de una pluralidad de datos, lo cual trae como resultado que el ciudadano se encuentre integrado, sin saberlo, en grupos que desconoce, quedando este último sometido al poder de las plataformas digitales capaces de condicionar su conducta de manera imperceptible. Estas actividades resultan especialmente riesgosas para los menores de edad pues no todos cuentan con las mismas herramientas para poder asimilar de manera cautelosa los contenidos que se encuentran en las redes sociales.

Piñar (2020) advierte que los algoritmos pueden configurar la identidad de la persona, dando como resultado una identidad controlada y vigilada; esto es, los algoritmos al perfilar a las personas al mismo tiempo limitan el marco de su desarrollo personal, cercenando la diversificación de la personalidad y por tanto su propia identidad.

En general, refiriéndose a los diseños de las redes sociales digitales Moralejo (2023) considera que, en virtud del principio de responsabilidad proactiva los gestores de la plataforma de la red social deberían establecer parámetros de privacidad por defecto respetuosos del derecho a la intimidad de sus usuarios, también deberían establecer por defecto la no indexación de los perfiles de los usuarios y en general, impedir el acceso indebido a los perfiles por personas que estén fuera de su círculo de amigos; sin embargo, sucede que estas pautas no son cumplidas por las redes sociales que, por defecto, establecen parámetros de confidencialidad poco respetuosos, en los que, salvo que se indique otra cosa, el perfil recientemente creado será accesible por todos los miembros de la red social o incluso por terceros ajenos, ya que muchas de ellas permiten que los motores de búsqueda indexen sus contenidos cuando se trate de cuentas abiertas e incluso con cuentas cerradas cualquier internauta podría visualizar la foto de perfil de un usuario de una red social.

A partir de lo desarrollado hasta este punto, es posible sostener que las plataformas de redes sociales aún no han logrado alcanzar estándares respetuosos de la normativa de protección de datos personales, llegándoseles incluso a calificar como sistemas inseguros para los menores de edad, ya sea por los problemas relativos a la obtención de un consentimiento válido, la ausencia de sistemas de verificación de edad eficaces o el uso abusivo de sistemas de perfilado.

Todo lo anterior resulta agravado cuando el menor de edad realiza un uso inadecuado o deficiente de las redes sociales consistente en la sobreexposición de su información personal, por lo que el acceso a las redes sociales por los menores de edad se convierte en una actividad que puede asociarse con la afectación del derecho a la protección de sus datos personales pues en la mayoría de las situaciones la actividad que se realiza a través de la red social trasciende el ámbito personal y familiar.

Lo anterior toma como fundamento lo manifestado por Castillejos (2021) quien sostiene que “la forma en que se emplee la tecnología determinará el efecto que pueda provocar en el usuario” (p.10). Asimismo, Sánchez (2024) enfatiza en que el derecho a la protección de datos personales está siendo afectada por la identidad digital del usuario, lo que termina influyendo en la forma en la que sus datos están siendo utilizados. En esta investigación se considera que el uso de redes sociales puede determinar la afectación del derecho a la protección de datos personales de los menores de edad.

Con relación a los menores, podemos afirmar que el uso de las redes sociales supone una constante exposición pública de su información personal que facilita la vulneración del derecho a la protección de sus datos personales atendiendo a su inherente vulnerabilidad. En efecto, las redes sociales no solo representan una oportunidad de cambio, sino también un espacio en el que se pueden presentar intromisiones ilegítimas en la facultad de control de sus datos personales.

Es innegable que al reconocimiento de los adolescentes como nativos digitales se une la consideración de estos como un colectivo especialmente vulnerable frente a los riesgos que se pueden presentar en los entornos digitales. En palabras de Toral (2020) dicha consideración se debe a que los menores no siempre cuentan con la suficiente capacidad de discernimiento para evaluar las consecuencias de sus actos, y, además, los menores son quienes de manera más intensa hacen uso de las redes sociales.

Efectivamente, los menores de edad al encontrarse en proceso de desarrollo, generalmente no cuentan con herramientas que les permitan conocer los alcances de las actividades que realizan en el ámbito de las redes sociales, es más, ignoran la importancia de los aspectos relacionados a la protección de sus datos personales por lo que muchas veces terminan cediéndolos sin reparo. Luego, sus datos de carácter personal son empleados por diversos actores en función a sus propios fines, los mismos que pueden ser de contenido ilícito.

En consecuencia, la manera en que ellos hacen uso de estas plataformas va a determinar la salvaguardia de sus datos personales.

En consonancia con ello, Ayllón (2022) sostiene que:

> La forma en la que los menores se desenvuelven en internet y, por ende, en las redes sociales, determina una mayor facilidad en lo que se refiere a la vulneración de algunos de sus Derechos, como sería el de la protección de datos de carácter personal, su honor, intimidad o propia imagen. (pp. 582-583)

De igual forma, Priego (2022) advierte el contexto de vulnerabilidad de los menores que se hacen uso de las redes sociales al señalar que estas "hacen a las personas más vulnerables y aumentan la posibilidad de lesión de su honor, intimidad e imagen, a la vez que favorecen un inapropiado uso de sus datos personales" (p.122).

Esta relación entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales se explica fundamentalmente por la exposición elevada de los datos personales. García (2020) sostiene que los menores suelen desconocer los riesgos a los que se exponen cuando comparten sus datos personales a través de su actividad en línea como las redes sociales. Refiriéndose a la red social TikTok, Castillejos (2021) advierte los problemas de seguridad digital de esta plataforma consistentes en el manejo de los datos personales y la sobreexposición de la vida personal de los usuarios.

Por su parte, Ravetllat y Basoalto (2021) explican la dinámica de la inserción de los menores en estas plataformas indicando que el acceso a las redes sociales sin que los menores de edad tengan un conocimiento suficiente sobre las consecuencias sobre su desarrollo integral implica permitir una serie de relaciones sociales proclives a la creación de espacios reservados de mayor dificultad en cuanto a su control.

De esta forma, la complejidad de las plataformas de redes sociales en cuanto a su configuración requiere que los usuarios que quieran salvaguardar sus datos personales tengan

conocimientos mínimos en asuntos de ciberseguridad o protección de datos personales; sin embargo, se sostiene que la mayoría de los menores carecen de estos elementos o los conocen de manera parcial. Por ello, en cuanto al uso que los menores hacen de las redes sociales, Pérez (2018) reconoce que generalmente los menores ceden sus datos en internet, espacios en los que el consentimiento se recaba mediante avisos legales que se caracterizan por ser muy técnicos y que no constituyen información útil al no entender plenamente su contenido.

Las redes sociales centran su funcionalidad en la generación de grupos de interés en función a los datos personales que los usuarios incluyen en sus perfiles; y por ello, los menores que quieran disfrutar al máximo de estas plataformas suelen narrar acontecimientos importantes de su vida a través de las redes sociales. Si bien es cierto, son los usuarios quienes establecen el nivel de acceso a su perfil optando por permitir el acceso a sus amigos, a los amigos de sus amigos, a toda la red social o incluso fuera de ella permitiendo que su perfil sea indexado por motores de búsqueda; sin embargo, a lo que se debería apuntar en las redes sociales es que cuando se trate de menores de edad el acceso a su perfil sea configurado por defecto a un espacio realmente restringido.

Las redes sociales TikTok y Facebook permiten el tratamiento de datos personales de otras personas sin recabar el consentimiento de su titular, lo cual puede ser razonable y admitido socialmente dentro un círculo doméstico o restringido al ámbito familiar (tratamiento con fines domésticos); no obstante, esta situación se vuelve compleja cuando los datos son tratados fuera del ámbito de personal o doméstico y el usuario se convierte en un responsable del tratamiento que está obligado a cumplir con el principio de consentimiento o en su defecto, estar amparado por alguna de las excepciones al consentimiento. No obstante, basta navegar unos minutos por la red para constatar que la mayor parte de los usuarios que se convierten en responsables del tratamiento no cumplen con la normativa de protección de datos y esto es realmente peligroso cuando hablamos de datos personales de menores de edad.

En general, se afirma que la realidad de los menores en la disposición de sus datos a través de las publicaciones que realizan en las redes sociales se aleja del cumplimiento de la normativa, por lo cual, las garantías de protección de derechos son insuficientes (Morillas, 2023).

La diversidad de datos personales que circulan en las redes sociales hace que sea más complicado para ellos el ejercicio real y efectivo del derecho a la protección de datos personales, componente capital en la dignidad de la persona que busca evitar intromisiones ilegítimas en la esfera personal.

Ante ello, resulta relevante lo que mencionó años atrás el especialista Troncoso (2012) al afirmar que un modelo ideal sería que las personas no cedieron datos de otras personas sin su consentimiento y que este debería ser el criterio al cual deben dirigirse los códigos de buenas prácticas.

En efecto, constituye un pilar importante regular la actuación de los gestores de las redes sociales, pero también resulta capital lograr generar mecanismos que coadyuven a los menores a enfrentar los riesgos que conlleva el uso de estas plataformas, este componente también es parte del derecho a la protección de datos personales.

2.1.12.La exposición excesiva de información personal de menores como riesgo para su desarrollo integral

Cuando se habla de redes sociales es inevitable su asociación con diferentes riesgos a los que están expuestos los menores muchas veces como consecuencia de su uso inadecuado que proviene del desconocimiento de asuntos vinculados a la seguridad de la información y la protección de sus datos personales.

El Instituto Nacional de Ciberseguridad (2019) a través de su proyecto Internet Segura for Kids (IS4K) sostiene que los riesgos en las redes sociales a los que los menores se enfrentan se producen en tres situaciones: En primer lugar, cuando los menores las utilizan de manera

inadecuada; luego, cuando acceden a contenidos inapropiados, y finalmente, cuando exponen su información personal. En relación a este último, indica que los menores deben hacer uso de las redes moderando la información que publican para evitar la pérdida de su privacidad, y de ese modo, evitar riesgos asociados a la suplantación de la identidad y el *grooming.*

Asimismo, la entidad antes mencionada sostiene que otro de los riesgos a los que los menores se exponen en las redes sociales y demás servicios online es el acceso indebido a su información por parte de terceros lo que puede derivar en daños a la privacidad, daños a la imagen y reputación online, *ciberbullyng*, *grooming*, extorsión y chantaje (Instituto Nacional de Ciberseguridad, 2020).

En efecto, la presencia de los menores en las redes sociales trae aparejado la exposición de sus datos personales, lo que en sí mismo constituye un riesgo que se vincula con la posibilidad de que esos datos sean empleados por usuarios malintencionados.

Así también lo ha enfatizado el Fondo de las Naciones Unidas para la Infancia (UNICEF, 2017) señalando que las Tecnologías de la Información y Comunicación, incluida en estas las redes sociales "han aumentado las posibilidades del uso indebido y la explotación de la privacidad de los niños, y han cambiado la forma en que los niños consideran su propia información privada" (p.7).

Gil (2013) explica que en la interacción en las redes sociales los menores exponen sus datos personales de tal forma que expanden el ámbito de su propia intimidad con la consecuencia aparejada de incremento del riesgo de conculcación de los derechos a la privacidad y a la protección de datos personales. En el mismo sentido, Farfán (2020) concluyó en su investigación que uno de los riesgos del acceso de los menores a las redes sociales está vinculado al manejo inadecuado de su información personal al no considerar la seguridad de sus datos personales.

Este riesgo fue explicado por Echeburúa y De Corral (2010) quienes afirman que en las redes sociales "se facilita la confusión entre lo íntimo, lo privado y lo público (que puede favorecer el mal uso de información privada por parte de personas desconocidas)". (p.92).

En consonancia con lo anterior, González (2021) advierte que frente a la aparente privacidad de la navegación existe siempre la posibilidad de vernos expuestos públicamente ya que al emplear la red se dejan datos que pueden llegar a ser compartidos públicamente como consecuencia de su protección deficiente.

Como consecuencia de este riesgo de sobreexposición de la información personal se presentan situaciones de discriminación, difamación, suplantación de identidad, chantaje, acoso sexual e incluso pornografía, trata de menores, casos *de cyberbullyng, sexting, grooming online*, entre otros que se caracterizan por su impacto negativo en el desarrollo social, psicológico y emocional del menor.

A modo de ejemplo, Florit (2022) explica que el *grooming* online se alimenta de todo tipo de imágenes y datos colgados en la red del menor del cual el adulto extrae información para su aprovechamiento. Asimismo, en relación al abuso sexual enfatiza en que la información de las menores contenida en fotografías inocentes puede llegar a formar parte de redes de pedofilia.

En síntesis, las redes sociales son espacios en los que la línea divisoria entre lo público y lo privado se difumina, como consecuencia de ello, la información puede ser revelada a un número indefinido de personas, perdiéndose el control de los datos personales.

2.1.13.Mecanismos especiales de protección para la seguridad de los datos personales de los menores

Conforme se ha podido revisar a lo largo del presente trabajo, los menores de edad sufren diversas afectaciones a sus derechos fundamentales que provienen de la sobreexposición

de su información personal en las redes sociales, por ello se requiere tomar las medidas pertinentes para su protección frente a ataques a su integridad física, psíquica y emocional.

Ante ello, debe resaltarse que, por su condición, los menores de edad requieren de una protección especial en situaciones que pueden resultar perjudicados sus derechos fundamentales; además, debe puntualizarse que estos han sido reconocidos como sujetos titulares de derechos cuyo ejercicio está en función de su edad y madurez. Es decir, en cualquier planteamiento respecto a la problemática del impacto de las redes sociales sobre la protección de sus datos personales, debe tomarse en cuenta esta doble consideración: la autonomía progresiva de los menores en el ejercicio de sus derechos y la necesidad de medidas especiales de protección a fin de evitar la afectación de sus derechos.

El interés superior del menor y su consiguiente protección especial se encuentra consagrado en diversos instrumentos internacionales. La Declaración Universal de los Derechos Humanos, proclamada en 1948 como un plan de acción que establece los derechos humanos fundamentales que deben protegerse en todas las regiones reconoció el principio de protección especial del menor al señalar que: *"La maternidad y la infancia tienen derecho a cuidados y asistencia especiales*". (art. 25°). Asimismo, la Declaración de los Derechos del Niño, adoptada en 1959 reconoce como principio la protección especial del niño señalando que "*El niño gozará de una protección especial y dispondrá de oportunidades y servicios, dispensado todo ello por la ley y por otros medios (...)".* (artículo 2°).

De igual forma, el marco internacional de protección de la infancia se reforzó con la adopción de pactos y convenciones como instrumentos jurídicos vinculantes para los Estados. El Pacto Internacional de Derechos Civiles y Políticos que entró en vigor en 1976 reconoce el derecho de todo niño, sin discriminación alguna, a las medidas de protección que su condición de menor requiere, tanto por parte de su familia como de la sociedad y el Estado (véase artículo 24°). Además, la Convención de la Naciones Unidas del 20 de noviembre de 1989, sobre los

Derechos del Niño, documento histórico que incorporó la visión del menor como titular de derechos, suscrito por el Perú en 1990, establece el interés superior del niño como un principio que los Estados deberán tomar en consideración en todas las medidas concernientes a los niños (ver artículo 3° de la Convención).

En el marco interamericano, la Convención Americana de Derechos Humanos (Pacto de San José), adoptada en 1969, reconoce que "*Todo niño tiene derecho a las medidas de protección que su condición de menor requiere por parte de su familia, de la sociedad y del Estado*" (art.19°).

En el ámbito nacional, nuestra Carta Política señala en su artículo 4° que "*la comunidad y el Estado protegen especialmente al niño, al adolescente (...)".* Asimismo, en consonancia con la normativa internacional, el artículo IX del Título Preliminar del Código del Niño y del Adolescente precisa que en toda medida concerniente al niño y al adolescente que adopte el Estado y en toda acción de la sociedad se deberá atender al principio del interés superior del niño y del adolescente y el respeto de sus derechos fundamentales.

De lo anterior se desprende que existe un imperativo dirigido al Estado de llevar a cabo todas las medidas políticas y legislativas necesarias para la realización del interés superior del menor y velar por su atención prioritaria. EL Tribunal Constitucional desarrolla esta idea señalando que:

> El fundamento constitucional de la protección del niño y del adolescente que la Constitución les otorga radica en la especial situación en que ellos se encuentran; es decir, en plena etapa de formación integral en tanto personas. En tal sentido, el Estado, además de proveer las condiciones necesarias para su libre desarrollo, debe también velar por su seguridad y bienestar. (Sentencia del Tribunal Constitucional, Expediente N° 3330-2004-AA/TC, de fecha 11 de julio de 2005, F.J.35).

Ahora bien, para efectos del tema que nos atañe, se debe tomar en consideración lo señalado por el Comité de los Derechos del Niño de las Naciones Unidas (2021) en su observación general núm.25 en la cual se enfatiza el interés superior del menor como una línea guía al determinar las medidas necesarias para garantizar los derechos de los niños en el entorno digital.

De esta manera, considerando que las redes sociales digitales son espacios en los que los menores se encuentran expuestos a diversas afectaciones a sus derechos fundamentales, y en específico, injerencias a su derecho a la protección de sus datos personales, surge la obligación de los Estados de hacer frente a esta problemática asegurando la protección especial de los menores.

Como consecuencia de dicho imperativo, se han presentado diversas iniciativas desde diferentes espacios tanto globales como regionales. A modo de ejemplo, la Unión Europea ha realizado una activa labor en la regulación de esta materia con el fin de hacer frente a los riesgos del entorno digital.

En España se ha logrado expedir un novedoso instrumento jurídico que hace realmente efectiva la protección de los menores. Se trata de la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, en cuyo Título X denominado “Garantía de derechos digitales” se regulan importantes aspectos tales como el derecho a la seguridad digital y el derecho a la educación digital, así como, el régimen de protección de los menores en Internet, la protección de datos de los menores en Internet, el derecho al olvido en búsquedas de Internet y en servicios de redes sociales.

