DEPARTAMENTO DE DERECHO Y CIENCIA POLÍTICA

ESCUELA PROFESIONAL DE DERECHO

ALCANCES JURÍDICOS DE LA LEGISLACIÓN NACIONAL E INTERNACIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES EN LA IMPLEMENTACIÓN DE LA TECNOLOGÍA 5G, PERÚ 2021

Tesis presentada por las Bachilleres en Derecho:

Claudia Zarina Alvarez Valencia

Karol Andrea Llerena Ramos

Para optar el título profesional de Abogado

Asesor: Mtr. Juan Chipana Palomino

AREQUIPA, 2023

Trabajo de Titulación

INFORME DE ORIGINALIDAD

16%	16%	2%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	www.informatica-juridica.com Fuente de Internet	2%
3	vocemdat.com Fuente de Internet	1%
4	repositorio.une.edu.pe Fuente de Internet	<1%
5	repositorio.ucv.edu.pe Fuente de Internet	<1%
6	Submitted to Universidad Anahuac México Sur Trabajo del estudiante	<1%
7	www.trumpf.com Fuente de Internet	<1%
8	cdn.www.gob.pe Fuente de Internet	<1%
9	www.consejotransparencia.cl Fuente de Internet	

AGRADECIMIENTO

A nuestros padres por guiarnos en nuestra formación como personas y recordarnos que la diciplina y constancia nos llevará al camino del éxito.

A nuestro profesor Juan Chipana, por acompañarnos en el camino universitario y mostrarnos el mundo de las nuevas tecnologías.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El estudio presentó como objetivo general analizar los alcances jurídicos en la normativa respecto a protección de datos personales al implementar la Tecnología 5G en Perú, 2021. El enfoque del estudio fue cualitativo con nivel descriptivo de diseño fenomenológico de tipo hermenéutico, también el tipo de estudio resultó socio-jurídica; la población estuvo conformado por 5 especialistas y 70 usuarios de la Tecnología 5G a partir de las cuales se seleccionó como muestra a 3 especialistas y 70 usuarios de la Tecnología 5G de Arequipa; fue empleado por técnica la entrevista, encuesta y análisis documental a través de estos siguientes instrumentos: guía de entrevista, cuestionario y guía de análisis documental. Se obtuvo por resultados que los tres entrevistados coinciden al indicar que se deben aumentar la protección legal de cada dato personal en la ciudadanía conforme las normas internacionales; asimismo, los 70 usuarios encuestados indicaron en su mayoría (74,3%) que las leyes existentes e implementadas en Perú no protegería cada dato personal en el usuario de la Tecnología 5G. Por lo que se concluye que las leyes existentes e implementadas no protegen cada dato personal del usuario de la tecnología 5G en Perú, 2021.

Palabras claves: Tecnología 5G, datos personales, protección, legislación nacional, legislación internacional.

ABSTRACT

The general objective of the research was to analyze the scope of the legislation on the protection of personal data in the implementation of 5G Technology in Peru, 2021. The focus of the study was qualitative with a descriptive level of hermeneutic phenomenological design, with a socio-legal type of study. The population was made up of 5 specialists and 70 users of 5G Technology from which 3 specialists and 70 users of 5G Technology from Arequipa were selected as a sample. The interview, survey and documentary analysis were used as a technique through the interview guide, questionnaire and documentary analysis guide instruments. It was obtained by results that the three interviewees coincide in indicating that the legal protection of the personal data of citizens must be increased in accordance with international standards; Likewise, the 70 users surveyed indicated the majority (74.3%) that the existing and implemented laws in Peru do not protect the personal data of users of 5G Technology. Therefore, it is concluded that the existing and implemented laws do not protect the personal data of users of 5G technology in Peru, 2021.

Key words: 5G technology, personal data, protection, national legislation, international legislation.

INTRODUCCIÓN

La quinta generación de redes móviles es oficializada al mundo En 2018, pero su aparición fue en 2008 *"5G mobile communication systems based on beam-divisionmultiple Access and relays with group cooperation"*. Esta tecnología empezó a utilizarse como prueba en Estados Unidos y Rusia, evidenciando que baja a un 90% del gasto de energía de la red y recursos del 99.99%; sin embargo, Claramente, presenta retos de protección fundamentales, como la confidencialidad, la autenticidad, la integridad y el no repudio, y es vulnerable a los ataques cibernéticos típicos, como el robo de identidad, DoS y sniffing (Rodríguez, 2019). En La Unión Europea existe su Reglamento General para Protección de Datos, donde busca priorizarse la transparencia al momento de tratar cada dato, proteger datos desde los diseños y bajo defecto, imponiendo infracciones por 20 millones de euros hacia quienes no acaten esta normativa (Martínez, 2017). Por otro lado, en Estados Unidos no se tiene la normativa nacional para proteger datos personales, donde las regulaciones solo se desarrollan por algunos de sus estados, demostrando claramente que está atrasado, pese a venirse creando muchas de las empresas de tecnología más fuertes que trabajan actualmente desde internet.

La tesis se estructura en el Capítulo I: Planteamiento del Problema de Investigación conteniendo la formulación del problema de investigación, justificación, objetivos e hipótesis; e instrumentos; en el Capítulo II: Marco Teórico, conteniendo los antecedes de la investigación y bases teóricas; dentro del Capítulo III: Resultados de aplicación de instrumentos de información, conteniendo las entrevistas, encuestas, así como la discusión y, por último, las conclusiones, recomendaciones, referencias bibliográficas y los anexos.

CAPÍTULO I.

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

comunicación viene siendo una de las características centrales de la sociedad, tanto entre los hombres primigenios hasta nuestros días, pero esta cobra aún mayor valor en medio de la era de la información. No obstante, la implementación de la tecnología 5G resulta un desafío para muchos estados al existir una serie de riesgos vinculados a esta nueva generación de comunicaciones inalámbricas. La seguridad del dato personal viene a ser el derecho en cada persona de quienes pasan a recogerse, mantener y procesar datos, permitiéndoles saber qué datos se retienen, usan y corrigen las inexactitudes (CEPAL, 2020). Además, el avance 5G correspondería a la tecnología en comunicación inalámbrica de quinta generación. En comparación con la red de datos 4G actual, puede mejorar las experiencias para navegación del usuario en Internet normales en más de 10 veces (Nieny, 2021).

A nivel mundial, en América Latina, en 2018 los ciberataques aumentaron un 60%, con unos 746.000 asaltos con malware al día, suponiendo una media de 9 asaltos cada segundo (Kaspersky, 2018). La red móvil de quinta generación se lanzó oficialmente en 2018, naciendo realmente en 2008, con el plan *"5G mobile communication systems based on beam-divisionmultiple Access and relays with group cooperation"*. Esta tecnología empezó a utilizarse como prueba en Estados Unidos y Rusia, demostró que disminuye la utilización enérgica de la red en un 90 % y la disponibilidad en un 99,99 %; sin embargo, está claro que presenta problemas sobre seguridad fundamentales como la confidencialidad, la autenticidad, la integridad y el no repudio, y es vulnerable a los ataques cibernéticos típicos como robo, DoS y sniffing (Rodríguez, 2019). Desde la Unión Europea existe el Reglamento General para Protección de Datos, buscándose priorizar la transparencia al momento del trato de datos, proteger datos desde los diseños y bajo defecto, imponiendo infracciones por 20 millones de euros de quienes no acaten esta normativa (Martínez, 2017). Por otro lado, en Estados Unidos no se tiene la normativa nacional para proteger datos personales, donde las regulaciones solo se desarrollan por algunos de sus estados, demostrando claramente que está atrasado, pese a venirse

creando muchas de las empresas de tecnología más fuertes que trabajan actualmente desde internet. En China, no es reconocido el derecho personal sobre la intimidad, al igual que no existe el derecho para proteger datos personales desde su Constitución de 1982, no obstante, en 2016 fue aprobada la norma para seguridad cibernética en el gobierno chino (Duque & Gómez, 2020).

A partir del 2019, la mayoría de los países desarrollados han proporcionado a los usuarios tecnología de red móvil 5G del cual es esperado que la cantidad de usuarios sean 1,700 millones iniciando el 2025. La red 5G se caracterizan por soportar el uso dentro del campo de cada aplicación de internet en cada cosa (conforme las siglas en ingles *IoT*) (Almamoory & Rawdhan, 2021). De esta manera, la tecnología 5G permitiría la navegación bajo velocidad que llega a 10 GBps (gigabytes por segundo), siendo 10 veces más veloz que las mejores propuestas con fibra óptica de la actualidad, con la mencionada rapidez podría descargarse películas completas durante segundos. Asimismo, su latencia (tiempo para responder la red) mejora de forma significativa de modo que, conforme al operador, podría disminuir hasta 5 milisegundos, tiempo que resulta casi imperceptible para los humanos, permitiéndonos así conectarse a tiempo real. Lo mencionado resulta especialmente relevante, por ejemplo, al disminuir el tiempo para responder desde vehículos con autonomía, mejorando la seguridad y confianza de cada peatón de los alrededores y los ocupantes (National Geographic España, 2022).

En el contexto peruano, la tecnología 5G fue implementada en el año 2021 desde el Ministerio de Transportes y Comunicaciones autorizando dos empresas, tanto Entel como Claro, para desplegar la operatividad 5G en la banda de frecuencia existentes. Las bandas de frecuencia que actualmente utilizan instrumentos especiales para transmitir 4G pueden duplicar o triplicar la velocidad; esto es llamado "Parte de la tecnología 5G". Con el tiempo, las antenas 5G se deberán implementar; la misma que aumentará las velocidades en un factor de 10 (ESAN, 2022).

La coyuntura de República Dominicana y Perú, evidencian en su técnica legislativa la incorporación de disposiciones específicas contra el ciberdelito a través de leyes especiales. Por el contrario, en naciones como Nicaragua, Colombia y Panamá tomaron la

decisión de incluir disposiciones sobre ciberdelincuencia en sus códigos penales. En ocasiones, el ciberdelito se concentra en el nombre que se destina a resguardar jurídicamente cada medio electrónico (como en Panamá) o proteger los datos e información (como el caso de Colombia), y dentro del capítulo que trata sobre crímenes de informática (como Costa Rica y Guatemala), sin embargo, demás naciones persiguen el estándar técnico-legislativo conservadores, enfocándose en la creación de "eficiencias equivalentes", con lo cual se ha revisado parcialmente el código, adaptando caracteres clásicos delictivos para que pueda ser aplicado para combatir ciberataques (Vinelli, 2021).

1.1. FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

1.1.1. Problema general

¿Cuáles son los alcances jurídicos de la legislación nacional e internacional sobre protección de datos personales en la implementación de la Tecnología 5G en Perú 2021?

1.1.2. Problemas específicos

1) ¿Cuál es el nivel de conocimiento de los usuarios de la tecnología 5G en las implicancias y riesgos que puede generar sobre sus datos personales?

2) ¿Cuál es el nivel de conocimiento y la responsabilidad de los operadores de servicios, empresas de telecomunicaciones y proveedores de la tecnología 5G en la manipulación de los datos personales de los usuarios?

3) ¿Cuál es el efecto del RGPDP sobre la seguridad de los datos personales en la tecnología 5G en la legislación peruana?

4) ¿Son suficientes las normas que regulan la protección de datos frente a la tecnología 5G en la legislación peruana?

1.2. OBJETIVOS GENERAL Y ESPECÍFICOS

1.3.1. Objetivo general

Analizar los alcances jurídicos de la legislación sobre protección de datos personales en la implementación de la Tecnología 5G en Perú, 2021.

1.3.2. Objetivos específicos

1) Describir el nivel de conocimiento de los usuarios de la tecnología 5G en las implicancias y riesgos que puede generar sobre sus datos personales.

2) Analizar la responsabilidad de los operadores de servicios, empresas de telecomunicaciones y proveedores de la tecnología 5G en la manipulación de los datos personales de los usuarios.

3) Explicar los alcances jurídicos del RGPDP sobre la seguridad de los datos personales en la tecnología 5G en la legislación peruana.

4) Proponer la implementación de una modificatoria en las normas peruanas que regulan la protección de datos personales frente a la tecnología 5G.

1.3. JUSTIFICACIÓN

La importancia académica de la investigación se justifica por contribuir a progresar las limitaciones de vida, sugerir soluciones sobre diversos problemas, el bienestar en las personas junto a la ayuda para desarrollar nuevos profesionales que se dirijan a la investigación.

La importancia jurídica del tema tiene relevancia en vista del arribo del tema a tratar, la tecnología 5G a los países en desarrollo surgiendo la preocupación a desarrollar leyes que regulen a los proveedores, tipificar nuevos delitos informáticos y protección de derechos personales.

La importancia social del tema de investigación es estudiar el comportamiento de los proveedores y la respuesta que presentan los consumidores al arribo de la tecnología 5G relacionado a tratar cada dato personal.