En el artículo 83° de la citada normativa española se prevé el derecho a la educación digital estableciendo la obligación del sistema educativo de garantizar la inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y uso seguro de los medios digitales. Para ello se prevé que las administraciones educativas incluyan en la malla

curricular contenidos de competencia digital y elementos relacionados a situaciones de riesgo producto de la inadecuada utilización de las Tecnologías de la Información y Comunicación. Para reforzar este marco normativo, se encuentra en proyecto una Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. Por otro lado, en el ámbito latinoamericano el artículo 23° de la Ley Orgánica de Protección de Datos Personales de Ecuador contempla el derecho a la educación digital.

En igual sentido, cabe resaltar la importante labor que ha realizado la Agencia Española de Protección de Datos en relación a la adopción de medidas concretas para la protección de los menores en el ciberespacio. Destaca la iniciativa digital denominada «Canal Prioritario» para comunicar la difusión ilícita de contenido sensible cuyo funcionamiento se basa en la puesta a disposición de la población de un sistema que tiene como objetivo dar una respuesta inmediata (menor a 72 horas) a situaciones excepcionalmente delicadas como cuando se trata de la difusión de contenido violento o sexual que pueda afectar los derechos.

En nuestro contexto regional, se ha expedido el "Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes" más conocido como el Memorándum de Montevideo. Se trata de un documento de trabajo elaborado en el marco del Seminario Derechos, Adolescentes y Redes Sociales en Internet llevado a cabo en Montevideo los días 27 y 28 de julio de 2009, el cual contó con la participación de diversos representantes de instituciones públicas y privadas de diferentes países. Este documento realiza algunas recomendaciones destinadas a garantizar la adecuada protección de datos personales de los menores en el ciberespacio. Se enfoca en reforzar el sistema educativo con una clara intención preventiva.

Por otro lado, en el año 2017 la Red Iberoamericana de Protección de Datos aprobó el documento denominado «Estándares de Protección de Datos Personales para los Estados Iberoamericanos», el mismo que busca establecer un conjunto de directrices orientadoras en

materia de protección de datos personales que los Estados Iberoamericanos pueden adoptar y desarrollar en su legislación nacional. En su contenido, en el capítulo referente al tratamiento de datos de los menores se establece que los Estados Iberoamericanos promoverán en la formación académica de los menores el uso responsable y seguro de las tecnologías de la información y comunicación. (artículo 8.2).

Asimismo, la Red Iberoamérica de Protección de Datos en su Plan Estratégico 2021-2025 ha establecido como unos de sus objetivos parte de su estrategia para hacer frente a los cambios de la privacidad la promoción del desarrollo de la educación digital en los planes de estudio para la prevención de los riesgos de internet en el ámbito escolar (apartado 6.2).

En un sentido similar, en la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales adoptada en el 2023 en el marco de la XXVIII Cumbre Iberoamericana de Jefas y Jefes de Estado de Gobierno, estos últimos se comprometieron a impulsar estrategias dirigidas al desarrollo de competencias para el desempeño seguro en entornos digitales por parte de los menores, así como sus familias y comunidades.

Estos documentos regionales contienen importantes aspectos destinados a garantizar una protección efectiva de los datos personales de los menores en la red; sin embargo, es claro que el Estado Peruano aún no ha adoptado íntegramente los criterios establecidos, subestimando así su obligación de garantizar un verdadero disfrute del derecho a la protección de datos personales del menor. Es decir, todavía no se han adoptado todas las medidas posibles que garanticen su seguridad en el acceso a las redes sociales digitales. No se han expedidos políticas y/o programas destinados a la prevención. Tampoco se han adoptados medidas suficientes para favorecer el desarrollo de su personalidad e impartirle un nivel de educación que le permita disfrutar sus derechos, en particular su derecho a la protección de datos personales.

Como se ha venido desarrollando, a nivel nacional se ha regulado el tratamiento de datos personales a fin que este se realice con respeto irrestricto de los derechos fundamentales de los menores; empero, no se han desarrollado medidas específicas para garantizar sus derechos en la Red.

Al respecto, cabe precisar que si bien, los reclamos por la afectación a los derechos de la infancia son dirigidos al Estado, la obligación de velar por su protección y plena vigencia recae en toda la comunidad conforme lo establece la Norma Fundamental. De esta forma, se entiende que es una labor que atañe en conjunto al Estado, la Sociedad y la Familia.

En relación a la participación de la familia, Morillas (2023) sostiene que la "la patria potestad es la primera garantía de protección ante los riesgos de la sociedad digital" (p.86). De esta manera, los padres deberían estar en la capacidad de promover las condiciones favorables para el desarrollo de su personalidad, procurando que los menores acceden a las redes sociales con seguridad y ejerciendo los controles parentales pertinentes. Sin embargo, en países como el nuestro se ha reconocido que los padres, pese a tener la responsabilidad primordial de la crianza de sus hijos, no siempre cumplen de forma apropiada su rol ya que dedican gran parte de su tiempo a desempeñar labores remuneradas, aunado a ello, muchos padres desconocen contenidos relacionados a la ciberseguridad y resguardo de datos personales, e incluso son ellos quienes suelen exponer información personal de sus hijos en sus perfiles de redes sociales.

Dado lo anterior, resulta trascendental trabajar con las familias en la utilización saludable de la Red, ya que su participación es clave en la educación digital (Agencia Española de Protección de Datos, 2024). Además, cabe seguir puntualizando en el rol primordial que desempeña el Estado consistente en intervenir para proteger los derechos del niño. Así lo ha establecido la Convención sobre los Derechos del Niño que dispone que los Estados "*prestarán la asistencia apropiada a los padres y a los representantes legales para el desempeño de sus funciones en lo que respecta a la crianza del niño (…)*" (artículo 18°).

En el mismo sentido, el Comité de los Derechos del Niño de las Naciones Unidas (2021) ha exhortado a los Estados partes a lograr que los padres tengan oportunidades de adquirir conocimientos digitales para ayudar a los niños a reconocer y enfrentar situaciones de riesgo.

Siendo así, corresponde al Poder Público impulsar políticas públicas que hagan efectivos los derechos de los menores en el entorno digital, estableciendo normas que refuercen los derechos digitales, sobre todo en momentos en los que la capacidad de innovación de la tecnología se hace más célere.

El Consejo de Derechos Humanos de las Naciones Unidades (2024) sostiene que la responsabilidad de los Estados frente al derecho de protección de datos personales en la era digital supone no solo la abstención de violarlo, sino también la inclusión de medidas positivas para su efectivo disfrute. De ahí que, la labor sustantiva del derecho a la protección de datos personales no solo consiste en su reconocimiento como derecho, sino también en la ejecución de mecanismos de carácter preventivos que apunten a favorecer una verdadera cultura de protección de datos personales.

Es claro que el papel del usuario menor de edad es vital, pero para ello es importante brindarle todas las herramientas necesarias para hacer efectivo su protección. En este aspecto, también es importante el papel de la industria con la emisión de Políticas de responsabilidad social empresarial como la adhesión a códigos de conducta para el complimiento de la normativa.

En general, desde esta perspectiva de los derechos, lo que se busca es que tanto el sector público como privado logren garantizar un espacio de uso responsable de las redes sociales sin riesgo para el desarrollo físico y moral del menor. La industria podría contribuir estableciendo canales prioritarios y de fácil acceso para que los menores puedan solicitar la eliminación de contenidos violentos o inapropiados.

En la implementación de medidas reales y concretas que coadyuven a combatir los riesgos que se derivan del uso de las redes sociales por los menores es importante que los adolescentes participen activamente en la salvaguardia de sus datos personales. Si estos no son conscientes del riesgo que representa la exposición de sus datos personales es innegable que se continuará con el círculo de afectación. En esta cuestión también es importante resaltar que el Derecho y la educación deben ir de la mano para proteger los derechos de los menores, ya que esta última podría reforzar la tarea de concientizar a los involucrados en relación al tratamiento adecuado de sus datos personales.

Así lo ha resaltado el Comité de los Derechos del Niño de las Naciones Unidas (2021) al subrayar el deber de los Estados partes de integrar la alfabetización digital en la educación escolar como parte de los planes de estudio en los que se incluyan tópicos de estrategias destinadas a proteger los datos personales de los menores. Además, el Consejo de Derechos Humanos de las Naciones Unidades (2024) en su informe sobre mecanismos legales de salvaguarda para la protección de datos personales en la era digital recomienda a los Estados miembros promover de forma prioritaria la información y educación en materia de protección de datos personales, en todos los niveles y en todos los campos a fin de que las personas estén en la capacidad de ejercer sus derechos y recurrir a los mecanismos de tutela pertinentes.

En síntesis, comprender la vulnerabilidad de los menores implica alcanzar un alto nivel de protección de los menores que abarque la salvaguardia de sus datos personales protegiendo al mismo tiempo su derecho de acceso a Internet. Conforme lo afirma Díaz (2018) se trata de reconocer a los menores como protagonistas del diseño de políticas que se establezcan respecto a su protección frente a los riesgos que se derivan del uso de las TICs.

De esta manera, es primordial un enfoque multidisciplinario que contenga la prevención y la capacitación de familias, niños, adolescentes, educadores y agentes sociales para promover

un entorno digital seguro (Asociación Española de Psiquiatría de la Infancia y la Adolescencia, 2024).

En general, el avance de la tecnología debe ir de la mano con el respeto a la persona humana, de tal forma que en el centro de cualquier innovación tecnológica se encuentre la consideración a su dignidad humana; más aún, cuando se trata de niños, niñas y adolescentes para quienes existe la obligación por parte del Estado de garantizar una navegación segura a través de la implementación de instrumentos legales que fomenten la concientización sobre las consecuencias que acarrea su presencia en las redes sociales.

Sin duda, ello supondría el reconocimiento de una responsabilidad colectiva en la salvaguardia de sus derechos; y en ese sentido, “al proteger a la parte débil y tras su incorporación de manera habitual puede dar sensación de exigibilidad al margen de la mera relación entre las partes” (Gil, 2018, p. 114).

III.MÉTODO

3.1. Tipo de investigación

La presente investigación fue de **tipo básica,** también conocida como investigación teórica ya que se enfocó fundamentalmente en expandir el conocimiento teórico sobre un área determinada a fin de comprender el fenómeno estudiado.

El enfoque aplicado al presente estudio fue el **enfoque cuantitativo** ya que se buscó conocer y estudiar una realidad objetiva a través del análisis de datos para lograr una generalización de los resultados obtenidos. Hernández et al. (2014) sostiene que la investigación cuantitativa se basa en "la recolección de datos para probar las hipótesis con base en la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento y probar teorías" (p.4).

3.1.1.Nivel de Investigación

Atendiendo a sus objetivos, la investigación tuvo un **alcance correlacional** ya que buscó conocer el grado de asociación o relación existente entre las variables uso de redes sociales y vulneración del derecho a la protección de datos personales en una determinada población.

3.1.2.Diseño

El diseño del estudio **fue no experimental de tipo transeccional** porque no se realizó manipulación intencional de las variables, sino que se observaron las situaciones ya existentes; es decir, el fenómeno tal como se presentó en su contexto natural; además, la recolección de los datos se realizó en un único momento.

3.2. Ámbito temporal y espacial

El ámbito espacial de la investigación abarcó la Institución Educativa N°1138 José Abelardo Quiñones- Ugel 06 ubicado en el jirón Melitón Carbajal N°200, de la urbanización

Valdivieso y el distrito de Ate; y en relación al ámbito temporal, esta se desarrolló desde el mes de abril de 2023 al mes de agosto de 2024.

3.3. Variables

Atendiendo al enfoque de investigación cuantitativa, las variables de la presente investigación fueron el uso de redes sociales y la vulneración del derecho a la protección de datos personales.

3.3.1.Operacionalización de variables

Tabla 1

Operacionalización de variables

Variable	Definición conceptual	Dimensiones	Indicadores
Uso de redes sociales	Sitio Web que permite conformar redes de usuarios que comparten intereses comunes a través de la creación de perfiles en los que se exhibe información personal.	Facebook	-Configuración -Interacción
		TikTok	-Configuración -Interacción
Vulneración del Derecho a la protección de datos personales	Afectación del derecho fundamental consistente en el poder de disposición y control del titular respecto a sus datos personales frente a terceros, sea el Estado o un particular.	Protección Jurídica	-Consentimiento -Perjuicio
		Mecanismos de Prevención	-Entorno Familiar -Nivel Institucional

Nota. Elaboración Propia.

3.3. Población y muestra

La población es definida como el "conjunto de todos los casos que concuerdan con una serie de especificaciones" (Lepkowski, 2008, como se cita en Hernández et al., 2014, p. 174).

La población de esta investigación estuvo constituida por todos los estudiantes matriculados en el cuarto y quinto grado de secundaria, cuya edad oscile entre los 14 y 17 años y tengan acceso a las redes sociales Facebook y TikTok, pertenecientes a la Institución Educativa N°1138 José Abelardo Quiñones, durante el año escolar 2024.

Esta delimitación poblacional se realizó por razones prácticas de la investigación toda vez que permitió que los cuestionarios sean respondidos por adolescentes que tengan entendimiento mínimo de conceptos jurídicos.

Por otro lado, dado que se tuvo acceso a la totalidad de la población (187 estudiantes) no se aplicó ningún criterio muestral (muestra censal).

3.4. Instrumentos

Para medir las variables de interés de la presente investigación se empleó el **cuestionario**. Este instrumento se estructuró de manera minuciosa con un total de 17 ítems para abordar las 2 dimensiones de la variable uso de redes sociales y 9 ítems para abordar las 2 dimensiones de la variable vulneración del derecho a la protección de datos personales.

El instrumento obtuvo **validez a través del juicio de expertos**, quienes valoraron y validaron el cuestionario, calificando el instrumento como excelente con respecto a su claridad, objetividad, actualidad, organización, suficiencia, intencionalidad, consistencia, coherencia, metodología y conveniencia. Los validadores expertos miembros del equipo fueron seleccionados en base a su experiencia en la disciplina.

Por otro lado, se utilizó el coeficiente de **Alfa de Cronbach para evaluar la confiabilidad del instrumento.** Luego de la aplicación de la prueba piloto a 30 estudiantes, el valor encontrado fue de 0,962 para la variable uso de redes sociales; mientras que, la variable

vulneración del derecho a la protección de datos personales mostró un alfa de Cronbach de 0.934. Estos resultados reflejaron que ambas variables cuentan con alta consistencia interna, lo que garantizó que los ítems utilizados en el cuestionario sean confiables para evaluar las dimensiones correspondientes.

3.5. Procedimientos

La presente investigación se desarrolló en las siguientes etapas:

a.)Revisión de la literatura: Comprendió la obtención de las referencias bibliográficas y otros materiales útiles para el propósito de estudio, luego de lo cual se recopiló e integró información relevante que sirvió para circunscribir el problema de investigación, elaborar las hipótesis y definir las variables. Asimismo, comprendió la construcción de las bases teóricas.

b.)Definición y selección de la muestra: Se delimitó la población y la obtención de la muestra representativa a efectos de obtener los datos necesarios para el análisis cuantitativo.

c.)Recolección de los datos: Comprendió la elección y elaboración del instrumento para recolectar los datos según el planteamiento del problema. Luego de ello, se aplicó el instrumento y se obtuvo y codificó los datos para su análisis a través del programa estadístico.

d.)Análisis e interpretación de los resultados: Se analizó e interpretó las hipótesis planteadas mediante prueba estadística y se prepararon los resultados para su presentación.

3.6. Análisis de datos

Luego de la recopilación y codificación de los datos, estos fueron analizados cuantitativamente mediante la matriz de datos y el **programa estadístico Statistical Package for the Social Sciences (SPSS) en su versión 27** que sirvió para obtener los resultados que se plasmaron en tablas y gráficas. Para determinar la prueba estadística adecuada de correlación se evaluó la normalidad de las variables de estudio a través de la **prueba de Kolmogorov-Smirnov.**

Finalmente, para la determinación de la correlación de las variables se utilizó el **coeficiente Rho de Spearman.**

IV.RESULTADOS

4.1.Análisis descriptivo de los resultados

Tabla 2

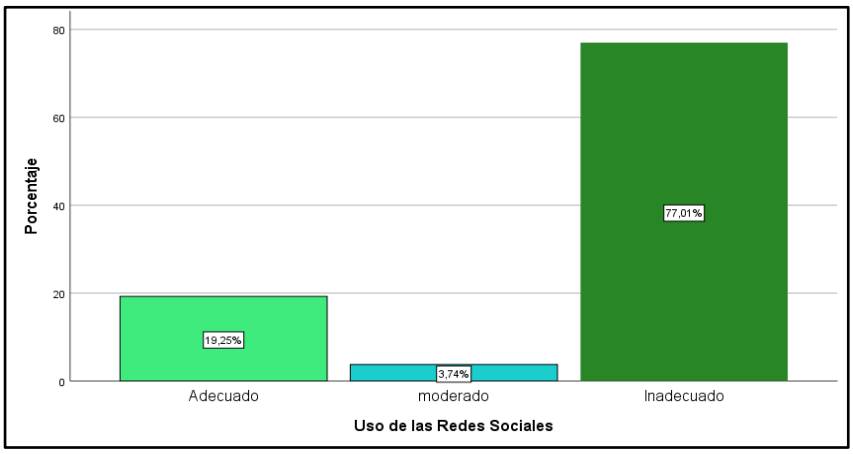
Distribución de datos según la variable uso de redes sociales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

Uso de redes sociales	fi	%
Adecuado	36	19.3
Moderado	7	3.7
Inadecuado	144	77.0
Total	187	100.0

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 1

Uso de redes sociales



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 2 muestra la manera en que los estudiantes de la I.E. N° 1138 José Abelardo Quiñones en el año 2024 hacen uso de redes sociales. Los resultados indican que la mayoría de los estudiantes (77.0%) utiliza las redes sociales de manera inadecuada, lo cual es un hallazgo significativo, ya que sugiere una alta exposición de sus datos personales en estas plataformas. Solo un 19.3% reporta un uso adecuado, mientras que apenas un 3.7% tiene un uso moderado. Estos datos son fundamentales para la investigación ya que confirman que

los estudiantes exponen de forma excesiva su información personal en las redes sociales, lo que potencialmente aumentaría el riesgo de perder el control de sus datos personales.