Las principales limitaciones a efectos de desarrollar la presente investigación serán dos: La primera el acceso a la información respecto a la realidad peruana en vista que existe poca información respecto al tema ya que recientemente se ha autorizado dos proveedores que implementan la tecnología 5G que son Claro y Entel. La segunda limitación está relacionado al aspecto económico esto implica desarrollar el estudio para acceder a base de datos especializados como Scopus, Springer, Scielo y otros con el propósito de recopilar información relevante, confiable y actualizada demandan costos que equivalen por cada artículo un monto de entre S/ 150.00 a S/ 200.00.

Los principales alcances jurídicos en el desarrollo de la investigación serán a las teorías y enfoques conceptuales relacionados a la tecnología 5G y proteger cada dato personal bajo la normativa peruana existente. Asimismo, la investigación será viable en vista que se superará las limitaciones oportunamente, en vista que se tendrá accesos a las principales bibliografías tanto virtual como físico, a las que demandan un costo y a los que son de acceso gratuito con al apoyo económico de familiares y con los ingresos mensuales de las investigadoras.

El progreso de la investigación se respetarán las leyes pertinentes relacionados a los derechos del autor para ello se aplicarán adecuadamente la normativa APA en su edición 7ma bajo las cuales serán citados adecuadamente cada autor sobre las ideas utilizadas para esta exploración.

1.4. HIPÓTESIS

1.4.1. Hipótesis general

Dado que la implementado de la Tecnología 5G significa el uso masivo de los datos personales.

Es probable que, nuestro sistema regulatorio requiera ajustes para salvaguardar los datos personales de los usuarios en las nuevas plataformas tecnológicas a raíz de la implementado de la Tecnología 5G.

1.5. METODOLOGÍA JURÍDICA

Este trabajo guarda un enfoque Cualitativo, de acuerdo con Clavijo et al. (2014) presenta por propósito fundamental una estrategia de método cualitativo para describir las propiedades de algún suceso, en otras palabras, no simplemente se trata de enumerar factores o características vinculados con el fenómeno, no es buscar la medición o probar el grado en cómo determinada cualidad está conforme un evento en particular, más bien se trata de encontrar cada cualidad como resulte factible, por lo tanto, se trata de comprender profundamente el objeto por estudiar, más que a precisiones. Las estrategias de éste método significan que los investigadores realizan una serie de actividades diferentes; entrevistas, conversaciones, diferentes formas de observación, notas en campo, registros informativos con herramientas virtuales o clásicas, agrupando ello, son cada actividad utilizada por los sujetos de investigación al tratar obtener información, permitiéndole ser capaz de satisfacer sus preocupaciones sobre los siguientes temas: el entorno del evento y centrar su búsqueda en el entorno natural sin modificar la realidad.

Asimismo, mantiene un nivel descriptivo, donde "Tiene como finalidad especificar propiedades y características de conceptos, fenómenos, variables o hechos en un contexto determinado" (Hernández-Sampieri y Mendoza, 2018, p. 108). Tal como la definición anterior en la presente investigación se describió las variables tecnología 5G y la legislación peruana a partir de la recopilación de datos.

Por otro lado, el método a desarrollarse será hermenéutico, el cual "se enfoca menos en la interpretación del investigador y más en describir las experiencias de los participantes" (Hernández-Sampieri y Mendoza, 2018, p. 549). Con lo indicado, en el estudio dio a conocer cada resultado de analizar los alcances jurídicos de las normas implementadas a fin de proteger los datos personales frente a la tecnología 5G.

De esta manera tendremos una investigación de tipo socio-jurídica, es un tipo de estudio jurídico centrado en la normativa jurídica, centrándose en estudiarlo bajo una perspectiva particular, como ejemplo, un especial énfasis en la eficacia de las normas jurídicas frente a hechos que ocurren en diferentes secuencias, en diferentes momentos de formulación, validez y eficacia. Normas para lograr los fines de los legisladores y el fin del gobierno, y cuando se enfrenten a problemas, sucesos o personas que se regulan. Como tal, es una investigación que estrecha la relación entre los sistemas normativos y la realidad social a lo largo del desarrollo (Clavijo et al., 2014).

Respecto a nuestra población es definido siendo el "Conjunto de todos los casos que concuerdan con determinadas especificaciones" (Hernández-Sampieri y Mendoza, 2018, p. 199). Tal como indica la definición anterior la población se conformó con 5 especialistas y/o profesionales sobre derecho informático y proteger datos personales y 70 usuarios que cuenten con la tecnología 5G.

Para lo anteriormente descrito, se trabajará con una muestra el cual es definido siendo un "Subgrupo del universo o población del cual se recolectan los datos y que debe ser representativo de esta, si se desean generalizar los resultados" (Hernández-Sampieri y Mendoza, 2018, p. 196). La muestra estuvo conformada por 3 especialistas y/o profesionales expertos en derecho informático y protección de datos personales y 70 usuarios que cuentan a la fecha con tecnología 5G.

Con lo expresado en párrafo anterior obtendremos un muestreo, el cual es el procedimiento desarrollado de donde es extraíble una muestra sobre determinada población siendo bajo dos tipos: i) muestreos probabilísticos que viene a ser un procedimiento en la que se aplican formulas estadísticas, es decir un "subgrupo de la población en el que todos los elementos de esta tienen la misma posibilidad de ser elegidos" (Hernández-Sampieri y Mendoza, 2018, p. 200). Y ii) el muestreo no probabilístico o dirigida, que es el procedimiento en la que el investigador a criterio propio selecciona un "subgrupo de la población en la que la elección de los elementos no depende de la probabilidad sino de las características de la investigación" (Hernández-Sampieri y

Mendoza, 2018, p. 200). De la definición, para efectos de este estudio se empleó un muestreo no probabilístico dirigida.

Para ello se empleó una técnica para efectos de recolección de datos el análisis documental, entrevista y encuesta, aplicándose estas mediante los instrumentos cuestionario, guía de entrevista y guía de análisis documental.

El análisis documental viene a ser la operación de un investigador de seleccionar cada idea con mayor relevancia e importante de determinado documento para poder explicar y manifestar de manera clara e inequívoca su contenido, es decir, la información del autor o información contenida desde este. Un análisis de documentos permitiría recuperar o interpretar data para "identificar un documento, proporcionar un punto de acceso en una búsqueda de documentos, indicar su contenido o utilizarse como sustituto de un documento". Pese a que un análisis resulta las operaciones intelectuales, sus resultados pueden plasmarse de diferentes formas, como, resúmenes, ensayos, etc. (Clavijo et al., 2014).