Tabla 3

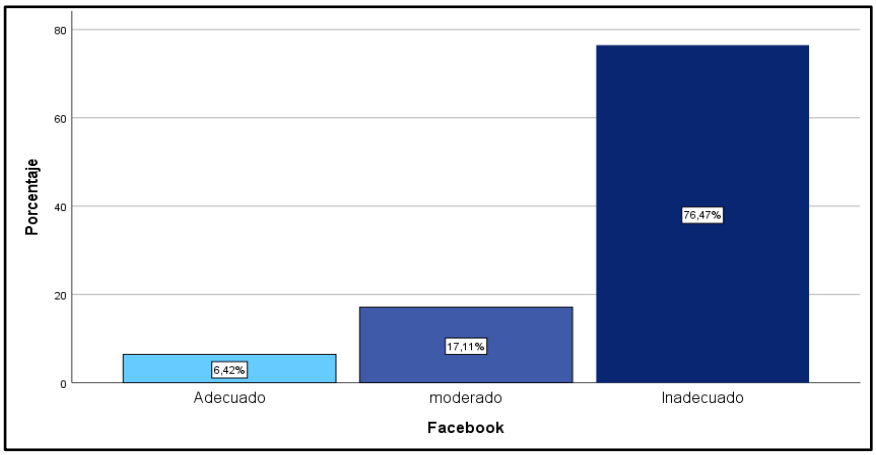
Uso de redes sociales según su dimensión Facebook en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

Facebook	fi	%
Adecuado	12	6.4
Moderado	32	17.1
Inadecuado	143	76.5
Total	187	100.0

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 2

Uso de Facebook



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 3 refleja el uso de Facebook en los estudiantes de la I.E. N° 1138 José Abelardo Quiñones en el 2024. Los resultados muestran que el 76.5% de los estudiantes usan Facebook de manera inadecuada, mientras que solo un 17.1% lo utiliza de forma moderada y un 6.4% lo hace de manera adecuada. Este predominio del uso inadecuado de Facebook revela un aspecto relevante al sugerir que esta red social tiene una alta penetración

en el desenvolvimiento digital de los estudiantes incrementando la exposición a riesgos relacionados con el derecho a la protección de datos personales.

Tabla 4

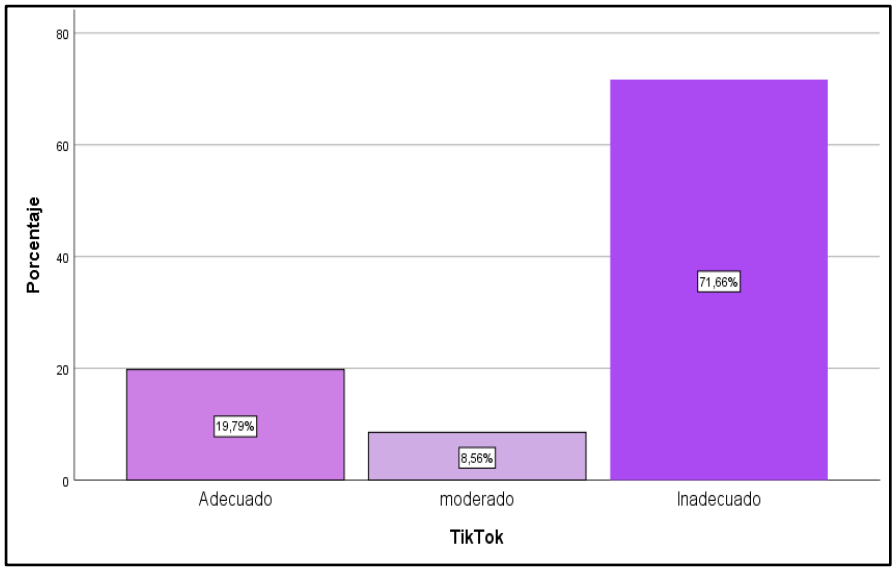
Uso de redes sociales según su dimensión TikTok en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

TikTok	fi	%
Adecuado	37	19.8
Moderado	16	8.6
Inadecuado	134	71.7
Total	187	100.0

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 3

Uso de TikTok



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 4 representa el uso de TikTok en los estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. Los datos indican que el 71.7% de los estudiantes usan TikTok de manera inadecuada, mientras que un 19.8% lo utiliza de forma adecuada y un 8.6% lo hace de forma moderada. Al igual que con Facebook, la alta frecuencia de uso

inadecuado de TikTok es un hallazgo de gran trascendencia para la investigación, ya que refleja una posible vinculación de esta plataforma digital con la esfera de control de datos personales de los estudiantes.

Tabla 5

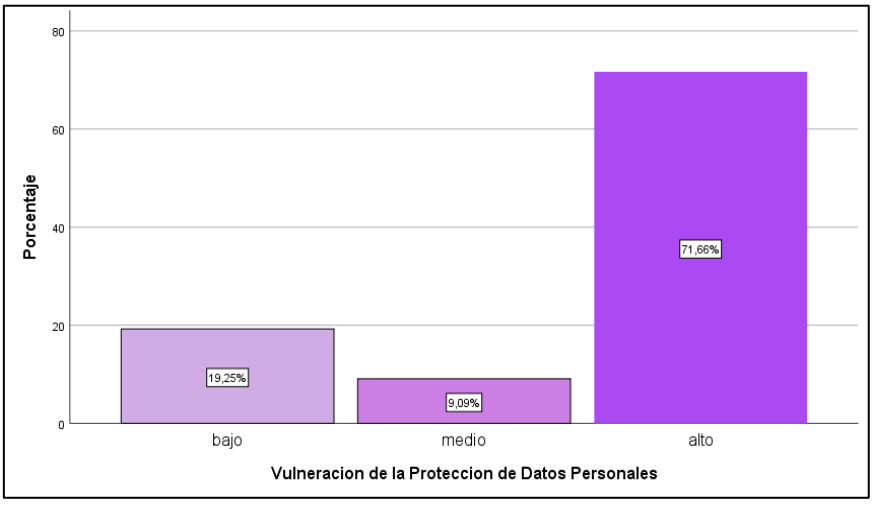
Nivel de vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

Vulneración del derecho a la protección de datos personales	fi	%
Bajo	36	19.3
Medio	17	9.1
Alto	134	71.7
Total	187	100.0

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 4

Vulneración del Derecho a la protección de datos personales



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 5 presenta el nivel de vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. Los resultados muestran cifras preocupantes (71.7%) de estudiantes que experimentan un alto nivel

de vulneración de su derecho a la protección de datos personales, mientras que solo un 19.3% presenta un nivel bajo y un 9.1% un nivel medio. Este hallazgo es sumamente relevante, ya que indica que la mayoría de los estudiantes sufren intromisiones ilegítimas en su esfera personal lo que a su vez refleja una asociación con el uso de redes sociales como Facebook y TikTok.

Tabla 6

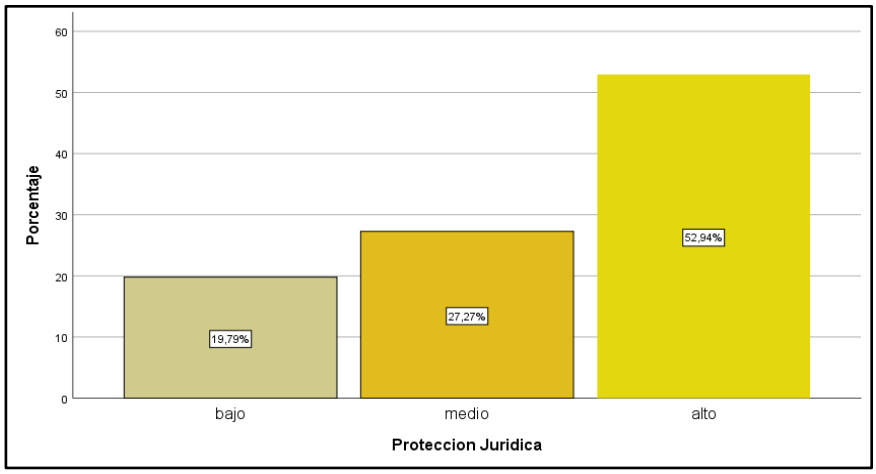
Nivel de vulneración del Derecho a la protección de datos personales según su dimensión Protección Jurídica en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

Protección Jurídica	fi	%
Bajo	37	19.8
Medio	51	27.3
Alto	99	52.9
Total	187	100.0

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 5

Vulneración del Derecho a la protección de datos personales según su dimensión Protección Jurídica



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 6 muestra el nivel de vulneración sobre la protección jurídica de los datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. Los

resultados revelan que el 52.9% de los estudiantes tienen una alta vulneración sobre la protección legal de sus datos personales, mientras que un 27.3% posee un nivel medio y un 19.8% un nivel bajo. Los datos refieren que más de la mitad de los estudiantes no reciben una adecuada protección jurídica, es decir, consideran que han sido víctimas de conductas que contravienen la normativa de protección de datos personales, especialmente la referida al consentimiento.

Tabla 7

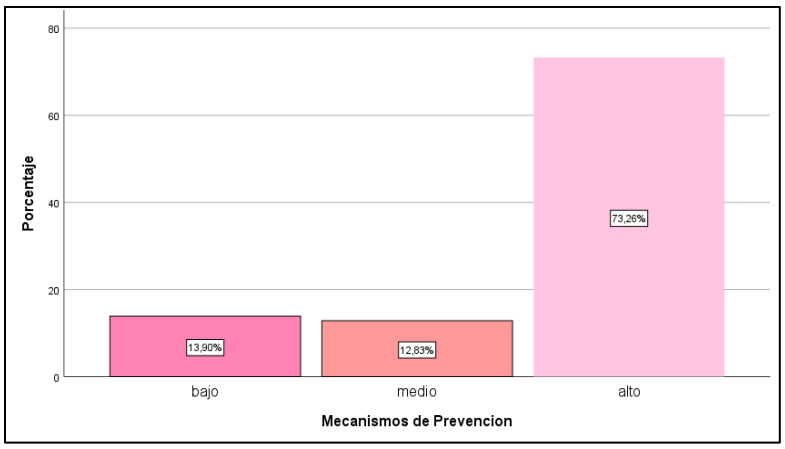
Nivel de vulneración del Derecho a la protección de datos personales según su dimensión Mecanismos de Prevención en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

Mecanismos de Prevención	fi	%
bajo	26	13.9
medio	24	12.8
alto	137	73.3
Total	187	100.0

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 6

Vulneración del Derecho a la protección de datos personales según su dimensión Mecanismos de Prevención



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 7 refleja la distribución de frecuencias de la vulneración del derecho a la protección de datos personales según su dimensión mecanismos de prevención en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024. Los resultados indican que, en cuanto a los mecanismos de prevención, el 73.3% de los estudiantes tiene un alto nivel de vulneración, mientras que un 12.8% sufre una vulneración media y un 13.9% muestra una vulneración baja. Estos datos revelan que dentro de las acciones para proteger y promover el derecho a la protección de datos personales no se han contemplado de manera eficaz mecanismos preventivos que tengan por finalidad dotar de herramientas a los estudiantes para hacer frente a las amenazas a su esfera de control de datos personales durante la navegación en las redes sociales.

Tabla 8

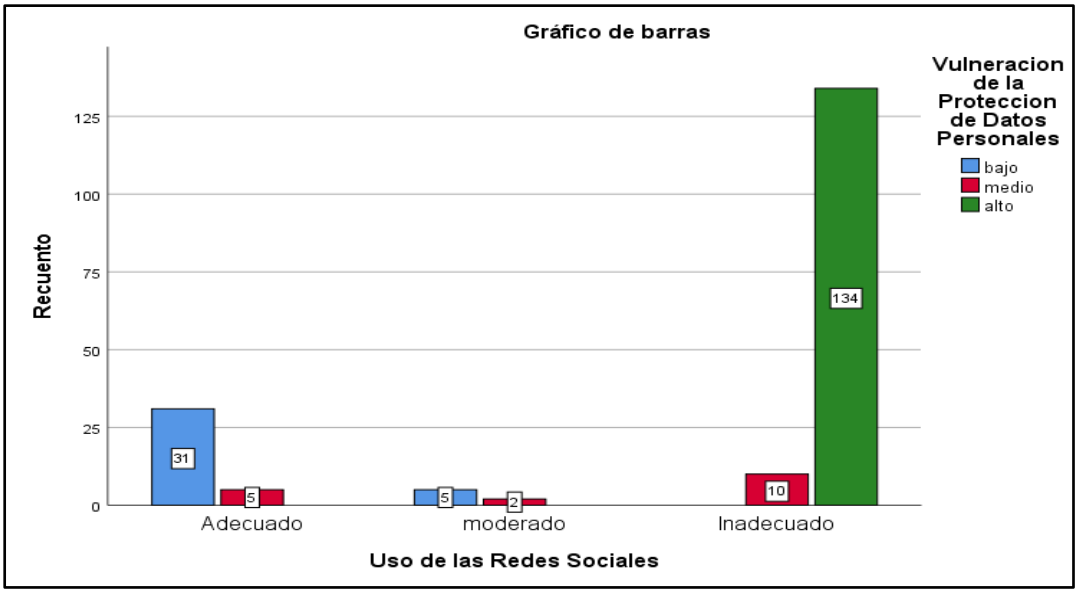
Relación entre el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

Uso de redes Sociales		Vulneración del Derecho a la protección de datos personales			Total
		Bajo	Medio	Alto	
Adecuado	fi	31	5	0	36
	%	16.6%	2.7%	0.0%	19.3%
Moderado	fi	5	2	0	7
	%	2.7%	1.1%	0.0%	3.7%
Inadecuado	fi	0	10	134	144
	%	0.0%	5.3%	71.7%	77.0%
Total	fi	36	17	134	187
	%	19.3%	9.1%	71.7%	100.0%

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 7

Uso de redes sociales vs. vulneración del Derecho a la protección de datos personales



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 8 refleja la relación entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales en los estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. Los resultados indican que el 71.7% de los estudiantes que utilizan redes sociales de manera inadecuada experimentan un alto nivel de vulneración de su derecho a la protección de datos personales. En cambio, aquellos que hacen un uso adecuado o moderado de las redes sociales no presentan altos niveles de vulneración, siendo la mayoría de ellos quienes registran un nivel bajo de vulneración (16.6% y 2.7%, respectivamente). Estos hallazgos son relevantes para la investigación ya que confirman una correlación clara: Los estudiantes que usan redes sociales de manera inadecuada están significativamente más expuestos a la afectación de su derecho a la protección de datos personales mientras que aquellos con un uso adecuado o moderado sugieren menores niveles de vulneración

Tabla 9

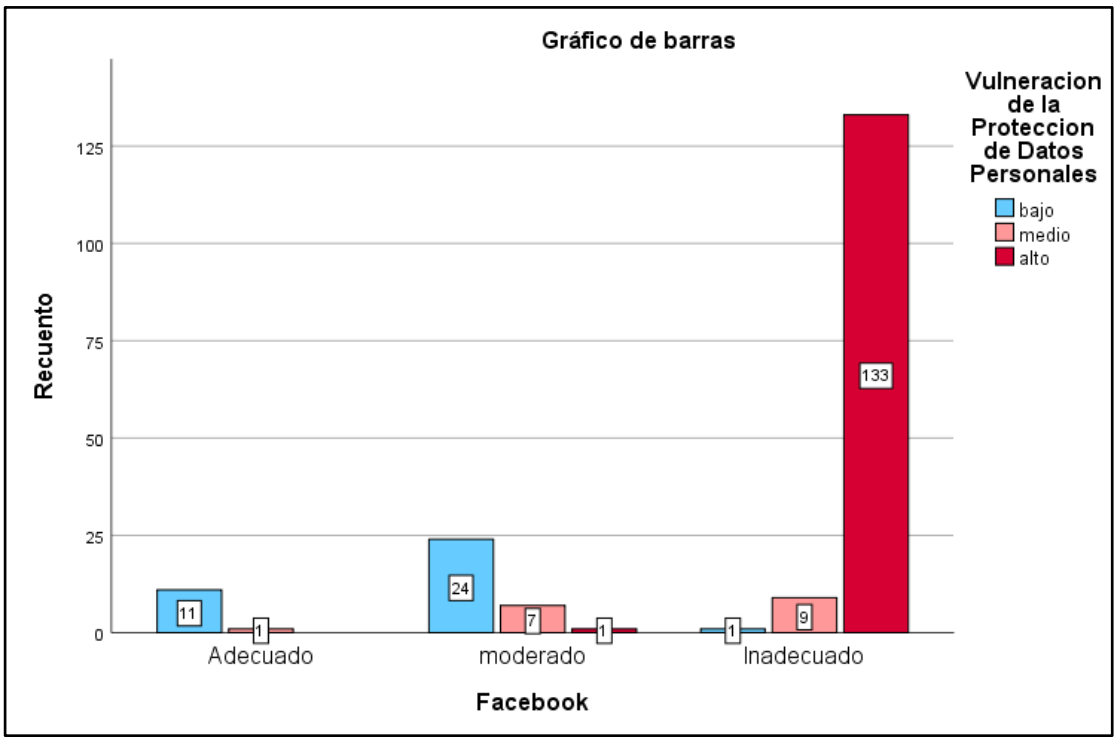
Relación entre el uso de Facebook y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

Facebook		Vulneración del Derecho a la protección de datos personales			Total
		Bajo	Medio	Alto	
Adecuado	fi	11	1	0	12
	%	5.9%	0.5%	0.0%	6.4%
Moderado	fi	24	7	1	32
	%	12.8%	3.7%	0.5%	17.1%
Inadecuado	fi	1	9	133	143
	%	0.5%	4.8%	71.1%	76.5%
Total	fi	36	17	134	187
	%	19.3%	9.1%	71.7%	100.0%

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 8

Uso de Facebook vs. vulneración del Derecho a la protección de datos personales



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 9 refleja la relación entre el uso de Facebook y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. Los datos muestran que el 71.1% de los estudiantes que utilizan Facebook de manera inadecuada experimentan un alto nivel de vulneración de su derecho a la protección de datos personales, mientras que un 0% de los que lo usan de manera adecuada y un 0.5% de los que lo usan de manera moderada reportan altos niveles de vulneración. Esto sugiere una clara correlación entre el uso inadecuado de Facebook y una mayor vulneración del derecho a la protección de datos personales. Los estudiantes que usan la red social Facebook de forma adecuada o moderada presentan en su mayoría bajos niveles de vulneración (5.9% y 12.8%, respectivamente).