Asimismo, la encuesta viene a ser una técnica no directa para acopiar datos. Resulta una configuración redactada como consultas de donde es obtenida la información referente a ambas variables por estudiar. Resulta la herramienta de investigación para acopiar datos, se puede aplicar en forma presencial o no directa empleando la virtualidad (Sánchez et al., 2018). Por otro lado, la entrevista resulta la técnica de obtención de datos, consistiendo en una conversación de dos individuos: un entrevistador “investigador” junto al entrevistado; es llevada a cabo teniendo como propósito adquirir de ellos información ayudando a resolver la cuestión científica planteada en la investigación realizada. En términos generales, los entrevistados son personas que tienen una buena comprensión del tema de la materia (Clavijo et al., 2014).

De esta manera se hizo uso de un instrumento el cual sería la “herramienta que forma parte de una técnica de recolección de datos. Puede darse como una guía, un manual, un aparato, una prueba, un cuestionario o un test” (Sánchez et al., 2018, p. 78). A

partir de esta definición se empleó como instrumento para acopiar datos una guía de análisis documental, guía de entrevista y cuestionario.

CAPÍTULO II.

MARCO TEÓRICO

3.1. ANTECEDENTES DE LA INVESTIGACIÓN

3.1.1. Desarrollo histórico de la tecnología 5G

Desde 1979, en Japón fue lanzado la primera red móvil a nivel mundial, seguido por la divulgación del sistema de móvil Nórdica de telefonía (NMT) en Finlandia, Dinamarca, Suecia y Noruega, la cual permitió comunicarse mediante voz, pero teniendo calidad baja y sin alguna seguridad. Posteriormente, llegó la red 2G en 1990, siendo un gran avance tecnológico en su momento al brindarle a la telefonía móvil las capacidades para envío de información mediante mensajes de texto, usando protocolos que se dedican a manejar la voz, como el protocolo más comercial, *GSM*.

Para el 2000, llegó la 3ra generación de red móvil, que buscaron brindar una conexión a terminales móviles con internet, empezando a conocerse dentro del mercado la aplicación que se dedican a la comunicación de celulares, con tasas mayores con velocidad en subida y bajada, posibilitando intercambiar información con WhatsApp, correos o distintas apps que simplifica la comunicación, acercando a la población, conforme su utilización (Adachi y Nakajima, 2000).

Ya para el 2010, cuando llegó la cuarta generación de redes móviles, su Core actualmente se constituye por componentes de red, donde fundamentalmente es referida al hardware que se dedica a una específica función para la red móvil, teniendo la carga financiera y operativa demasiado grande y en la actualidad con exigencia tecnológica se encuentra conforme al límite funcional. El terminal móvil utiliza mayor cantidad d datos, bajo las revoluciones por la red 5G es empleado el concepto de virtualizar la red, donde cada elemento de red será alojado de forma virtual para servidores que gestionan las operaciones de cada elemento (Pérez, 2009).

Según 3GPPP, 5G apareció oficialmente en 2018, remontándose el surgimiento a 2008, con el plan "Sistema de comunicación móvil 5G y realización de cooperación grupal

basada en acceso múltiple por división de haces". La empresa de telecomunicaciones pionera en alcanzar velocidades 5G fue la sueca Ericsson; Huawei le siguió con un acuerdo en 2014 con la operadora rusa Megafon buscando la estandarización de tecnología 5G. De manera similar, estados en la UE como Reino Unido y Alemania, al igual que empresas de tecnología como NTTD, Samsung Electronics, Nokia y Alcatel, han estado invirtiendo fuertemente en tests en laboratorios buscando lograr datos críticos que puedan contribuir a la adopción de la tecnología. Poner en práctica. Como resultado, se han formado alianzas estratégicas de operadores telefónicos, universidades y organizaciones de telecomunicaciones en diferentes países, con proyectos que incluyen NGMN Alliance, Mobile Cloud Network, 5GNOW y, en particular, METIS200, donde se permitirá sentar las bases funcionales de 5G, teniendo como niveles de rendimiento estimado que los volúmenes del tráfico resulte superior en 1000 veces al presente, 10 billones de dispositivos en conexión, entre 10 y 100 veces superior de alcanzables tasas de datos del usuario y reducir la latencia de cinco veces al presente, integridad en cada dato e incremento de vida en 10 veces para las baterías (Rodríguez, 2019).

El desarrollo tecnológico ha avanzado mucho a comparación de la generación primera en comunicación móvil, incluyendo la cuarta generación, siendo la más utilizada en las redes móviles modernas, llegando ahora a la generación quinta de dispositivos móviles resulta relevante entender cómo se relacionan las relaciones en red, entendiendo los pasos de red en telecomunicaciones más complejas y sofisticadas que atienden mejor cada necesidad de la ciudadanía, poseyendo nuevas formas de pensar y los componentes que la componen.

La terminología Internet de las cosas se acuñó inicialmente con el británico Kevin Ashton desde el auspicio de 1999 enfocada a Procter & Gamble, describiendo el sistema donde cada objeto del entorno físico pueda conectarse al Internet mediante sensores que automaticen las recopilaciones de datos. aplicado a las cadenas del suministro (Celín, 2019). Según Gartner (2017), habrá 8.400 millones de dispositivos conectados en 2017, un aumento del 31% con respecto a 2016, y alcanzará una gran cantidad con 20.415 millones de dispositivos conectados en 2020; de igual forma, para 2025, el número global de los

dispositivos conectados aumentarán de 20 350 millones en 2017 a 75 440 millones, lo que demuestra que el impacto de la tecnología IoT está creciendo y es enorme.

3.1.2. Evolución histórica de derechos fundamentales para protección de datos personales

Proteger cada dato personal siendo el derecho basico de especial importancia en estos momentos, en una vida encaminada a la alta velocidad de conexión a internet y de las telecomunicaciones, de la globalización hiperconectada y de la masiva emisión de datos y su posterior tratamiento y almacenamiento. Debe entenderse que tiene sentido hablar del derecho a proteger cada dato siendo el derecho básico en la sociedad actual, pero carece de sentido hablar sobre protecciones de datos individuales sin otorgar al sujeto derechos del control, ya que los datos que derivan de la persona resultan parte de este y, por consiguiente, el sujeto nunca deberá perder el control sobre los mismos.

Se trata de un derecho reconocido prácticamente en todos los ordenamientos jurídicos, pero entender el fundamento del derecho de proteger datos requieren necesariamente acceder a los derechos de privacidad, pues estos experimentaron su desarrollo jurídico paralelo al desarrollo de las nuevas tecnologías. Empezando a hablar sobre privacidad se debe remontar en América a finales del siglo XIX, donde dos jóvenes abogados de Boston publicaron en 1890 un artículo en Harvard Law Review; en este, Samuel Warren y Louis Brandeis se refirieron a la privacidad como derecho a “que se nos deje en paz”, Construir sobre los cimientos conocidos hoy del sistema jurídico como los “asuntos de relevancia pública”, impidiendo la publicación de aquello que resulte de interés general o público, siendo una suerte de presunción a favor del control individual sobre la información personal (Talens, 2019).

La coyuntura de Perú, evidencian en su técnica legislativa la incorporación de disposiciones específicas contra el ciberdelito a través de leyes especiales. Por el contrario, en demás países de la región tomaron la decisión de incluir disposiciones sobre ciberdelincuencia en sus códigos penales. En ocasiones, el ciberdelito se concentra en el nombre que se destina a resguardar jurídicamente cada medio electrónico o la protección

de datos e información, y dentro del capítulo que trata sobre crímenes de informática, sin embargo, demás naciones persiguen el estándar técnico-legislativo conservadores, enfocándose en la creación de “eficiencias equivalentes”, con lo cual se ha revisado parcialmente el código, adaptando caracteres clásicos delictivos para que pueda ser aplicado para combatir ciberataques (Vinelli, 2021).

3.2. BASE TEÓRICA

3.2.1. Principios del tratamiento de protección de datos

La protección de datos es el proceso de proteger la información personal o privada de daños, pérdidas o uso indebido y ocuparse de su correcta gestión, procesamiento y almacenamiento. Esto también significa que los datos protegidos deben pertenecer a una persona física (Compliance Aspekte, 2022). Por otro lado, la privacidad de la información forma parte del campo de la protección de datos que se ocupa del correcto manejo de los datos, con énfasis en el cumplimiento de la normativa de protección de datos (Data Privacy Manager, 2023).

Pero la seguridad de los datos es más que proteger la información confidencial de los piratas informáticos. También implica cumplir con las normas que protegen la información personal. Si es dueño de un negocio o toma decisiones, conoce la complejidad y el cambio constante de las regulaciones. Aquí es donde entran los estándares de seguridad de datos (Reflecfiz, 2023).

El cumplimiento de datos se refiere al proceso de garantizar que los datos se recopilen y gestionen de acuerdo con ciertas reglamentaciones o estándares. Es posible que las organizaciones deban cumplir con las leyes de privacidad de datos, las regulaciones de la industria u obligaciones contractuales (Miron, 2022).

La privacidad de los datos se considera un requisito fundamental para la aceptación del consumidor y se puede garantizar a través de la representación, autenticación y autorización del flujo de datos de las actividades realizadas, como la recopilación, retención, procesamiento y transmisión de datos. Los riesgos de privacidad de datos están

directamente relacionados con actividades no autorizadas de recopilación, uso, acceso, almacenamiento e intercambio de datos. Estas actividades pueden ser la causa de la fuga de datos personales y el compromiso de la privacidad del usuario, especialmente en lo que respecta a los datos de salud, ya que tienen diferentes prioridades y son muy valiosos y sensibles. En este sentido, se requieren medidas de protección y seguridad adecuadas (Shahid et al., 2022).

Asimismo, el tratamiento de los datos personales viene a ser cualquier operación o conjunto de operaciones en relación con datos personales, independientemente del proceso utilizado, en particular la recopilación, registro, organización, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o disponibilidad, alineación o combinación, y bloquear, eliminar o destruir (Brevo, 2023).

3.2.1.1. Principios de procesamiento

Según la Comisión Económica para América Latina y el Caribe (2020), los principios elementales de seguridad de dato resultan estos:

Principio de Calidad de los Datos: Cada dato personal debe ser relevante para el fin para el que se utiliza y ser preciso, actual y completo en la medida requerida para ese fin.

Principio para limitar la recopilación de datos: debiendo existir límites para recopilar cada dato personal, y dichos datos deberán lograrse a través de medios justos y legales, con el consentimiento o conocimiento de la persona en cuestión cuando corresponda.

El principio de restricción de uso: el dato personal no será divulgado, proporcionarán ni utilizarán para fines que no estén de acuerdo con especificaciones de la finalidad, salvo consentimientos de los interesados o exigido por las autoridades o por la ley (según sea el caso) para la investigación, la estadística y la planificación social.

Principio de declaración de finalidad: la finalidad de la recolección de datos debe ser expresada máximo al momento donde es producida la recolección, su utilización es limitada a cumplir cada finalidad u otra incompatible con la finalidad original, especificando que la finalidad cambia en cada momento.

Principios de seguridad: Deberán emplearse medidas razonables de seguridad que protejan datos personales del riesgo, ya sea por pérdidas, accesos no autorizados, uso, destrucciones, divulgación o modificar aquellos datos. La limitación para usar y divulgar los datos debe ser reforzadas con medidas de seguridad físicas, como uso de tarjetas de identificación y bloqueo de puertas; organizacionales, como los grados del permiso que accedan a cada dato, especialmente en el sistema informático, siendo el seguimiento y cifrado de cada amenaza de actividad inusual y las respuestas para las mismas.

Principio de participación individual: todo individuo posee el derecho para solicitar las confirmaciones del controlador de datos u otra fuente de que poseen datos personales; los datos relacionados con usted personalmente generan dudas y si su reclamo es exitoso, se le proporcionarán datos corregidos, eliminados, rectificados o completado.

Principio de Transparencia: Debe existir una política general que sea transparente sobre las evoluciones, prácticas y políticas vinculadas a cada dato personal, y debe haber métodos flexibles que determine la naturaleza y existencia de cada dato personal, su finalidad del uso y residencia habitual. identidades de quienes controlan esos datos.

En cuanto a los principios anteriores, debe señalarse que, conforme la legislación nacional, el artículo 11 de la Ley N° 29733 “Ley de Protección de Datos Personales” también establece un conjunto de principios orientados y concuerdan con los principios anteriores. Los ejemplos incluyen los principios de legalidad, consentimiento, propósito, proporcionalidad, calidad, seguridad, cláusulas de apelación y niveles adecuados de protección.