Tabla 10

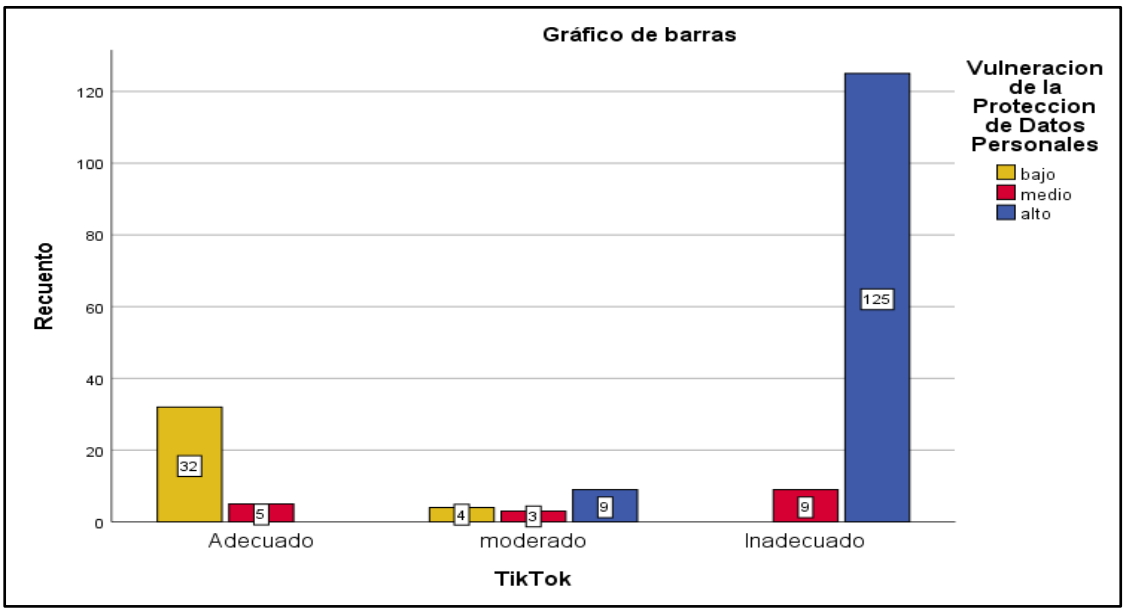
Relación entre el uso de TikTok y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

TikTok		Vulneración del Derecho a la protección de datos personales			Total
		Bajo	Medio	Alto	
Adecuado	fi	32	5	0	37
	%	17.1%	2.7%	0.0%	19.8%
Moderado	fi	4	3	9	16
	%	2.1%	1.6%	4.8%	8.6%
Inadecuado	fi	0	9	125	134
	%	0.0%	4.8%	66.8%	71.7%
Total	fi	36	17	134	187
	%	19.3%	9.1%	71.7%	100.0%

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Figura 9

Uso de TikTok vs. vulneración del Derecho a la protección de datos personales



Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 10 refleja la relación entre el uso de TikTok y la vulneración del derecho a la protección de datos personales en los estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. Los resultados indican que el 66.8% de los estudiantes que utilizan TikTok de manera inadecuada experimentan un alto nivel de vulneración de su derecho a la protección de datos personales, mientras que solo un 4.8% de los que lo usan de manera moderada y un 0% de los que lo usan de manera adecuada reportan altos niveles de vulneración. Los estudiantes que usan TikTok de forma adecuada muestran en su mayoría niveles bajos de vulneración (17.1%) y aquellos con un uso moderado tienen una distribución más variada entre los niveles de vulneración, con solo un 4.8% reportando altos niveles. Estos datos reflejan una fuerte correlación entre el uso inadecuado de TikTok y un alto nivel de vulneración del derecho a la protección de datos personales.

4.2. Análisis Inferencial y/o Contrastación de hipótesis

4.2.1.Prueba de normalidad de las variables (Kolmogórov-Smirnov n>50)

Formulación de la Hipótesis Nula (H_0) y Alterna (H_1)

H_0: La distribución de la variable cumple la normalidad.

H_1: La distribución de la variable no cumple la normalidad.

Regla de decisión:

- P valor es mayor o igual que el valor a (0.05) se acepta la hipótesis nula (H_o)
- P valor es menor que el valor a (0.05) se acepta la hipótesis alterna (H_1)

Tabla 11

Prueba de Normalidad Kolmogórov-Smirnov para el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

	Kolmogórov-Smirnov		
	Estadístico	gl	Sig.
Facebook	0.461	187	0.000
TikTok	0.441	187	0.000
Uso de redes sociales	0.472	187	0.000
Protección Jurídica	0.331	187	0.000
Mecanismos de Prevención	0.446	187	0.000
Vulneración del Derecho a la protección de datos personales	0.441	187	0.000
P valor <0.05** significativo			

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: En la Tabla 11 se presentan los resultados de la prueba de normalidad Kolmogórov-Smirnov para las dos variables relacionadas y sus dimensiones internas, las mismas que presentan resultados p valores:0.000<0.05 por lo que se demuestra que los datos no siguen una distribución normal. Esta falta de normalidad sugiere el empleo de pruebas no paramétricas. Por lo tanto, para esta investigación se sugiere utilizar métodos estadísticos no

paramétricos (correlación de Rho Spearman) para analizar los datos y obtener conclusiones válidas en el contexto del presente estudio.

4.2.2.Prueba de hipótesis general

Nivel de significancia: $\alpha = 0.05 = 5\%$ de margen máximo de error.

Regla de decisión:

$p \geq \alpha \rightarrow$ se acepta la hipótesis nula H_0

$p < \alpha \rightarrow$ se rechaza la hipótesis nula H_0

H_1: Existe una relación significativa entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. 1138 José Abelardo Quiñones,2024.

H_0: No existe una relación significativa entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. 1138 José Abelardo Quiñones, 2024.

Tabla 12

Correlación de Spearman entre el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024

			Vulneración del Derecho a la protección de datos personales	Uso de redes sociales
Rho de Spearman	Vulneración del Derecho a la protección de datos personales	Coeficiente de correlación	1.000	,909**
		Sig. (bilateral)		0.000
		N	187	187
	Uso de redes sociales	Coeficiente de correlación	,909**	1.000
		Sig. (bilateral)	0.000	
		N	187	187
P valor <0.05** significativo				

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 12 muestra la correlación de Spearman entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. Con un p valor (Sig =0.000) menor que el nivel de significancia 0.05. se colegie que existe suficiente evidencia estadística para rechazar la hipótesis nula (H_o) y aceptar la hipótesis alternativa propuesta por el investigador (H_1), confirmándose la existencia de una correlación significativa. Asimismo, el coeficiente de correlación de Spearman de 0.909 indica una fuerte correlación positiva entre las dos variables. A partir de estos resultados se deduce que, si los puntajes de la variable uso de redes sociales aumentan, la vulneración al derecho de protección de datos personales también aumenta; esto es, a mayor exposición en el uso de redes sociales, mayor nivel de vulneración del derecho a la protección de datos personales, confirmando la existencia de una relación significativa entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales en estudiantes en la I.E. N° 1138 José Abelardo Quiñones en 2024.

4.2.3.Prueba de hipótesis específica 1

Nivel de significancia: $\alpha = 0.05 = 5\%$ de margen máximo de error.

Regla de decisión:

$p \geq \alpha \rightarrow$ se acepta la hipótesis nula H_0

$p < \alpha \rightarrow$ se rechaza la hipótesis nula H_0

H_1: Existe una relación significativa entre el uso de la red social Facebook y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, 2024.

H_0: No existe una relación significativa entre el uso de la red social Facebook y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, 2024.

Tabla 13

Correlación de Spearman entre el uso de Facebook y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones,2024

			Vulneración del Derecho a la protección de datos personales	Facebook
Rho de Spearman	Vulneración del Derecho a la protección de datos personales	Coeficiente de correlación	1.000	,887**
		Sig. (bilateral)		0.000
		N	187	187
	Facebook	Coeficiente de correlación	,887**	1.000
		Sig. (bilateral)	0.000	
		N	187	187
P valor <0.05** significativo				

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 13 muestra la correlación de Spearman entre el uso de Facebook y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones en 2024. Se observa un p valor (Sig.=0.000) menor a 0.05, por lo que se rechaza la hipótesis nula (H_o) y se acepta la hipótesis alternativa (H_1). Además, los valores arrojados por la prueba Rho de Spearman fueron de 0.887, lo que indica una fuerte y significativa correlación positiva entre el uso de Facebook y el nivel de vulneración del derecho a la protección de datos personales. Esto sugiere que un mayor nivel en el uso de Facebook está asociado con un mayor nivel de vulneración del derecho a la protección de datos personales.

4.2.4.Prueba de hipótesis específica 2

Nivel de significancia: $\alpha = 0.05 = 5\%$ de margen máximo de error.

Regla de decisión:

$p \geq \alpha \rightarrow$ se acepta la hipótesis nula H_0

$p < \alpha \rightarrow$ se rechaza la hipótesis nula H_0

H_1: Existe una relación significativa entre el uso de la red social TikTok y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, 2024.

H_0: No existe una relación significativa entre el uso de la red social TikTok y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, 2024.

Tabla 14

Correlación de Spearman entre el uso de TikTok y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones,2024

			Vulneración del Derecho a la protección de datos personales	TikTok
Rho de Spearman	Vulneración del Derecho a la protección de datos personales	Coeficiente de correlación	1.000	,841**
		Sig. (bilateral)		0.000
		N	187	187
	TikTok	Coeficiente de correlación	,841**	1.000
		Sig. (bilateral)	0.000	
		N	187	187
P valor <0.05** significativo				

Nota. Elaboración propia en base a los resultados del programa spss vs 27.

Interpretación: La Tabla 14 muestra la correlación de Spearman entre el uso de TikTok y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. Se observa un p valor (Sig.=0.000) menor a 0.05, por lo que existe suficiente evidencia estadística para rechazar la hipótesis nula (H_o) y aceptar la hipótesis alternativa (H_1). Además, el coeficiente de correlación de Spearman es de 0.841, lo que indica una fuerte y significativa correlación positiva entre el uso de TikTok y el nivel de vulneración del derecho a la protección de datos personales. Esto sugiere que un mayor uso de TikTok está asociado con un mayor nivel de vulneración del derecho. Por lo tanto, se concluye confirmando que el uso de la red social TikTok se encuentra relacionado significativamente con la afectación del derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024.

V.DISCUSIÓN DE RESULTADOS

Esta investigación tuvo por objetivo general determinar la relación existente entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024. Los resultados señalan la existencia de una fuerte correlación positiva entre las variables uso de redes sociales y vulneración del derecho a la protección de datos personales, debido al coeficiente de correlación de Spearman que devolvió un valor de 0.909. Esto quiere decir que la manera en la que los estudiantes se desenvuelven en las redes sociales, exponiendo su información personal, tiende a relacionarse con la vulneración del derecho a la protección de datos personales, propiciando intromisiones ilegítimas en su esfera personal. Frente a ello, se confirma la hipótesis planteada en esta investigación, en la cual se refiere que existe una relación significativa entre el uso de redes sociales y la vulneración del derecho a la protección de datos personales en los estudiantes en la I.E. 1138 José Abelardo Quiñones, 2024.

Estos resultados confirman lo expuesto por Chávez (2022) quien en su investigación concluyó que en el ámbito de las redes sociales de ocio se suscitan diversas violaciones a los derechos fundamentales relacionados a intromisiones ilegítimas a la protección de datos personales de los niños y adolescentes. Así también, estos resultados son corroborados con la investigación de tipo de cuantitativa de Zevallos (2021) quien demostró que las redes sociales repercuten directa y muy significativamente en la vulneración de los derechos a la salvaguarda de los datos personales, considerando que a mayor exposición en redes sociales mayor es la vulneración de los derechos a la salvaguarda de los datos personales. Para Castillejos (2021) las trasformaciones digitales traen un kit de pros y contras, por lo que la manera en que se emplee la tecnología determinará el efecto que pueda provocar en el usuario. En efecto, la libertad en las redes sociales trae aparejada el deber de autocuidado que implica la obligación del usuario de tomar decisiones sobre el adecuado manejo de sus datos personales, decisiones

que pueden repercutir en la afectación de sus derechos fundamentales. En relación a ello, Ayllón (2022) enfatiza en que la manera en la que los menores se desenvuelven en las redes sociales determina una mayor facilidad en lo que atañe a la vulneración de algunos derechos como podría ser la protección de datos personales.

En tal sentido, bajo lo referido anteriormente y al analizar los resultados, se confirma que el uso de las redes sociales traducida en la exposición de la información personal como nombres o fotografías personales se vincula con la afectación del derecho a la protección de datos personales de los usuarios menores de edad. Este grupo etario, pese a su aparente dominio de las herramientas digitales no está en la capacidad de llevar a cabo la vigilancia necesaria sobre el uso que terceros hacen de su información personal en las redes sociales, lo que repercute en su facultad de control, aspecto primordial del derecho fundamental a la protección de datos personales.

En cuanto al objetivo específico consistente en determinar la relación existente entre el uso de la red social Facebook y la vulneración del derecho a la protección de datos personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones, 2024. Los resultados indican la existencia de una fuerte y significativa correlación positiva entre el uso de Facebook y la vulneración del derecho a la protección de datos personales, debido al coeficiente de correlación de Spearman que arrojó un valor de 0.887. Esto sugiere que el modo en que es empleado Facebook por los estudiantes se relaciona con el nivel de vulneración de su derecho a la protección de datos personales, es decir, su uso puede determinar a la pérdida del control de sus datos personales. Con estos resultados, se confirma la hipótesis planteada en esta investigación, en la cual se refiere que existe una relación significativa entre el uso de la red social Facebook y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones en 2024.

Los resultados anteriores concuerdan con lo expuesto por Hidalgo (2020) quien en su investigación concluyó sosteniendo que los mecanismos de protección autorregulados por Facebook no cumplen con la finalidad del derecho a la protección de datos personales y que la referida red social posibilita que un tercero pueda acceder a la información de cada usuario debido a la sobreexposición de la información. En un sentido similar, Jauregui y Maldonado(2023) concluyeron su investigación afirmando que Facebook puede ocasionar vulneraciones a la intimidad del usuario, considerando que el tratamiento de datos personales constituye un activo para la publicidad de Facebook, lo cual tiene relación con la presente investigación ya que la vulneración a la intimidad lleva implícita la vulneración del derecho a la protección de datos personales que se encuentra en riesgo de afectación por el uso de la plataforma en cuyo modelo de negocio subyace la acumulación de datos personales, privilegiando de esta manera la exposición excesiva de la información personal de los usuarios.

Sobre este tema, Morrillas (2023) sostiene que la forma de acceso y disposición de sus datos personales en las publicaciones que realizan en redes sociales los menores se aleja considerablemente de la normativa aplicable, esto es, la garantía de protección de sus derechos es insuficientes. Por su parte, Ordóñez (2021) en su investigación revela la incidencia de la falta de concientización sobre los peligros del acceso a medios informáticos en la protección de datos personales de los menores edad. En esa misma línea, la investigación de Rodríguez (2021) revela que el exceso de la información compartida en redes sociales propicia que terceros usen la información con fines ilícitos.

Efectivamente, al no contar esta red social con mecanismos que garanticen una experiencia segura en la red y propiciar la máxima exposición de datos personales se pone en riesgo la garantía del derecho a la protección de datos personales de esta población vulnerable.

En cuanto al segundo objetivo específico consistente en determinar la relación existente entre el uso de la red social TikTok y la vulneración del derecho a la protección de datos

personales en estudiantes de la Institución Educativa N°1138 José Abelardo Quiñones,2024. Los resultados indican la existencia de una fuerte y significativa correlación positiva entre el uso de la red social TikTok y vulneración del derecho a la protección de datos personales, debido al coeficiente de correlación de Spearman que devolvió un valor de 0.841. Esto indica que el uso de la red social TikTok por parte de estudiantes que hacen pública su información personal está asociado a abusos en su esfera personal provenientes de la pérdida del control de sus datos personales.

En atención a lo anterior, se confirma la hipótesis de investigación que señala la existencia de una relación significativa entre el uso de la red social TikTok y la vulneración del derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones en 2024. En ese sentido, se tiene que en el estudio realizado por Manzano y Galarza (2020) se concluyó que los adolescentes exponen libremente sus datos personales en redes sociales, desconociendo la magnitud del peligro al que se enfrentan, por lo que constituye un grupo vulnerable en relación al cumplimiento de sus derechos humanos. Lo anterior se vincula con esta investigación ya que confirma que la interacción de los adolescentes en las redes sociales como TikTok se encuentra relacionado con la afectación de derechos fundamentales, como puede ser el derecho a la protección de datos personales, ello como consecuencia de los excesos derivados del uso y/o difusión de sus datos de carácter personal registrados en las redes sociales. Refiriéndose a la red social TikTok, Castillejos (2021) advierte sobre los problemas de seguridad digital de esta plataforma consistentes en el manejo de los datos personales y la sobreexposición de la vida personal de los usuarios. Lo anterior también se encuentra sustentado por Chávez (2022) quien afirma que la mayor inquietud sobre las redes sociales se centra en la elevada participación de los menores quienes publican todo tipo de información sobre ellos y otros usuarios lo que afecta su

protección. En el mismo sentido, Priego (2022) afirma que las redes sociales se encuentran ligadas a la posibilidad de lesión a la intimidad y el uso de inapropiado de los datos personales.