3.2.2. 5G Y REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

3.2.2.1. Iniciativas 5G relacionadas con temas de privacidad

El uso cada vez mayor de aplicaciones y dispositivos que brindan beneficios sociales y económicos a grandes poblaciones procesará grandes cantidades de datos sobre los consumidores a los que las organizaciones no tienen fácil acceso; no obstante, recopila grandes números de data personal y tecnología sofisticada siendo el problema de

seguridad y privacidad. problema relacionado y estos beneficios solo se pueden obtener cuando los dispositivos en los que los consumidores confían están diseñados a través de políticas bien organizadas (Chen et al. 2017).

Las oportunidades que presenta la tecnología 5G presenta vulnerabilidades planteadas con preocupaciones de privacidad y resguardo de cada dato. Unos podrían tratarse, otros solamente logran limitarse al reducir su impacto. Unos podrían argumentar en contra de la idea de las restricciones de seguridad y privacidad, que argumenta que los beneficios económicos de utilizar ciertos datos para informar decisiones económicas superan los costos sociales. Si continúan buscando formas de beneficiarse de la tecnología, lucharán por más poderes, buscando mayor resistencia. regulación. Cada dato generado y las capacidades revelan informaciones personales de la actividad diaria de las personas es un componente clave de analizar la big data diseñado para conocer los patrones y tendencias ocultas (Celín, 2019).

3.2.2.2. Seguridad de datos personales

Las consecuencias de la falta de seguridad pueden ser graves: una empresa puede ver deteriorada su imagen, perder la confianza del consumidor, tener que pagar grandes sumas de dinero para recuperarse de un incidente de seguridad o verse interrumpidas sus actividades. La seguridad de los datos personales es de interés para las personas y organizaciones que procesan los datos.

La seguridad de los datos consta de tres componentes principales: proteger la integridad, la disponibilidad y la confidencialidad de los datos. Por lo tanto, las organizaciones deben evaluar los siguientes riesgos:

- Acceso no autorizado o accidental a los datos: violación de la confidencialidad (p. ej., robo de identidad tras la divulgación de los talones de pago de todos los empleados de la empresa);

- Alteración no autorizada o accidental de datos: violación de la integridad (por ejemplo, acusar falsamente a alguien de mala conducta o delito como resultado de la modificación de los registros de acceso);

- Pérdida de datos o inaccesibilidad de los datos - Infracciones de disponibilidad (p. ej., falla en la detección de interacciones de medicamentos debido a la inaccesibilidad de los registros médicos electrónicos) (Consejo Europe de Protección de Datos [EDPB], 2023).

La protección de los datos, también conocida como privacidad de la información, es un aspecto de la protección de datos que implica el almacenamiento, el acceso, la retención, la inmutabilidad y la seguridad adecuados de los datos confidenciales (Bigelow, 2023). Asimismo, la privacidad de los datos es el principio de que las personas controlan cómo las empresas que tienen acceso a ella recopilan, administran y comparten su información personal. El concepto de privacidad de datos en la era digital generalmente se refiere al manejo de información personal confidencial, también conocida como información de identificación personal e información de salud personal (Stouffer, 2023).

Los consumidores de la tecnología 5G pretende que su dato personal esté seguro, sin compartir y procese y almacene en forma segura buscando no tener intrusión del usuario no autorizado. No obstante, hay opiniones para brindar mayores datos individuales es en beneficio del uso del servicio ofrecido. El consumidor confía en esta tecnología para hacer su vida más fácil y lograr sus objetivos, y la información que brindan puede facilitar el uso de estas herramientas. Cuando los consumidores no saben qué datos son recopilados y quiénes más lo reciben, puede ser complicado tener expectativas respecto a la forma de utilizar cada dato. El consumidor puede desconocer la cantidad de datos recopilados y las implicaciones futuras de esto en su privacidad y la necesidad de protegerlos anterior a que los problemas se vuelvan inmanejables y generalizados (Rodríguez, 2019).

En esta técnica, puede ocasionar distintas clases de paquetes y tráficos variables de diversos dispositivos, incluyendo cada sensor. Por lo tanto, los problemas para controlar activamente esta información en los entornos de red existentes se vuelven cada vez más importante. Además, en términos de seguridad, debido a las limitaciones de rendimiento

del entorno 5G, que está compuesto por dispositivos con especificaciones más bajas, existiría la problemática donde la tecnología de seguridad del dispositivo existente resulta complicada para aplicar. No obstante, al no tomarse la medida adecuada de seguridad, existe el riesgo de fugas de datos, ataques por denegar los servicios en gran escala y manipulación de datos (Chen et al. 2017).

3.2.2.3. Flujos de datos transfronterizos

Si bien algunos datos personales pueden confiarse a terceros y pueden transferirse al exterior, varias medidas de seguridad adoptarán el cifrado, como algoritmos homomórficos y enmascaramiento de datos que proteja datos confidenciales, donde la solución reduciría las disponibilidades del dato sin procesar e incremente el tiempo del procesamiento de datos. Un enfoque eficaz de privacidad deberá respetar las altas disponibilidades del dato sin procesar y reducir la latencia. Otro problema asociado con cada método actual para preservar la privacidad sería su alcance limitado. La mayoría de las veces, cada método solo es adecuado para escenarios de aplicaciones específicas, como atención médica inteligente, red inteligente, red automotriz o intercambio de datos privados con servicios en la nube, por lo que cada medida para proteger datos de privacidad de IoT más completas necesitan más investigación (Celín, 2019).

Como complicaciones en seguridad sobre IoT, podrían clasificares sobre dos categorías: desafíos técnicos y de seguridad. El desafío técnico surgiría de la ubicuidad y heterogeneidad sobre cada dispositivo IoT; por otro lado, el desafío por seguridad se encuentra relacionado con las funciones y principios que deberán aplicarse en la búsqueda de lograr una red segura. Los remanentes de tecnología a menudo están relacionados con las características inalámbricas, de energía, escalabilidad y distribución, donde el desafío de seguridades necesita las capacidades para garantizar las seguridades a través de la confidencialidad, la autenticación, seguridad de extremos a extremos e integridad. IoT requiere seguridad al desarrollar y su ciclo operativo en cada dispositivo y concentrador del IoT (Talens, 2019).

3.2.3. CORRELACIÓN ENTRE LA TECNOLOGÍA 5G Y OBLIGACIONES Y DERECHOS

3.2.3.1. Tarifas de datos de alta velocidad

La tecnología 5G viene a ser la columna vertebral del ecosistema *IoT*. Estos ecosistemas que se habilitan en 5G lograrían brindar la infraestructura sostenida que desarrolle aún más dichos ecosistemas de IoT (Rodríguez, 2019).

Los avances inalámbricos de quinta generación ofrecerán el ancho de banda sin precedentes con mayor capacidad, velocidad y menores costos en cada bit. Ofrecerá la capacidad para transferir masivamente hasta gigabits, admitirá 65 000 conexiones simultáneas y ofrece tener mayor seguridad que 4G. Sin embargo, donde el espectro asignado a IoT es en su mayoría sin licencia y limitado en bandas de frecuencia, múltiples redes de IoT coexisten e interfieren entre sí en la misma banda de frecuencia, consecuentemente, con un acelerado aumento del usuario inalámbrico y crecimiento de organizaciones, los desarrollos del Internet de las Cosas han sido restringida. Los recursos del espectro son muchas veces escasos (Chen et al. 2017).

Sin embargo, el espectro con licencia, como evolucionar en largo plazo (LTE) y las bandas de comunicación de quinta generación (5G), puede brindar altas garantías en QoS para zonas amplias donde el operador logre evadir interferencias y controlar el nivel de la utilización. Por lo tanto, la combinación de 5G e IoT es opción buena opción en el servicio futuro del IoT que necesitan transmitir grandes cantidades de información en calidad alta (Liu et al. 2017).

En pocas palabra, la gran rapidez con la que trabajarían los dispositivos gracias al 5G combinado con *IoT* puede generar que terceros controlen y usen a traves de distintos medios, información de carácter confidencial y se realice un robo masivo de datos personales para un uso y tratamiento inadecuado. Consecuentemente, resulta necesario que los proveedores comuniquen con claridad a las empresas de telecomunicaciones sobre esta ventaja que podría convertirse en un potencial riesgo para sus usuarios.

3.2.3.2. Alta densidad de tráfico

Una característica clave del dispositivo IoT sería las capacidades para evolucionar y cambio dinámico de configuración del flujo de trabajo. Esto cambia la propiedad interna y performance del dispositivo IoT. Asimismo, el dispositivo móvil experimenta los envejecimientos del hardware y software, generando cambios conductuales de los flujos del trabajo y cada propiedad de los dispositivos (Rodríguez, 2019).

Conforme con Liu et al. (2017), las tecnologías 5G están basadas en lo siguiente:

- Acceder a radio económica parecida a fibra con velocidad para datos mayores de 10 Gb/s a través de la utilización con bandas de frecuencia superiores a 6 GHz y tecnologías relacionadas.
- Virtualización de funciones de red (NFV), que permite incorporar funciones específicas de red para el software ejecutados en hardware de propósito general sin requerir máquinas costosas del hardware específicas. Reduce costos para implementar, administrar y operar; permite compartir y reutilizar una funcionalidad igual para los usuarios.
- Software Defined Networking (SDN) permite que los controles en cada recurso de la red estén abiertos a terceros, proporcionando flexibilidades de adaptación a aplicaciones que requieren un nivel de experiencia.

En adición, tal como indica Liu et al. (2017), Las aplicaciones 5G más allá de la capacidad actual en la tecnología 4G tienen los siguientes requisitos básicos:

- Poca latencia de 1 ms (10 a 20 ms para 4G).
- Sirven 1 millón de dispositivos/km (unos 1000 dispositivos/km en 4G)
- Implemente rápidamente servicios nuevos por 1 hora, lo que llevaría días con la actual tecnología.

En ese sentido, a la capacidad actual de la T5G, no se encuentra en su máxima capacidad, aun así, aún pueden existir situaciones, suponiendo la amenaza en seguridad sobre datos personales, incluidos los datos sensibles.

3.2.3.3. Número masivo de dispositivos conectados (IOT)

Tal como indica International Data Corporation (2016), Se espera que el gasto en IoT crezca a una CAGR del 17 %, de $968 600 millones en 2015 a aproximadamente $1,3 billones en 2019, lo que demuestra que el impacto de la tecnología IoT en la sociedad se está expandiendo y es significativo.

El Internet de las cosas resulta la tecnología popular ampliamente empleada en las producciones industriales y aplicación social como el hogar inteligente, las atenciones médicas y automatizaciones industriales. Pese a que el Internet de las cosas puede ser una tecnología beneficiosa para la economía y la sociedad, su implementación presenta riesgos, dificultades y problemas de seguridad que deben tenerse en cuenta. En general, Internet de las cosas tiene la arquitectura con tres niveles, constando con la capa de red, una capa de percepción y por aplicación. Deberán aplicarse distintos principios en seguridad dentro de las capaz que logran el entorno de IoT asegurado. Además, el Internet de las cosas necesita funcionar con tecnologías que puedan admitir de manera eficiente la transferencia de grandes cantidades de datos y tener el ancho muy alto de bandas (Talens, 2019).

El propósito fundamental del sistema IoT es brindar información a cada usuario cuando resulte necesario. De acuerdo con los derechos de ARCO, los usuarios deben tener acceso inmediato a los datos no solo en circunstancias normales sino también en circunstancias catastróficas. Sin embargo, el dato personal en cada dispositivo IoT es enviado con Internet a la nube para procesarse o almacenarse, pero la velocidad actual para transmisión del dato de Internet no resulta muy rápida al requerir ciertas aplicaciones a tiempo real. Lleva algún tiempo responder a las solicitudes enviadas desde la nube al dispositivo IoT, lo cual es inaceptable para sensibles aplicaciones sobre la latencia (Liu et al. 2017).

En la misma línea, Celín (2019), Señalar que los marcos de IoT son vulnerables en todas las capas; consecuentemente, existen diversos requisitos y desafíos sobre seguridad que deberán considerarse. El actual estado de investigaciones de IoT está centrado de forma principal al protocolo para autentificar y controlar el acceso, pero con un avance

rápido de tecnologías, debiéndose incorporar protocolos novedosos de red como IPv6 (Protocolo de Internet versión 6) y 5G.

El Internet de las cosas posee mucho potencial en cambiar la manera de vivir actualmente, donde la preocupación principal para construir un marco totalmente inteligente sería la seguridad. Si los problemas de seguridad como la confidencialidad, privacidad, autenticación, controles del acceso, seguridad en extremo a extremo, gestionar la confianza, políticas y estándar global es abordado adecuadamente, en el futuro cercano se puede presenciar que IoT lo cambie todo parcialmente (Liu et al. 2017).