De esta forma, se entiende que la navegación en TikTok sin ningún de tipo de cuidado favorece que la plataforma se constituya en un espacio de exposición excesiva de información personal de los usuarios, y de esta manera, se facilite su uso indebido por parte de terceros, lo cual puede determinar la afectación del derecho a la protección de datos personales en donde estos últimos son tratados sin el cumplimiento de la normativa aplicable.

A partir de los resultados expuestos y las coincidencias halladas con diferentes investigaciones y aportes teóricos se desprende que mientras no se geste una normativa adecuada los menores continuarán inmersos en las redes sociales sin el cuidado pertinente de su información personal lo que se encuentra relacionado con altos niveles de vulneración de su derecho a la protección de datos personales.

Finalmente, teniendo en cuenta la relevancia de la problemática planteada, se requieren más estudios que puedan evaluar la asociación del uso de redes sociales y el nivel de vulneración de los derechos fundamentales de los estudiantes de la institución educativa en general, así como de otros centros educativos.

VI.CONCLUSIONES

6.1. Se determinó la existencia de una relación positiva fuerte y significativa entre las variables uso de redes sociales y vulneración del derecho a la protección de datos personales en estudiantes de la I. E N° 1138 José Abelardo Quiñones, 2024, debido al coeficiente de correlación de Spearman que devuelve un valor de 0.909. Este valor sugiere que, a medida que se incrementa la deficiencia en el uso de redes sociales, existe un aumento estadísticamente significativo de los niveles de vulneración del derecho a la protección de datos personales.

6.2. En los estudiantes de la I. E N° 1138 José Abelardo Quiñones, 2024 predomina un uso inadecuado de las redes sociales, por cuanto el 77% las utiliza de manera inadecuada, lo que sugiere una sobreexposición de sus datos personales en el uso de estas plataformas.

6.3. El nivel de vulneración del derecho a la protección de datos personales en los estudiantes de la I. E N° 1138 José Abelardo Quiñones, 2024 resulta preocupante, en el sentido que el 71.7% de estudiantes experimenta un alto nivel de vulneración, mientras que solo un 19.3% presenta un nivel bajo y un 9.1% un nivel medio de vulneración.

6.4. Existe una relación positiva fuerte y significativa entre el uso de la red social Facebook y la variable vulneración del derecho a la protección de datos personales en estudiantes de la I. E N° 1138 José Abelardo Quiñones, 2024, debido a que el coeficiente de correlación de Spearman devuelve un valor de 0.887. Esta relación refiere que las malas prácticas en la gestión de datos personales durante el uso de Facebook están vinculadas fuertemente con la afectación del derecho a la protección de datos personales.

6.5. Existe una relación positiva fuerte y significativa entre el uso de la red social TikTok y la variable vulneración del derecho a la protección de datos personales en estudiantes de la I.E N°1138 José Abelardo Quiñones, 2024, debido a la correlación de Spearman que devuelve un valor 0.841. Este hallazgo sugiere que las acciones asociadas al uso de la

red social TikTok desempeñan un papel importante en el incremento del uso no autorizado de los datos personales.

VII.RECOMENDACIONES

7.1. Promover instrumentos legislativos que garanticen el reconocimiento de los derechos digitales de los usuarios para proteger las libertades e intereses en el ámbito digital, con inclusión de la protección de los menores en Internet, derecho a la seguridad digital, derecho a la educación y competencias digitales, y derecho a la identidad digital. Dada la celeridad de las innovaciones tecnológicas, la normativa debe contener principios y medios flexibles que garanticen su rápida actualización frente a la transformación digital.

7.2. Promover acciones de política educativa dirigidas a la integración de la ciberseguridad en los planes de estudios escolares a fin de preparar a los estudiantes en temas sobre la privacidad, protección de datos personales, identidad digital y seguridad de la información en línea. Asimismo, se debe propiciar el desarrollo de competencias digitales docentes con programas de capacitación a nivel nacional enfocados en el uso eficiente y responsable de las Tecnologías de la Información y Comunicación.

7.3. Impulsar iniciativas de alfabetización digital de padres y/o tutores a través de acciones de capacitación o campañas de sensibilización sobre modelos de negocios que mercantilizan datos personales, uso responsable de la información personal y violencia digital con el fin de que se gestione de manera adecuada la huella digital de los menores a su cargo.

7.4. Establecer un Canal de Atención, ágil, sencillo y de fácil acceso para los menores en el cual se atiendan con prioridad las denuncias por uso inadecuado de datos personales en las redes sociales gestionándose la eliminación – en menos de 48 horas- de contenidos digitales que afectan su integridad. Un sistema rápido, en línea, con mecanismos de asistencia legal especialmente diseñado para los menores.

7.5. Los proveedores de servicios de redes sociales deben comprometerse en materia de protección de datos, reforzando sus sistemas de verificación asociado a la edad que permitan limitar el acceso de forma efectiva de los menores de 14 años, conforme se encuentra en la legislación peruana. Asimismo, se debe enfatizar en el diseño de redes sociales adecuados a la edad de los menores y seguros desde el principio, lo que debe verificarse a través de procesos prácticos y mecanismos de seguimiento pertinentes.

VIII.REFERENCIAS

Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa. (2019). *Manual de legislación europea en materia de protección de datos*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf

Agencia Española de Protección de Datos. (2024). *Menores, salud digital y privacidad.* https://www.aepd.es/guias/estrategia-menores-aepd-lineas-accion.pdf

Agencia Española de Protección de Datos, Agencia Vasca de Protección de Datos, & Autoridad Catalana de Protección de Datos. (2017a). *Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento*. https://www.aepd.es/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

Agencia Española de Protección de Datos, Agencia Vasca de Protección de Datos, & Autoridad Catalana de Protección de Datos. (2017b). *Guía para el cumplimiento del deber de informar.* https://www.aepd.es/guias/guia-modelo-clausula-informativa.pdf

Aguilar, D. E., & Said, E. (2010). Identidad y subjetividad en las redes sociales virtuales: caso de Facebook. *Zona Próxima*, (12), 190-207. https://www.redalyc.org/pdf/853/85316155013.pdf

Aparicio, J. P. (2019). Principios del tratamiento y derechos de los interesados en la nueva normativa de protección de datos personales: Consideraciones de carácter general y algunos apuntes para el ámbito universitario. *Rueda: Universidad, Ética Y Derechos,* (3/4), 19-40. https://revistas.uca.es/index.php/Rueda/article/view/5423

Asamblea General de las Naciones Unidas. (2022). *Derecho a la privacidad.* https://docs.un.org/es/A/77/196

Asociación Española de Psiquiatría de la Infancia y la Adolescencia. (2024). *Recomendaciones de Uso de Nuevas Tecnologías en la Infancia y Adolescencia*. https://aepnya.es/wp-content/uploads/2024/06/AEPNYA-Recomendaciones-de-Uso-de-Nuevas-Tecnologias-en-la-Infancia-y-Adolescencia-1.pdf

Ayllón, J. D. (2022). Consentimiento de los menores de edad en las redes sociales: especial referencia a TikTok. *Actualidad Jurídica Iberoamericana,* (16), 580-609.

Barrón, P. (2019). La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales). *Cuadernos Europeos de Deusto,* (61), 29-65. https://doi.org/nm2w

Blasco, H. (2021). El impacto de las redes sociales en las personas y en la sociedad: redes sociales, redil social, ¿o telaraña? *Tarbiya, Revista De Investigación E Innovación Educativa*, (49). https://doi.org/10.15366/tarbiya2021.49.007

Boyd, D. M., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. [Sitios de redes sociales: Definición, historia y estudio]. *Journal of Computer-Mediated Communication, 13*(1), 210-230. https://doi.org/gzn

Castillejos, B. (2021). Ambivalencia en TikTok: aprendizaje permanente y riesgos de seguridad coexistiendo. *IE Revista De Investigación Educativa De La Rediech*, *12*(e1294), 1-14. https://doi.org/10.33010/ie_rie_rediech.v12i0.1294

Castro, K. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. *IUS ET VERITAS, 18*(37), 260-276. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/12229

Chávez, L. E. (2022). *Las redes sociales y el derecho fundamental a la intimidad de los niños, niñas y adolescentes en el Perú* [Tesis de pregrado, Universidad Nacional Santiago Antúnez de Mayolo]. Repositorio Institucional de la Universidad Nacional Santiago

Antúnez de Mayolo. https://repositorio.unasam.edu.pe/item/c63af6b3-8daa-442f-9c2b-796b085c41d8

Chipana, J. (2019). La (in)validez de los contratos celebrados por menores de edad en el código civil peruano. *Revista de Derecho Yachaq*, (10), 117-128.

Comité de los Derechos del Niño de las Naciones Unidas. (2021). *Observación general núm.25 (2021) relativa a los derechos de los niños en relación con el entorno digital.* https://documents.un.org/doc/undoc/gen/g21/053/46/pdf/g2105346.pdf

Comité Europeo de Protección de Datos. (2020). *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679.* https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

Comité Europeo de Protección de Datos. (2021). *Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD.* https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_es.pdf

Consejo de Derechos Humanos de las Naciones Unidades. (2024). *Mecanismos legales de salvaguarda para la protección de datos personales y la privacidad en la era digital.* https://docs.un.org/es/A/HRC/55/46

Defensoría del Pueblo. (2019). *Manual de Protección de Datos Personales.* https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Personales.pdf

Díaz, L. M. (2018). Menores e Internet: Entre las oportunidades y los riesgos. Un punto de partida para entender las políticas criminales. En A. Batuecas Caletrío & J.P Aparicio Vaquero (Coords.), *Algunos desafíos en la protección de datos personales* (pp. 137-169). Editorial Comares.

Díaz, V. (2011). Mitos y realidades de las redes sociales: Información y comunicación en la Sociedad de la Información. *Prisma Social*, (6), 1-26. https://www.redalyc.org/pdf/3537/353744578007.pdf

Donoso, L., & Reusser, C. (2021). *Protección de Datos Personales*. Academia Judicial de Chile.

Echeburúa, E., & De Corral, P. (2010). Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: Un nuevo reto. *Adicciones, 22*(2),91-96. https://doi.org/10.20882/adicciones.196

Farfán, L. R. (2020). *Riesgos sociales por uso inadecuado de las redes sociales en los niños de quinto grado del colegio Miguel Cortés. Sullana. 2020* [Tesis de pregrado, Universidad Cesar Vallejo]. Repositorio Institucional de la Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/75876

Florit, C. (2022). *Los menores e internet. Riesgos y derechos*. Bosch Editor.

Fondo de las Naciones Unidas para la Infancia. (2017). *Niños en un Mundo Digital. Estado mundial de la infancia 2017*. https://www.unicef.org/media/48591/file/SOWC_2017_SP.pdf

Galarza, K. L., & Manzano, T. S. (2020). *El Estado como garante del derecho a la protección de datos personales y el derecho a la intimidad de adolescentes inmersos en las redes sociales en el Ecuador* [Tesis de maestría, Universidad de Otavalo]. Repositorio Digital Universidad de Otavalo. https://repositorio.uotavalo.edu.ec/items/0b9a508c-66c7-43f1-80c0-1d60ebcfdffd

Galvis, L. (2019). *Protección de datos personales de Niños, Niñas y Adolescentes. En el marco de la juridificación y prevención del riesgo digital en Colombia* [Tesis de doctorado, Universidad Santo Tomás]. Repositorio Institucional de la Universidad de Santo Tomás. https://repository.usta.edu.co/handle/11634/22124

García, M. C. (2020). Datos personales y menores de edad. En I. González Pacanowska (Coord.), *Protección de Datos personales* (pp. 161-238). Tirant Lo Blanch; Asociación de Profesores de Derecho Civil.

García- Ripoll, M. (2020). El consentimiento al tratamiento de datos personales. En I. González Pacanowska (Coord.), *Protección de Datos personales* (pp. 79-159). Tirant Lo Blanch; Asociación de Profesores de Derecho Civil.

Garduño, G., & Magaña, M. (2022). Los avisos de privacidad en redes sociales: un estudio frente a la libre contratación. En J. M. Soberanes & G. Garduño (Coords.), *La interacción de las redes sociales, la tecnología y los derechos humanos* (pp. 171-182). Eunsa.

Gil, C. (2018). La autorregulación y los códigos de conducta en las redes sociales. En A. Batuecas Caletrío & J. P Aparicio Vaquero (Coords.), *Algunos desafíos en la protección de datos personales* (pp. 87-115). Editorial Comares.

Gil, A. M. (2013). La privacidad del menor en internet. *Revista de Derecho, Empresa y Sociedad*, (3), 60-96.

González, E. (2021). Los derechos digitales fundamentales: ¿Es necesaria su reconfiguración en el ordenamiento jurídico? *Revista de Derecho Administrativo-CDA*, (20), 234-267.

Grupo de Trabajo del Artículo 29. (2007). *Dictamen 4/2007 sobre el concepto de datos personales*. Unión Europea. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Grupo de Trabajo del Artículo 29. (2009). *Dictamen 5/2009 sobre las redes sociales den línea*. Unión Europea. https://www.aec.es/wp-media/uploads/DPD-00207.pdf

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill e Interamericana Editores de C. V.

Hidalgo, I. (2018). *Derecho a la protección de datos personales.* Universidad Nacional Autónoma de México; Instituto Nacional de Estudios Históricos de las Revoluciones de México. https://www.inehrm.gob.mx/recursos/Libros/DerProtectDatos.pdf

Hidalgo, Y. H. (2020). *El paradigma del derecho global para la protección de datos personales en redes sociales* [Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo]. Repositorio Institucional de la Universidad Católica Santo Toribio de Mogrovejo. https://tesis.usat.edu.pe/handle/20.500.12423/2808

Huber, R. (Ed.). (2009). *Jurisprudencia del Tribunal Constitucional Federal Alemán: extractos de las sentencias más relevantes compiladas por Jürgen Schwabe*. Konrad Adenauer.

Instituto Nacional de Ciberseguridad. (2019). *Guía de Seguridad en redes sociales para familias*. https://www.incibe.es/sites/default/files/contenidos/materiales/Campanas/is4k-guia-rrss.pdf

Instituto Nacional de Ciberseguridad. (2020). *Uso y configuración segura*. https://www.incibe.es/menores/tematicas/uso-y-configuracion-segura

Iriarte, E. A., & Bolaños, G. G. (2024). La legítima inquietud: ¿puedo saber cómo otros usuarios de redes sociales obtuvieron mis datos personales publicados en sus perfiles? *Forseti Revista de Derecho*, *13*(19), 157-187.

Jauregui, O. D. (2023). *Los datos personales y su tratamiento como activo para la publicidad de Facebook* [Tesis de pregrado, Universidad Católica San Pablo]. Repositorio Institucional de la Universidad Católica San Pablo. https://repositorio.ucsp.edu.pe/item/2b88f4b1-2f4d-4249-9bdd-ccdb40804492

Landa, C. (2017). *Los Derechos Fundamentales*. Fondo editorial de la Pontificia Universidad Católica del Perú.

Linares, S. (2020). La autonomía del derecho fundamental a la autodeterminación informativa. En L. R. Sáenz Dávalos (Coord.), *El Hábeas Data en la actualidad: Posibilidades y límites* (pp. 381-398). Centro de Estudios Constitucionales del Tribunal Constitucional.

Mayorga-Veloz, A.P., Noboa-Avalos, E. J., Pajuña-Inchiglema, C.D., & Mosquera- Endara, M. del R. (2024). Las redes sociales y la violación del derecho a la intimidad. *Verdad y Derecho. Revista Arbitrada de Ciencias Jurídicas y Sociales*,*3*,230-241. https://doi.org/10.62574/t2gt9v96

Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes. (2009). https://www.iijusticia.edu.ar/Memo.htm

Merino, J. A. (2023). El derecho al olvido en las redes sociales y su aparente conflicto con otros derechos. En J. M. Soberanes & G. Garduño (Coords.), *La interacción de las redes sociales, la tecnología y los derechos humanos* (pp. 255-272). Eunsa.

Meta. (26 de julio de 2022). *Condiciones del servicio* [Página de Facebook]. Recuperado el 04 de mayo de 2024, de https://www.facebook.com/terms/

Meta. (26 de junio de 2024). *Política de privacidad* [Página de Facebook]. Recuperado el 24 de agosto de 2024, de https://www.facebook.com/privacy/policy/version/25238980265745528/

Moralejo, N. (2023). *Los derechos de los menores y las redes sociales*. Tirant Lo Blanch.

Morillas, M. (2023). La protección de datos, atendiendo a la edad de los usuarios, como garantía en la prevención de los riesgos de la sociedad digital. *Revista Internacional de Doctrina y Jurisprudencia*, *29*, 65-90. https://doi.org/10.25115/ridj.vi29.9324

Ordóñez, L. O. (2021). *El derecho fundamental a la protección de datos personales en Ecuador* [Tesis de doctorado, Universidad de Cádiz]. Repositorio Institucional de la Universidad de Cádiz. https://rodin.uca.es/handle/10498/26411

Orihuela, J. L. (2008). Internet: la hora de las redes sociales. *Nueva Revista de Política, Cultura y Arte*, (119), 57-65. https://hdl.handle.net/10171/2962

Pérez, R. (2018). La Protección de los datos del menor en el uso de las Tecnologías de la Información y Comunicación (TIC). *Revista de Derecho Privado, 102*(3), 67-109. https://doi.org/nnjq

Perkins, T. (2022). *TikTok Analysis* [Análisis de TikTok]. Internet 2.0. https://internet2-0.com/content/files/2023/07/TikTok-Technical-Analysis-17-Jul-2022.-Media-Release.pdf

Polo, A. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, *1*(108), 165-193. https://doi.org/10.5944/rdp.108.2020.27998

Polo, A. (2021). Datos, Datos, Datos: El dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos. *Cuadernos Europeos de Deusto, 69*(1), 165-194. https://doi.org/10.18543/ed-69(1)-2021pp211-240

Priego, V. (2022). Los derechos de las personas menores de edad en entornos digitales. Oportunidades, riesgos y protección. En V. Priego (Coord.), *Protección jurídica de las personas menores de edad. Un estudio multidisciplinar (*pp. 119-180). Dykinson.

Ravetllat, I., & Basoalto, C. (2021). La protección de datos personales de niños, niñas y adolescentes: respuestas desde el ordenamiento jurídico chileno. *Estudios constitucionales, 19*(1), 111-145. https://doi.org/nm2x

Red Iberoamericana de Protección de Datos. (2017). *Estándares de Protección de datos Personales para los Estados Iberoamericanos*. https://www.redipd.org/documento/estandares-iberoamericanos-2017.pdf

Red Iberoamericana de Protección de Datos. (2020). *Plan Estratégico 2021-2025: Nuevos tiempos para la privacidad, nuevas estrategias.* https://www.redipd.org/documento/plan-estrategico-ripd-2021-2025.pdf

Rodríguez, C. (2021). *Las formas discursivas y la protección de datos personales en las redes sociales. Facebook Inc. ¿Consentimiento informado? Sí&Acepto* [Tesis de maestría, Universidad de San Andrés]. Repositorio Digital San Andrés. https://repositorio.udesa.edu.ar/items/f468177a-3ddc-461a-ac28-4927823be665

Román, J. (2023). ¡¡ Alerta!! ¿Estás protegiendo tu privacidad y tus datos personales? En J. M. Soberanes & G. Garduño (Coords.), *La interacción de las redes sociales, la tecnología y los derechos humanos* (pp. 357-371). Eunsa.

Sánchez, M. J., & Romero, Y. (2021). El régimen jurídico de las redes sociales y los retos que plantea el acceso a dichas plataformas. *Cuadernos de Derecho Transnacional*, *13*(1), 1139-1148. https://doi.org/10.20318/cdt.2021.6023

Sánchez, M. F. (2024). Privacidad, huella digital y derecho a la protección de datos personales en Internet. Revisa Internacional de Derechos Humanos, *14(*2), 101-149. https://doi.org/10.26422/ridh.2024.1402.san

Secretaría General Iberoamericana. (2023). *Carta Iberoamericana de Principios y Derechos en los Entornos Digitales*. https://www.segib.org/wpcontent/uploads/Carta_iberoamericana_derechos_digitales_ESP_web.pdf

Terrones, Y. (2021). *Derechos fundamentales de los niños y adolescentes en redes sociales* [Tesis de maestría, Universidad Nacional Federico Villarreal]. Repositorio Institucional

de la Universidad Nacional Federico Villarreal. https://repositorio.unfv.edu.pe/handle/20.500.13084/5238

TikTok. (02 de enero de 2024). *Política de privacidad* [Página de TikTok]. Recuperado el 12 de agosto de 2024, de https://www.tiktok.com/legal/page/row/privacy-policy/es

TikTok. (febrero de 2021). *Términos de Servicio* [Página de TikTok]. Recuperado el 12 de agosto de 2024, de https://www.tiktok.com/legal/page/row/terms-of-service/es

Toral, E. (2020). Menores y redes sociales: consentimiento, protección y autonomía. *Derecho Privado y Constitución*, (36), 179-218. https://doi.org/10.18042/cepc/dpc.36.05

Troncoso, A. (2012). Las redes sociales a la luz de la propuesta de Reglamento general de protección de dato personales. Parte uno. *IDP. Revista de Internet, Derecho y Política,* (15), 61-75. https://doi.org/10.7238/idp.v0i15.1646

Warren, S., & Brandeis, L. (1890). The Right to Privacy [El derecho a la privacidad]. *Harvard Law Review*, *4*(5), 193-220. https://doi.org/10.2307/1321160

We are social & Meltwater. (2024). *Digital 2024 Global Overview Report. The essential guide to the world´s connected behaviours*. https://datareportal.com/reports/digital-2024-global-overview-report

We are social & Meltwater. (2024). *Digital 2024 Perú. The essential guide to the latest connected behaviours*. https://datareportal.com/reports/digital-2024-peru

Zamudio, M. L. (2021). *El derecho a la protección de datos personales de los trabajadores frente al control laboral a través del sistema de geolocalización GPS. límites y propuestas* [Tesis de maestría, Pontificia Universidad Católica del Perú]. Repositorio Institucional de la Pontificia Universidad Católica del Perú. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/20150

Zamudio, M. L. (2022). Reflexiones sobre la observancia del derecho fundamental a la protección de datos personales en diversos actos regulados por el Código Civil. *Ius Et Praxis,* (55), 65-90. https://doi.org/nnjr

Zevallos, M. E. (2021). *Redes sociales y su incidencia en la vulneración del derecho a la intimidad en los habitantes de Trujillo, 2020* [Tesis de doctorado, Universidad César Vallejo]. Repositorio Institucional de la Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/69219

Normativa

Constitución Política del Perú. [Const], 29 de diciembre de 1993 (Perú).

Convención Americana sobre Derechos Humanos, 22 de noviembre de 1969.

Convención sobre los Derechos del Niño, 20 de noviembre de 1989.

Declaración de los Derechos del Nino, 20 de noviembre de 1959.

Declaración Universal de los Derechos Humanos, 10 de diciembre de 1948.

Decreto Legislativo N°1384. Decreto Legislativo que reconoce y regula la capacidad jurídica de las personas con discapacidad en igualdad de condiciones. (04 de setiembre de 2018). Presidencia de la República del Perú. https://cdn.www.gob.pe/uploads/document/file/192139/DL_1384.pdf?v=1593814894

Decreto Supremo Nº 003-2013-JUS. Reglamento de la Ley N°29733, Ley de Protección de Protección de Datos Personales. (22 de marzo de 2013). Presidencia de la República del Perú. https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1075450

Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenido y servicios digitales. (20 de mayo de 2019). Parlamento Europeo y Consejo de la Unión Europea. https://www.boe.es/doue/2019/136/L00001-00027.pdf

Ley N° 27337. Código de los Niños y Adolescentes. (07 de agosto del 2000). Congreso de la República del Perú. https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H682689

Ley N° 29733. Ley de Protección de Datos Personales. (03 de julio de 2011). Congreso de la República del Perú. https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1034642

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (06 de diciembre del 2018). Jefatura del Estado de España. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Pacto Internacional de Derechos Civiles y Políticos, 16 de diciembre de 1966.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (27 de abril de 2016). Parlamento Europeo y el Consejo de la Unión Europea. https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Jurisprudencia

Asunto C–25/17. (10 de julio de 2018). Tribunal de Justicia (Gran Sala) de la Unión Europea. https://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=ES

Asunto C-360/10, caso SABAM c. Netlog NV. (16 de febrero de 2012). Sala Tercera del Tribunal de Justicia de la Unión Europea. https://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=ES

Expediente N.° 3330-2004-AA/TC-Lima (11 de julio de 2005). Tribunal Constitucional del Perú. https://www.tc.gob.pe/jurisprudencia/2005/03330-2004-AA.pdf

Expediente N°04739-2007-PHD/TC-Lima. (15 de octubre de 2007). Tribunal Constitucional del Perú. https://tc.gob.pe/jurisprudencia/2008/04739-2007-HD.pdf

Expediente N°04387-2011-PHD/TC-Lima. (29 de agosto de 2013). Tribunal Constitucional del Perú. https://www.tc.gob.pe/jurisprudencia/2013/04387-2011-HD.html

Expediente N.° 02839-2021-PHD/TC- Lima. (22 de agosto de 2022). Tribunal Constitucional del Perú. https://tc.gob.pe/jurisprudencia/2022/02839-2021-HD.pdf

Sentencia 3077/2006. (15 de junio de 2006). Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de España. https://is.muni.cz/el/phil/podzim2011/SJ0B768/um/27414290/Sentencia_de_AN_Proteccion_de_Datos.pdf

Opiniones consultivas

Opinión Consultiva N° 43-2020-JUS/DGTAIPD. (09 de octubre de 2020). Autoridad Nacional de Protección de Datos Personales. https://cdn.www.gob.pe/uploads/document/file/1536674/OC%2043.pdf.pdf?v=1626281343

Opinión Consultiva Nº 19-2019-JUS/DGTAIPD. (07 de marzo de 2019). Autoridad Nacional de Protección de Datos Personales. https://www.gob.pe/institucion/anpd/informes-publicaciones/1373790-oc-n-19-2019-jus-dgtaipd-sobre-obligacion-de-solicitar-el-consentimiento-para-el-tratamiento-de-datos-personales

Resoluciones Administrativas

Resolución del Proceso Sancionador PS/00070/2019. (18 de noviembre de 2020). Agencia Española de Protección de Datos Personales. https://www.aepd.es/documento/ps-00070-2019.pdf

Resolución R/01870/2017. (21 de agosto de 2017). En el procedimiento sancionador PS/00082/2017. Agencia Española de Protección de Datos Personales. https://www.aepd.es/sites/default/files/2019-12/PS-00082-2017_REC.pdf

Resolución Directoral N° 1114-2022-JUS/DGTAIPD-DPDP. (17 de marzo del 2022). En el Procedimiento Administrativo Sancionador N° 008-2020-JUS/DGTAIPD-PAS. Dirección de Protección de Datos Personales de la Autoridad Nacional de Protección de Datos Personales. https://cdn.www.gob.pe/uploads/document/file/3293229/RD%201114-2022.pdf.pdf

Resolución Directoral N° 2377-2018-JUS/DGTAIPD-DPDP. (24 de setiembre de 2018). En el Expediente N° 011-2018-PTT. Dirección de Protección de Datos Personales de la Autoridad Nacional de Protección de Datos Personales. https://cdn.www.gob.pe/uploads/document/file/605996/RD-2377-2018-DPDP.pdf

Resolución Directoral N° 925-2018-JUS/DGTAIPD-DPDP. (02 de mayo de 2018). En el Expediente N° 021-2017-PTT. Dirección de Protección de Datos Personales de la Autoridad Nacional de Protección de Datos Personales. https://cdn.www.gob.pe/uploads/document/file/2888738/RD-925-2018-DPDP.pdf.pdf?v=1646660182

IX.ANEXOS

Anexo A: Matriz de Consistencia

Uso de redes sociales y vulneración del Derecho a la protección de datos personales en estudiantes de la Institución Educativa N° 1138 "José Abelardo Quiñones", 2024

<table>
<tr><th>PROBLEMAS</th><th>HIPÓTESIS</th><th>OBJETIVOS</th><th>VARIABLES</th><th>DIMENSIONES</th><th>INDICADORES</th><th>METODOLOGÍA</th></tr>
<tr><td><u>Problema General</u>
¿Qué relación existe entre el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024?</td><td><u>Objetivo General</u>
Determinar la relación existente entre el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024</td><td><u>Hipótesis General</u>
Existe una relación significativa entre el uso de redes sociales y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024</td><td>Variable 1:

Uso de redes sociales.</td><td>Facebook

TikTok</td><td>- Configuración
- Interacción</td><td rowspan="4">Tipo de Investigación: Cuantitativa

Alcance de Investigación: Correlacional

Diseño de Investigación: No Experimental-Transversal.

Población: 187 estudiantes.

Muestra: Censal

Técnica de recolección de datos: Encuesta

Instrumento: Cuestionario

Técnica de Procesamiento de datos: Coeficiente Rho de Spearman

Análisis de Datos: Estadístico SPSS- 27</td></tr>
<tr><td><u>Problemas Específicos</u>

¿Qué relación existe entre el uso de la red social Facebook y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024?</td><td><u>Objetivos Específicos</u>

Determinar la relación existente entre el uso de la red social Facebook y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N° 1138 José Abelardo Quiñones, 2024</td><td><u>Hipótesis Específicas</u>

Existe una relación significativa entre el uso de la red social Facebook y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, 2024</td><td rowspan="2">Variable 2:

Vulneración del Derecho a la protección de datos personales.</td><td>Protección Jurídica</td><td>- Consentimiento
- Perjuicio</td></tr>
<tr><td>¿Qué relación existe entre el uso de la red social TikTok y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, 2024?</td><td>Determinar la relación existente entre el uso de la red social TikTok y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, 2024.</td><td>Existe una relación significativa entre el uso de la red social TikTok y la vulneración del Derecho a la protección de datos personales en estudiantes de la I.E. N°1138 José Abelardo Quiñones, 2024.</td><td>Mecanismos de Prevención</td><td>- Nivel Institucional
- Entorno familiar</td></tr>
</table>

Anexo B: Instrumento de recolección de datos

Universidad Nacional Federico Villarreal

CUESTIONARIO SOBRE EL USO DE REDES SOCIALES Y VULNERACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES

A.) PRESENTACIÓN

Estimado participante se te solicita tu valiosa colaboración para completar el presente cuestionario que forma parte de una investigación sobre el uso de las redes sociales y su afectación al Derecho a la protección de datos personales de los estudiantes de la I.E. N° 1138 José Aberlardo Quiñones, 2024.

Quisiera pedir tu ayuda para que contestes algunas preguntas que no te tomarán mucho tiempo.

B.) INSTRUCCIONES

Se te presentarán algunas preguntas y afirmaciones, por favor te pido que contestes a todas ellas con la mayor sinceridad posible, marcando un aspa "**X**" solo en una de las cinco opciones de respuesta. **No hay respuestas correctas o incorrectas**. Recuerda: **NO** debes marcar dos opciones.

Nota de confidencialidad: Tus respuestas serán anónimas y confidenciales. En ningún momento se te solicitará tus nombres. La información que se obtenga solo se utilizará para fines académicos.

De antemano: ¡MUCHAS GRACIAS POR TU COLABORACIÓN!

Antes de comenzar:

¿Qué son los datos personales?

Es toda aquella información que permite identificarte, como por ejemplo: tu nombre y apellidos, fotografías o videos de ti, tu fecha de nacimiento, tu dirección, tu número de teléfono, tu voz, creencias religiosas, entre otros.

- **Edad del participante:** _____

- A continuación, se te presentan algunas preguntas, por favor respóndelas marcando con un aspa (x) en alguno de los casilleros que se ubican en la columna derecha.

VARIABLE 1: USO DE REDES SOCIALES						
	INDICADORES	**Siempre**	**La mayoría de las veces sí**	**Algunas veces sí, algunas veces no**	**La mayoría de las veces no**	**Nunca**
DIMENSIÓN: FACEBOOK	**CONFIGURACIÓN**					
	1. ¿Sueles incluir tus nombres completos como nombre de usuario para identificarte en Facebook?					
	2. ¿Sueles configurar tu perfil de Facebook en modo público?					
	3. ¿Sueles añadir tu número de teléfono en tu perfil de Facebook?					
	4. Cuando configuras tu privacidad en Facebook ¿Permites que los motores de búsqueda como Google enlacen tu perfil de Facebook?					
	INTERACCIÓN					
	5. Cuando navegas en Facebook ¿Aceptas solicitudes de amistad de personas desconocidas?					
	6. Cuando navegas en Facebook ¿Compartes tus datos personales (imágenes personales, dirección, número de teléfono, etc.) con personas desconocidas?					
	7. Cuando navegas en Facebook ¿Compartes tus datos personales en grupos abiertos al público?					
	8. Cuando navegas en Facebook ¿Sueles publicar fotografías o videos que te identifican en tu perfil de Facebook?					
	9. En las publicaciones que realizas en Facebook ¿Compartes información de tu ubicación?					
DIMENSIÓN: TIKTOK	**CONFIGURACIÓN**					
	10. ¿Sueles configurar tu cuenta de TikTok en modo público?					
	11. ¿Permites que TikTok acceda a la lista de contactos de tu teléfono personal?					
	12. ¿Sueles activar la opción de TikTok que permite que cualquier persona del mundo pueda enviarte mensajes directos?					
	13. ¿Sueles activar la opción de TikTok que permite que otras personas descarguen los videos o fotografías que publicas?					
	INTERACCIÓN					
	14. Cuando navegas en TikTok ¿Aceptas solicitudes de seguimiento de personas desconocidas?					
	15. Cuando navegas en TikTok ¿Compartes tu información personal con usuarios desconocidos?					
	16. Cuando navegas en TikTok ¿Subes contenidos en los que expones públicamente imágenes que te identifican?					
	17. Cuando navegas en TikTok ¿Subes contenidos en los que expones públicamente imágenes que identifican a tus familiares directos (papá, mamá, hermanos)?					

- Ahora, indica en qué grado estás de acuerdo o en desacuerdo con cada una de las siguientes afirmaciones, poniendo una marca (como esta: X) en cualquiera de las opciones**.**

VARIABLE 2: VULNERACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES						
	INDICADORES	**Muy de acuerdo**	**De acuerdo**	**Ni de acuerdo ni en desacuerdo**	**En desacuerdo**	**Muy en desacuerdo**
DIMENSIÓN: PROTECCIÓN JURÍDICA	**CONSENTIMIENTO**					
	18.Considero que mis datos personales han sido recopilados sin mi autorización por otros usuarios de redes sociales.					
	19. Considero que mis datos personales han sido difundidos públicamente en redes sociales sin mi autorización.					
	PERJUICIO					
	20. En algún momento me he sentido avergonzado por la difusión de mis datos personales sin mi autorización en redes sociales.					
	21. En algún momento me he sentido obligado a hacer cosas que no quería solo para evitar que mis datos personales sean divulgados en redes sociales.					
	22. En algún momento he sentido que he sido víctima de acoso escolar por la difusión sin mi autorización de mis datos personales en redes sociales.					
DIMENSIÓN: MECANISMOS DE PREVENCIÓN	**INSTITUCIONAL**					
	23. Considero que ninguna entidad pública o privada me ha brindado información sobre cómo proteger mis datos personales en las redes sociales.					
	24. Considero que en mi centro educativo no me han brindado información sobre la forma de proteger mis datos personales en las redes sociales.					
	25. Considero que no existen medios sencillos y fáciles de usar para denunciar la difusión en redes sociales de contenido íntimo sobre mí.					
	ENTORNO FAMILIAR					
	26. Considero que ninguno de mis padres o tutores me han brindado información sobre la forma de proteger mis datos personales en las redes sociales.					

¡GRACIAS POR PARTICIPAR!

VALORACIÓN:

SIEMPRE	LA MAYORÍA DE LAS VECES SÍ	ALGUNAS VECES SÍ, ALGUNAS VECES NO.	LA MAYORÍA DE LAS VECES NO	NUNCA
1	**2**	**3**	**4**	**5**

MUY DE ACUERDO	DE ACUERDO	NI DE ACUERDO, NI EN DESACUERDO	EN DESACUERDO	MUY EN DESACUERDO
1	**2**	**3**	**4**	**5**

Anexo C: Fichas de validación del instrumento a través de juicio de expertos

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
FACULTAD DE DERECHO Y CIENCIA POLÍTICA
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTO

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: JORGE ARTURO ANDUJAR MORENO
1.2. GRADO ACADÉMICO: DOCTOR EN DERECHO
1.3. INSTITUCIÓN QUE LABORA: DOCENTE UNFV
1.4. TÍTULO DE LA INVESTIGACIÓN: USO DE REDES SOCIALES Y VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN ESTUDIANTES DE LA I.E 1138 JAD. 2024
1.5. AUTOR DEL INSTRUMENTO: KAREN JAZMIN GUZMAN MEZA
1.6. NOMBRE DEL INSTRUMENTO: CUESTIONARIO
1.7. CRITERIOS DE APLICABILIDAD:

a. De 01 a 09: (No válido, reformular) b. De 10 a 12: (No válido, modificar)
c. De 12 a 15: (Válido, mejorar) d. De 15 a 18: (Válido, precisar)
e. De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALIATIVOS/CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy bueno (15-18)	Excelente (18-20)
		a	b	c	d	e
1.CLARIDAD	Está formulado con lenguaje apropiado.					19
2.OBJETIVIDAD	Esta expresado con conductas observables.					19
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					19
4.ORGANIZACIÓN	Existe una organización y lógica.					19
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad.					19
6.INTENCIONALIDAD	Adecuado para valorar los aspectos del estudio.					19
7.CONSISTENCIA	Basado en el aspecto teórico, práctico y del tema de estudio					19
8.COHERENCIA	Entre las variables, dimensiones, indicadores e ítems.					19
9.METODOLOGÍA	La estrategia responde al propósito del estudio.					19
10.CONVENIENCIA	Crea nuevas pautas para la investigación y construcción de teorías.					19
Sub Total						
TOTAL						

VALORACIÓN CUANTITATIVA (Total x 0.4): .....
VALORACIÓN CUALITATIVA: EXCELENTE
OPINIÓN DE APLICABILIDAD: VÁLIDO PARA APLICAR

Lugar y fecha: LIMA 26.06.24

Firma del experto:

DNI: 07270377

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
FACULTAD DE DERECHO Y CIENCIA POLÍTICA
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTO

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: JESUS WILFREDO MUNIVE TAQUIA
1.2. GRADO ACADÉMICO: MAESTRO EN DERECHO CONSTITUCIONAL
1.3. INSTITUCIÓN QUE LABORA: DOCENTE UNFV
1.4. TÍTULO DE LA INVESTIGACIÓN: USO DE REDES SOCIALES Y VULNERACIÓN DEL DERECHO A LA PROTECCION DE DATOS PERSONALES EN ESTUDIANTES DE LA I.E N°1138 JA. 2024
1.5. AUTOR DEL INSTRUMENTO: KAREN JARMIN GUZMAN MEZA
1.6. NOMBRE DEL INSTRUMENTO: CUESTIONARIO SOBRE EL USO DE LAS REDES SOCIALES Y LA VULNERACIÓN A LA PROTECCIÓN DE DATOS PERSONALES.
1.7. CRITERIOS DE APLICABILIDAD:

a. De 01 a 09: (No válido, reformular) b. De 10 a 12: (No válido, modificar)
c. De 12 a 15: (Válido, mejorar) d. De 15 a 18: (Válido, precisar)
e. De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALIATIVOS/CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy bueno (15-18)	Excelente (18-20)
		a	b	c	d	e
1.CLARIDAD	Está formulado con lenguaje apropiado.					20
2.OBJETIVIDAD	Esta expresado con conductas observables.					20
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					20
4.ORGANIZACIÓN	Existe una organización y lógica.					20
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad.					20
6.INTENCIONALIDAD	Adecuado para valorar los aspectos del estudio.					20
7.CONSISTENCIA	Basado en el aspecto teórico, práctico y del tema de estudio					20
8.COHERENCIA	Entre las variables, dimensiones, indicadores e ítems.					20
9.METODOLOGÍA	La estrategia responde al propósito del estudio.					20
10.CONVENIENCIA	Crea nuevas pautas para la investigación y construcción de teorías.					20
Sub Total						
TOTAL						

VALORACIÓN CUANTITATIVA (Total x 0.4): .....
VALORACIÓN CUALITATIVA: EXCELENTE
OPINIÓN DE APLICABILIDAD: VÁLIDO PARA APLICAR

Firma del experto:
DNI: 09198891

Lugar y fecha: Lima, Lima 26.06.24

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
FACULTAD DE DERECHO Y CIENCIA POLÍTICA
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTO

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: JOSE ESTELA HUAMAN
1.2. GRADO ACADÉMICO: DOCTOR EN DERECHO
1.3. INSTITUCIÓN QUE LABORA: DOCENTE UNFV
1.4. TÍTULO DE LA INVESTIGACIÓN: USO DE REDES SOCIALES Y VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN ESTUDIANTES DE I.E N°1138 - JAR, 2024
1.5. AUTOR DEL INSTRUMENTO: Karen Jazmin Guzman Heza.
1.6. NOMBRE DEL INSTRUMENTO: Cuestionario
1.7. CRITERIOS DE APLICABILIDAD:

a. De 01 a 09: (No válido, reformular) b. De 10 a 12: (No válido, modificar)
c. De 12 a 15: (Válido, mejorar) d. De 15 a 18: (Válido, precisar)
e. De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALIATIVOS/CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy bueno (15-18)	Excelente (18-20)
		a	b	c	d	e
1.CLARIDAD	Está formulado con lenguaje apropiado.					19
2.OBJETIVIDAD	Esta expresado con conductas observables.					19
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					19
4.ORGANIZACIÓN	Existe una organización y lógica.					19
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad.					19
6.INTENCIONALIDAD	Adecuado para valorar los aspectos del estudio.					19
7.CONSISTENCIA	Basado en el aspecto teórico, práctico y del tema de estudio					19
8.COHERENCIA	Entre las variables, dimensiones, indicadores e ítems.					19
9.METODOLOGÍA	La estrategia responde al propósito del estudio.					19
10.CONVENIENCIA	Crea nuevas pautas para la investigación y construcción de teorías.					19
Sub Total						
TOTAL						

VALORACIÓN CUANTITATIVA (Total x 0.4): .....
VALORACIÓN CUALITATIVA: EXCELENTE
OPINIÓN DE APLICABILIDAD: VÁLIDO PARA APLICAR

Firma del experto:
DNI: 06711521

Lugar y fecha: Lima, LIMA, 02.07.24

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
FACULTAD DE DERECHO Y CIENCIA POLÍTICA
FICHA DE VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
JUICIO DE EXPERTO

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: DR. WALTER MAURICIO ROBLES ROSALES.
1.2. GRADO ACADÉMICO: DOCTOR EN DERECHO
1.3. INSTITUCIÓN QUE LABORA: DOCENTE - UNFV
1.4. TÍTULO DE LA INVESTIGACIÓN: USO DE REDES SOCIALES Y PROTECCIÓN DE DATOS PERSONALES EN LOS ESTUDIANTES DE LA I.E. N° 1138 JAQ. 2024
1.5. AUTOR DEL INSTRUMENTO: KAREN JAZMIN GUZMAN MEZA
1.6. NOMBRE DEL INSTRUMENTO: CUESTIONARIO
1.7. CRITERIOS DE APLICABILIDAD:

a. De 01 a 09: (No válido, reformular) b. De 10 a 12: (No válido, modificar)
c. De 12 a 15: (Válido, mejorar) d. De 15 a 18: (Válido, precisar)
e. De 18 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALIATIVOS/CUANTITATIVOS	Deficiente (01-09)	Regular (10-12)	Bueno (12-15)	Muy bueno (15-18)	Excelente (18-20)
		a	b	c	d	e
1.CLARIDAD	Está formulado con lenguaje apropiado.					20
2.OBJETIVIDAD	Esta expresado con conductas observables.					20
3.ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					20
4.ORGANIZACIÓN	Existe una organización y lógica.					20
5.SUFICIENCIA	Comprende los aspectos en cantidad y calidad.					20
6.INTENCIONALIDAD	Adecuado para valorar los aspectos del estudio.					20
7.CONSISTENCIA	Basado en el aspecto teórico, práctico y del tema de estudio					20
8.COHERENCIA	Entre las variables, dimensiones, indicadores e ítems.					20
9.METODOLOGÍA	La estrategia responde al propósito del estudio.					20
10.CONVENIENCIA	Crea nuevas pautas para la investigación y construcción de teorías.					20
Sub Total						
TOTAL						

VALORACIÓN CUANTITATIVA (Total x 0.4): .....
VALORACIÓN CUALITATIVA: EXCELENTE
OPINIÓN DE APLICABILIDAD: VALIDO PARA APLICAR

Lugar y fecha: Lima, 02/07/24

Firma del experto:
DNI: 15631358

Anexo D: Resultados del coeficiente de confiabilidad del instrumento

Para el nivel de confiabilidad del instrumento se aplicó una prueba piloto a 30 estudiantes, con el fin de validar los ítems; luego, los resultados obtenidos se ingresaron al programa SPSS-27 y se procedió a determinar la consistencia interna empleando el coeficiente de confiabilidad Alfa de Cronbach, el mismo que toma valores entre 0 y 1. Cuanto más se aproxime al 1, mayor será la fiabilidad del instrumento.

Tabla D1

Estadística de fiabilidad

Variable	Alfa de Cronbach	Ítems	Muestra piloto
Uso de redes sociales	0.962	17	30
Vulneración del Derecho a la protección de datos personales	0.934	9	30

Nota. Elaboración propia en base a los resultados del programa spss vs 27

El análisis de confiabilidad de las variables en la muestra piloto revela que la variable uso de redes sociales presenta un alfa de Cronbach de 0.962 con 17 ítems y una muestra de 30 participantes, indicando una excelente consistencia interna. De manera similar, la variable vulneración del Derecho a la protección de datos personales muestra un alfa de Cronbach de 0.934 con 9 ítems y también una muestra de 30 participantes, lo que sugiere una elevada confiabilidad en sus mediciones. Estos resultados reflejan que ambas variables tienen una alta consistencia interna, garantizando que los ítems utilizados en el cuestionario son confiables para evaluar las dimensiones correspondientes.

Anexo E: Base de datos

MUESTRA	V1: USO DE REDES SOCIALES																	V2:VULNERACIÓN DEL DERECHO A LA								
	D1: FACEBOOK									D2: TIKTOK								D1: PROTECCIÓN					D2: MECANISMOS			
	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	I18	I19	I20	I21	I22	I23	I24	I25	I26
1	4	5	5	1	2	2	2	4	3	5	4	5	5	5	4	5	3	4	4	4	3	4	3	2	4	4
2	2	5	2	2	3	2	1	2	5	2	4	2	1	3	2	1	1	2	1	2	2	1	3	2	2	2
3	2	1	1	1	2	1	1	2	1	5	2	2	3	3	1	2	2	1	1	2	2	1	3	5	2	4
4	2	2	2	1	2	1	1	5	4	5	1	1	4	1	1	4	1	1	1	2	2	1	3	5	2	5
5	2	2	1	2	1	1	1	2	1	5	3	3	3	2	1	4	1	4	4	4	4	4	5	2	4	2
6	2	5	5	2	4	1	2	1	5	1	2	2	1	3	1	1	1	4	1	2	1	1	1	2	2	2
7	4	5	5	1	1	1	1	4	1	4	2	3	3	4	1	3	1	3	2	2	2	2	1	1	2	2
8	2	2	1	1	2	1	1	2	1	2	1	1	2	3	1	3	3	1	1	1	1	1	3	2	2	2
9	4	2	1	1	2	1	1	4	1	1	1	1	3	3	1	1	1	2	2	2	2	2	1	1	1	1
10	4	5	5	1	1	1	1	4	5	3	3	1	1	1	1	2	3	2	1	1	1	1	2	1	4	2
11	4	5	5	4	3	4	4	2	4	4	4	5	4	5	3	4	4	5	4	3	4	4	4	4	4	5
12	4	5	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	4	4	4	4	4
13	2	1	1	2	2	1	1	2	4	3	1	1	2	2	2	3	2	1	2	2	1	1	4	1	1	1
14	4	5	5	4	3	4	4	4	4	4	4	4	4	5	3	4	3	4	3	4	4	4	4	5	4	5
15	3	5	5	4	3	4	4	5	4	5	4	4	5	4	4	5	3	4	4	4	4	4	4	5	4	4
16	4	5	4	4	4	4	4	4	4	4	4	4	4	4	3	4	3	4	5	4	4	5	5	4	4	4
17	4	5	2	3	4	4	2	4	4	5	4	4	4	4	4	3	4	5	5	4	4	4	4	4	4	4
18	2	5	5	3	3	4	2	4	4	5	4	2	3	4	4	5	4	4	3	4	5	4	4	5	4	4
19	3	5	5	5	2	3	3	3	4	5	4	5	5	4	3	5	5	4	5	4	3	4	4	4	5	4
20	4	2	5	5	1	1	1	2	4	3	4	2	1	1	1	1	3	2	1	1	1	2	4	4	4	3
21	2	2	1	2	2	2	2	2	1	5	2	1	2	4	1	2	1	2	2	2	2	2	3	2	2	1
22	2	1	1	1	1	1	2	2	5	5	1	3	1	3	1	1	1	2	2	2	2	2	3	4	4	2
23	4	5	3	4	4	4	4	4	4	5	4	4	4	4	3	4	3	2	5	5	4	3	5	5	5	4
24	4	1	4	1	4	1	1	3	4	5	1	1	4	1	1	4	1	1	1	1	1	1	1	3	4	4
25	4	5	3	3	4	4	5	5	4	3	4	5	4	4	4	5	4	5	4	3	3	3	5	3	4	5
26	4	5	4	3	5	4	4	4	4	5	4	4	4	4	4	3	4	2	5	4	4	4	4	2	4	3
27	4	5	5	4	4	3	4	4	4	4	4	3	4	3	4	4	4	4	4	4	4	3	4	4	4	4
28	2	2	1	2	2	2	3	3	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
29	4	1	1	1	1	1	1	4	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	4	5	5	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4
31	4	5	5	4	5	1	4	4	3	5	5	4	4	3	4	4	4	4	4	4	4	3	4	4	4	4
32	4	5	4	4	4	2	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4
33	2	2	1	3	2	1	1	2	1	1	2	1	2	2	1	1	1	3	2	2	2	2	2	3	1	1
34	4	5	5	5	4	4	4	4	4	5	4	4	5	5	5	4	4	4	5	3	4	4	4	4	4	4
35	4	4	4	5	4	4	2	4	4	5	4	5	4	3	4	4	5	4	4	4	4	5	4	4	5	4
36	4	5	5	5	5	4	5	4	3	4	3	2	5	5	5	3	4	4	5	4	5	4	4	4	4	5
37	5	5	5	3	4	4	3	4	4	5	4	5	4	5	5	4	5	5	4	5	4	4	4	4	4	4
38	4	5	5	4	4	4	4	4	4	5	4	4	5	5	4	3	3	4	4	4	3	4	5	5	4	2
39	5	5	5	4	4	5	4	4	4	1	4	4	4	4	5	4	5	4	4	4	2	4	5	5	4	3
40	4	5	5	4	4	4	4	4	4	5	2	1	5	5	2	3	4	4	4	4	3	4	5	5	4	2
41	4	5	5	4	3	2	2	5	4	4	4	4	5	2	2	4	4	4	4	4	3	4	5	4	2	3
42	1	3	1	2	1	1	1	2	1	1	2	1	1	1	1	3	1	3	2	4	1	1	1	1	2	2
43	4	5	4	3	2	4	3	4	2	3	4	3	4	5	4	4	4	5	3	4	3	5	4	4	4	5
44	4	5	4	3	4	4	3	3	4	5	5	4	5	4	3	4	5	4	5	4	5	4	5	4	4	2
45	4	5	5	4	4	4	4	4	4	5	4	4	4	5	2	4	5	3	4	4	4	4	5	5	4	5
46	4	5	4	4	5	4	3	2	4	5	4	4	4	3	4	5	5	4	4	4	4	4	5	4	4	3
47	5	5	5	4	2	4	4	4	4	5	4	4	3	4	4	4	5	4	4	4	4	4	5	4	4	4
48	4	5	5	5	5	4	2	4	4	4	4	3	2	4	4	4	5	4	4	5	3	5	4	5	4	2
49	5	5	5	4	3	4	4	4	4	5	4	4	3	5	4	3	4	5	4	4	4	4	5	5	5	5
50	4	5	5	5	5	4	4	4	3	4	4	5	4	4	4	4	4	4	4	5	4	4	5	4	2	3
51	4	5	5	4	5	4	4	3	4	5	4	4	4	4	4	5	4	5	4	4	4	4	5	5	5	5
52	4	5	4	4	3	2	4	4	4	4	5	4	4	4	4	5	4	4	4	4	4	3	4	4	4	3
53	4	5	5	3	2	4	4	4	4	5	5	4	4	4	3	4	4	4	4	4	4	4	4	4	5	3
54	5	5	5	4	4	4	4	5	5	5	4	4	5	4	4	4	4	4	4	4	4	5	4	4	4	4
55	1	2	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	2	1	1	1	1	4	1	2
56	5	5	4	5	4	3	4	4	4	5	5	4	4	4	4	4	4	4	4	4	4	3	4	4	5	2
57	4	5	4	4	4	4	2	4	2	5	4	5	4	4	4	5	4	4	5	4	4	5	4	4	4	5
58	4	5	5	3	4	4	4	4	4	3	4	4	5	4	4	4	5	4	4	3	4	4	4	4	4	3
59	4	5	4	5	4	4	4	3	4	4	4	4	5	3	4	4	3	4	3	4	2	4	4	4	4	3
60	4	5	5	4	5	4	4	4	5	4	4	4	4	4	4	4	4	3	4	4	4	4	4	3	4	4

61	5	2	3	3	5	1	1	4	1	1	1	1	1	1	1	1	1	2	4	4	1	1	3	1	2	1
62	3	3	3	1	3	4	3	4	3	5	5	4	3	4	3	1	1	5	3	2	1	2	3	2	3	2
63	4	5	5	4	3	4	4	4	4	5	4	4	5	5	5	4	5	2	5	5	4	4	5	4	4	4
64	3	5	4	4	4	2	4	4	4	4	3	4	4	4	3	4	4	4	4	4	4	3	4	4	4	5
65	4	5	5	5	5	5	4	4	2	4	4	5	5	5	4	4	4	4	4	4	5	4	4	3	4	4
66	4	5	4	4	4	4	4	4	5	4	5	5	5	5	4	4	5	4	5	4	5	4	5	4	4	3
67	2	5	4	2	4	4	4	4	3	4	4	3	4	4	5	4	3	3	3	4	4	4	5	4	5	3
68	3	5	4	4	4	4	4	4	4	4	5	4	4	3	4	4	4	4	4	5	4	5	4	4	4	4
69	1	3	1	1	4	1	2	4	1	4	1	1	1	5	1	2	1	2	1	5	4	2	3	2	3	4
70	4	5	5	5	4	4	5	4	4	5	5	5	4	4	4	4	4	5	4	4	4	4	5	4	4	3
71	4	3	4	4	4	4	4	3	4	5	5	4	2	4	4	4	4	3	4	2	4	4	4	4	4	4
72	2	1	3	1	3	1	1	2	2	3	1	1	2	3	1	1	1	3	2	2	2	1	4	3	5	2
73	5	4	3	4	4	5	4	4	4	5	5	2	4	4	4	4	4	4	3	4	4	4	4	5	4	5
74	5	5	5	5	5	4	2	4	4	5	4	5	5	4	4	4	4	3	4	4	4	3	4	4	4	4
75	3	5	5	5	4	4	5	2	4	3	4	4	5	4	4	4	4	4	4	5	4	4	5	4	5	4
76	4	5	5	5	4	4	5	2	4	5	4	4	4	5	4	4	5	4	4	2	4	4	5	4	4	4
77	5	5	4	4	4	4	4	4	3	5	4	3	4	4	4	5	5	5	4	3	4	4	5	4	4	3
78	4	5	5	5	4	4	4	4	5	5	4	5	4	4	4	4	4	3	4	4	4	4	4	4	5	3
79	4	5	5	2	5	4	4	4	4	5	5	5	5	5	5	5	5	4	5	2	5	4	4	5	4	5
80	5	1	1	1	1	1	1	3	1	1	2	2	1	1	1	1	1	3	1	1	1	1	4	1	1	3
81	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	3	5	4	4	4
82	4	4	5	4	4	4	4	4	5	4	5	4	3	2	4	4	4	4	4	4	5	4	4	5	4	2
83	4	5	5	5	4	4	4	5	5	5	4	4	4	5	4	4	5	5	4	4	3	4	4	4	4	4
84	4	4	5	5	4	4	4	5	4	5	4	5	4	5	4	4	5	4	5	4	5	4	4	5	4	3
85	4	3	5	4	4	4	4	5	4	5	5	5	5	5	5	5	4	4	5	4	5	3	4	5	4	3
86	4	5	5	4	5	4	4	4	4	5	5	2	4	3	4	4	4	5	4	3	4	4	1	4	4	4
87	4	5	5	3	4	4	4	4	3	5	4	5	4	4	4	5	4	3	4	4	5	4	5	4	4	3
88	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	1	4	1
89	4	5	4	3	4	4	5	4	4	3	4	4	4	4	4	4	4	3	4	4	5	4	4	4	3	4
90	2	2	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	3	4	2	1
91	4	4	4	4	5	3	4	5	3	5	5	5	5	5	2	5	5	4	5	4	5	4	5	4	4	4
92	4	2	1	1	1	1	1	1	5	1	1	1	1	2	1	1	1	2	2	2	2	2	2	2	2	2
93	4	5	4	4	4	5	5	3	4	4	4	4	4	4	2	3	4	4	4	4	5	4	5	4	3	4
94	4	4	5	5	3	4	4	5	5	4	5	5	5	4	4	4	4	4	4	4	3	4	2	4	4	4
95	1	5	4	3	4	4	2	2	4	5	3	4	4	4	4	5	5	4	4	4	5	4	5	2	4	4
96	4	5	5	4	4	3	3	4	4	4	4	5	5	5	4	5	5	4	4	4	4	5	4	5	5	4
97	3	5	1	1	1	4	1	1	1	1	1	1	1	1	1	1	1	5	4	3	1	1	1	1	1	1
98	3	4	5	4	4	4	4	4	4	5	5	5	5	5	5	5	5	4	4	5	5	5	4	4	4	4
99	3	4	5	4	4	4	4	4	5	4	5	3	4	4	4	4	1	3	4	4	5	4	5	4	5	
100	4	5	5	5	5	4	3	5	4	5	2	4	4	4	2	4	4	2	4	4	4	4	5	4	3	5
101	3	4	5	5	4	5	4	5	4	5	4	4	4	5	4	4	5	5	5	4	5	4	5	4	4	4
102	2	4	5	4	4	4	5	4	5	5	5	4	5	4	5	4	4	5	4	5	4	5	4	4	5	4
103	3	5	5	5	4	4	5	4	4	5	4	4	4	5	4	4	5	4	4	4	4	5	4	4	4	4
104	4	5	5	4	4	4	4	5	4	5	4	5	4	4	5	4	4	4	4	4	5	4	3	4	4	4
105	4	5	5	3	4	4	3	2	4	5	5	4	4	4	4	4	5	5	5	4	5	4	5	5	3	4
106	4	5	5	4	5	4	4	4	4	5	5	4	4	4	4	4	4	4	2	4	4	4	4	4	4	4
107	4	5	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	5	5	4	4	5	4	5	4
108	4	4	4	2	4	3	2	4	4	2	3	4	4	5	4	4	4	2	5	4	3	4	4	4	5	4
109	1	1	2	3	1	1	1	2	1	3	3	1	1	2	2	1	1	3	2	4	2	2	2	1	2	1
110	4	3	4	4	4	4	4	5	4	5	4	4	4	4	4	3	4	5	5	4	5	5	5	4	5	5
111	4	5	5	2	4	5	4	4	5	5	5	5	4	4	4	4	4	5	5	5	5	5	5	5	5	5
112	4	5	1	3	4	4	4	5	4	5	5	5	5	4	5	3	4	5	2	4	4	5	4	5	5	4
113	4	4	4	4	4	4	2	4	4	5	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4
114	4	5	4	4	4	5	4	5	4	4	4	5	5	4	4	3	5	4	3	4	4	4	3	4	4	2
115	4	5	2	4	2	4	4	5	4	5	4	4	5	5	4	4	5	4	4	4	5	5	4	3	3	4
116	3	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	3	1	1	1	2	2	2	4
117	4	5	3	5	5	4	4	3	4	1	4	4	4	4	5	5	5	4	4	5	4	5	5	5	2	4
118	1	1	1	1	2	1	1	4	1	1	3	1	1	3	1	1	1	1	1	1	1	1	3	1	1	2
119	4	5	4	3	4	4	4	5	4	5	4	4	4	5	4	5	5	2	4	4	3	3	4	5	5	4
120	5	5	5	4	4	4	4	5	4	5	4	4	5	5	4	3	3	1	4	5	4	5	5	4	5	4

121	4	5	5	4	3	2	5	4	4	3	4	4	5	4	3	4	5	2	2	4	4	5	4	3	5	4
122	4	5	4	4	4	4	4	2	4	5	4	5	5	5	5	4	4	2	2	5	5	5	5	5	5	5
123	4	2	5	2	1	1	1	5	1	2	3	2	3	2	1	1	1	1	1	2	1	1	2	2	2	1
124	2	5	5	5	4	1	1	5	1	4	4	4	4	2	2	4	1	2	1	2	4	2	4	2	2	2
125	1	5	1	1	1	1	1	1	1	5	5	1	5	1	1	5	1	1	2	1	1	1	2	2	2	2
126	5	5	5	5	4	3	3	4	2	5	3	5	4	5	4	5	4	5	3	3	4	4	5	4	4	5
127	4	4	5	5	3	5	5	4	2	5	4	3	4	4	4	5	5	4	3	4	4	5	5	5	4	3
128	4	5	3	4	4	4	4	3	4	5	5	5	5	5	4	4	4	4	4	5	4	4	4	3	4	4
129	5	5	4	5	4	3	4	5	5	5	4	4	4	4	5	5	4	4	4	2	4	4	4	5	5	5
130	4	3	4	4	4	5	5	5	5	5	4	5	4	4	4	4	5	5	4	5	5	5	4	5	5	5
131	4	3	4	4	4	5	4	5	5	4	5	5	5	4	3	4	4	4	2	3	4	4	4	4	5	5
132	4	5	5	5	5	3	4	2	4	4	4	4	5	4	3	4	4	4	5	5	5	5	4	3	4	4
133	4	5	5	5	5	1	4	4	4	4	5	4	4	4	5	4	4	4	2	4	4	4	4	5	4	5
134	5	5	5	3	5	5	4	5	4	5	4	5	4	5	4	3	4	4	4	4	4	4	4	5	4	4
135	5	5	4	2	5	4	4	4	3	4	4	5	4	4	4	4	3	4	3	4	4	5	4	5	4	5
136	5	5	5	5	5	5	5	4	4	5	4	5	4	4	4	4	4	5	4	5	5	5	4	4	4	4
137	4	5	5	4	4	4	4	3	5	4	4	5	4	4	4	5	4	4	4	5	4	3	4	3	5	5
138	5	5	5	2	4	4	4	4	4	5	4	4	2	4	4	4	5	4	5	1	4	4	4	4	5	4
139	4	5	3	1	4	2	4	4	4	5	4	4	3	4	4	5	4	4	5	4	4	4	4	5	5	5
140	4	5	3	4	4	4	2	4	4	5	5	5	5	5	5	4	5	4	3	4	4	4	4	4	5	4
141	4	1	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	4	5	4	4	4
142	1	2	2	1	4	2	1	2	2	3	4	2	2	2	2	2	2	4	3	2	2	1	1	1	1	1
143	4	5	5	5	5	4	5	4	5	5	4	5	4	5	5	4	4	5	5	5	5	4	5	5	5	5
144	4	5	5	4	3	4	5	5	4	5	5		4	4	4	5	4	5	4	3	4	4	4	4	4	4
145	4	5	3	5	4	5	5	4	4	5	4	4	5	4	5	5	5	5	5	4	5	4	5	5	4	5
146	4	5	5	5	5	5	5	4	3	4	4	5	4	5	5	5	5	4	4	4	4	4	5	4	3	4
147	4	4	4	4	2	4	5	5	5	5	4	5	5	4	5	4	4	5	4	5	4	5	4	5	4	5
148	4	5	5	5	4	5	4	4	4	4	5	4	5	4	4	3	4	5	4	5	4	5	4	5	4	5
149	4	5	5	5	4	5	4	4	3	4	4	4	4	5	4	5	5	5	5	5	4	5	5	5	4	4
150	5	5	5	4	5	4	5	4	5	5	5	5	5	5	4	5	4	4	5	4	4	5	4	5	5	5
151	4	5	5	4	5	4	5	4	4	5	4	5	5	5	4	5	5	4	5	5	5	5	5	4	4	5
152	4	5	4	4	4	4	5	4	4	5	5	4	5	4	5	4	5	5	4	5	4	4	4	4	5	5
153	5	5	5	4	5	4	5	4	4	5	4	4	5	5	4	5	5	5	4	5	4	5	4	5	4	5
154	4	5	5	4	5	4	5	4	5	4	4	4	5	4	5	5	5	4	4	4	4	4	4	4	4	4
155	2	5	4	4	5	4	2	4	4	5	4	4	4	4	4	4	4	5	4	5	5	4	5	5	4	5
156	5	5	4	5	4	4	2	5	4	5	4	5	4	5	4	4	5	5	4	5	5	5	5	5	5	5
157	4	5	5	4	5	5	5	5	4	5	4	5	4	5	4	5	4	5	4	5	5	5	5	5	5	4
158	4	5	2	4	2	4	5	4	4	5	4	4	4	4	4	5	4	5	5	5	4	5	4	5	4	5
159	4	5	5	4	5	4	5	5	4	5	5	4	5	4	5	4	5	5	5	5	4	5	4	5	4	5
160	4	5	4	5	4	5	4	4	4	5	4	5	4	5	4	5	4	5	5	5	5	4	5	4	5	4
161	4	5	5	4	5	4	2	4	5	4	5	4	5	4	1	4	4	4	1	4	4	4	4	4	4	4
162	4	4	3	1	2	4	2	4	4	4	4	4	4	4	5	5	4	5	4	2	3	4	4	4	4	4
163	4	5	5	5	5	4	5	4	1	4	4	4	4	4	5	4	4	4	5	5	4	4	4	5	4	4
164	4	5	5	4	5	4	5	4	4	5	2	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4
165	5	5	5	4	5	4	5	5	4	5	5	5	5	5	4	5	4	5	4	4	5	5	5	5	4	5
166	1	2	2	1	4	3	2	2	2	2	3	2	2	2	1	2	2	3	2	2	2	3	2	2	1	1
167	4	4	5	5	5	5	4	3	4	5	5	5	5	4	5	4	5	4	4	3	5	4	5	4	5	5
168	2	1	2	2	2	1	2	2	5	2	2	2	1	2	1	2	2	2	4	2	4	1	1	1	2	4
169	2	1	2	1	1	1	1	5	4	5	4	1	1	1	1	1	2	2	2	2	3	1	2	2	2	2
170	5	5	5	4	5	4	5	4	3	5	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	5
171	5	5	5	5	5	4	4	4	4	5	5	5	5	4	5	4	5	4	5	5	4	5	4	5	4	5
172	4	5	5	5	4	4	4	4	4	5	4	5	4	5	4	4	5	4	4	4	3	5	4	4	4	4
173	4	5	5	5	4	5	4	5	4	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	5	5
174	4	4	5	4	5	4	5	4	5	5	5	5	5	4	4	4	4	5	4	5	4	4	4	4	4	4
175	4	5	5	5	5	4	4	4	4	5	5	4	4	4	5	5	4	5	5	5	5	4	5	5	4	5
176	2	1	1	1	1	1	1	1	2	5	2	1	2	1	2	1	2	2	2	2	2	2	2	2	2	2
177	4	5	5	4	5	4	4	4	4	5	5	5	5	5	5	5	5	4	4	4	4	4	4	4	4	4
178	1	1	1	1	2	4	2	5	1	2	4	1	1	1	1	1	1	1	1	1	2	1	2	1	3	4
179	1	1	1	1	3	1	2	1	4	1	2	4	3	2	2	2	2	2	2	2	1	2	1	4	4	2
180	4	5	5	4	5	4	4	4	4	5	5	5	4	4	4	4	4	5	4	5	4	5	5	4	5	5
181	4	5	5	5	5	5	3	5	4	5	4	5	4	5	5	5	5	4	4	5	5	5	5	5	5	4
182	4	4	5	4	4	5	4	5	4	5	4	4	4	4	5	5	4	4	5	4	5	4	5	4	5	4
183	2	1	2	1	2	1	3	3	4	1	2	2	1	2	2	1	4	1	1	1	2	1	2	4	3	4
184	4	5	5	5	1	2	4	3	2	5	4	4	2	4	4	5	4	4	4	4	3	4	4	5	5	5
185	5	5	5	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	5	5	5	4	4	4	2	4
186	2	1	1	1	2	4	4	1	2	1	1	1	1	4	1	2	1	1	1	2	1	2	2	2	4	2
187	5	4	5	5	5	5	4	3	2	5	1	4	4	4	4	5	4	5	5	5	5	4	5	5	5	5

Anexo F: Carta de Autorización para realización de encuesta

PERÚ | Ministerio de Educación | DIRECCIÓN REGIONAL DE EDUCACIÓN - LIMA | UGEL – 06 ATE-VITARTE I.E. N° 1138 "JOSE A. QUIÑONES"

Jr. Melitón Carbajal N° 200- Valdivieso –Ate Teléfono: 3261784

"Año del Bicentenario, de la consolidación de nuestra independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

AUTORIZACIÓN

Mediante la presente se autoriza a la ***Srta. Karen Jazmín Guzman Meza,*** *identificada con DNI 74804712, en su condición de Bachiller en Derecho por la Universidad Nacional Federico Villarreal, quien solicitó autorización para realizar una encuesta a los estudiantes del 4to y 5to del Nivel Secundaria, ello en razón a que se encuentra realizando un trabajo de investigación titulado "Uso de las redes sociales y Protección de Datos Personales en los estudiantes de la Institución Educativa N°1138 "José Abelardo Quiñones", 2024, encuesta que será realizada para la presentación de su tesis para optar por el título profesional de Abogada.*

Cabe precisar que la aplicación de la encuesta será de 15 minutos aproximadamente, de acuerdo a la disponibilidad de la institución.

Valdivieso,21 de agosto de 2024

Atentamente,

Lic. LEONARDO LUIS FELIX LUNA
DIRECTOR

LIC. LEONARDO FELIX LUNA
DIRECTOR