3.2.3.4. Sistema basado en IP (protocolos de internet)

Para las implementaciones de IoT, IPv4 ciertamente no puede acomodar una gran cantidad de objetos con reconocimiento de IP. Entonces, IPv6 existe y puede admitir dispositivos 3.4x1038. Sin embargo, estos números generan mucho tráfico, lo que genera demoras más prolongadas y más requisitos de ancho de banda (Rodríguez, 2019).

Se espera que la próxima generación de comunicaciones (5G) entregue velocidades de 10-800 Gbps en comparación con los 2-1000 Mbps de la tecnología actual (4G), y 5G será generado por dispositivos en Internet y debe ser capaz de manejar el tráfico. También es esperado donde una tecnología 5G sea compatible con IPv4 e IPv6. Las implementaciones de 5G estarán definidas por diversas tecnologías presentes y por desarrollar, como red heterogénea (HetNet), red definida por software (SDN), MIMO masivo y accesos múltiples inalámbricos. No obstante, la tecnología enfrenta su propio desafío en seguridad Tomando HetNet como ejemplo, los cambios frecuentes afectan de forma directa al proceso para autentificar la red, principalmente los requisitos por latencia baja de 5G. En adición, computaciones desde las nubes y SDN han aumentado las cantidades de invasiones DDoS por la naturaleza del autoservicio y por demandas de computación desde la nube. Las seguridades para 5G y cada tecnología emergente relacionada con 5G deberán observarse en forma integral para asegurar el IoT (Celín, 2019).

3.2.4. PROBLEMAS DE SEGURIDAD 5G, SUS RIESGOS Y POSIBLES SOLUCIONES

La seguridad en cada dato de IoT y el funcionamiento de la tecnología 5G es una preocupación principal, tanto en tránsito como en reposo. Enviar datos personales al almacenamiento en la nube significaría entregarlo a los proveedores bajo servicio externo. Asimismo, almacenar cada dato personal dentro del backend atrae al pirata informático y los hace vulnerables hacia un ataque externo. Por consiguiente, es necesario un monitoreo continuo y es generado respuestas automatizadas durante eventuales ataques (Liu et al. 2017).

Los principales desafíos en este contexto técnico son el desafío sobre privacidad y seguridad. En el futuro, tanto 5G como IoT enfrentarán los desafíos por recopilar grandes cantidades de datos personales y mantenerlos seguros. Por lo tanto, deben desarrollar tecnologías confiables para manejar las comunicaciones y almacenar datos personales de forma segura. Si bien la preocupación de seguridad y privacidad siguen sin resolverse, queda mucho trabajo por hacer para abordarlas. Asimismo, se espera que la creación del estándar en la industria mantenga un mínimo nivel sobre la privacidad para transmitir y almacenar datos con sensibilidad asociados con la salud, información financiera u otra defensa crítica o datos clasificados (Talens, 2019).

La red 5G promete ser el canal de comunicación clave de esta década. Todos los datos de las redes públicas o privadas podrían eventualmente usar la infraestructura de comunicaciones 5G, y vincular esto con el aumento de dispositivos conectados sugiere que prácticamente todos serán usuarios de la red y todos los dispositivos estarán conectados (Agencia Española de Protección de Datos [AEPD], 2020).

De forma no exhaustiva y en base a lo anterior, se pueden identificar al menos los siguientes riesgos de privacidad de datos. Muchos de estos riesgos están interrelacionados y no son nuevos, ya que existían en generaciones anteriores de teléfonos móviles, pero podrían multiplicarse si el despliegue de 5G está a la altura de las expectativas de éxito como el:

- Posicionamiento preciso de los usuarios: 5G usa más estaciones base y la distancia entre las estaciones base es más corta, lo que hace que el posicionamiento geográfico basado en la red sea más preciso.
- Analítica y toma de decisiones automatizada: El aumento del volumen y categoría de los datos que circulan en la red, multiplicado por el número de dispositivos a los que se conectará cada ciudadano a través de 5G (IoT), permitirá la personalización precisa de las personas y el desarrollo de servicios que permiten la toma de decisiones automatizadas sobre las personas (inteligencia artificial y servicios en tiempo real).
- Responsabilidad compartida entre fabricantes, operadores de red y proveedores de servicios: con el despliegue de redes 5G y la explosión de nuevos servicios, se espera que aumente significativamente la cantidad de instituciones que pueden participar en el procesamiento de datos personales. Esto crea el problema de responsabilidades poco claras para el procesamiento de datos, es decir, se minimizan las responsabilidades de las partes.
- Objetivos e intereses de privacidad divergentes entre las partes interesadas: En relación con lo anterior, los agentes que vayan a interferir en la red telefónica tendrán intereses de privacidad, comerciales, de seguridad nacional, etc. A diferencia de los fabricantes, operadores de telecomunicaciones y proveedores de servicios. Por otro lado, habrá diferentes regulaciones, incluida la obligación de proporcionar canales legales de comunicación a las fuerzas y organizaciones de seguridad en diferentes países.
- Responsabilidad compartida entre fabricantes, operadores de red y proveedores de servicios: Con el despliegue de redes 5G y la explosión de nuevos servicios, se espera que aumente significativamente la cantidad de agencias que pueden participar en el procesamiento de datos personales. Esto puede generar problemas de falta de claridad en las responsabilidades del tratamiento de datos, es decir, se diluyen las responsabilidades de las partes.
- Distintos objetivos e intereses de privacidad entre las partes interesadas: En relación con lo anterior, los proxies que intervendrán en las redes telefónicas

tendrán diferentes intereses de privacidad, comerciales, de seguridad nacional, etc., que los fabricantes, operadores de telecomunicaciones y proveedores de servicios. Por otra parte, habrá diferentes regulaciones, incluyendo la obligación de proporcionar canales legales de comunicación a las fuerzas y organismos de seguridad de diferentes países.

- Ausencia de un modelo de seguridad homogéneo: dado que 5G permite el despliegue de servicios a través de varios proveedores de servicios dentro del MEC, existe una gran cantidad de proxies en la cadena de comunicación e incluso en la red central del operador. Cada proxy puede adherirse a diferentes estándares de seguridad y puede contener partes correspondientes a protocolos de primera generación, por lo que la seguridad general será igual a la parte más débil.
- Crecimiento exponencial de las áreas expuestas a ciberataques: el aumento de los servicios, la conectividad, la interoperabilidad y los puntos de entrada y gestión de la red aumentarán la oportunidad de que se materialicen las amenazas a la privacidad.
- Problemas de privacidad que quedaron de la infraestructura interoperable estándar: cuando se implementa 5G con equipos comunes, la infraestructura previamente diferenciada técnicamente será vulnerable a los mismos ataques que la tecnología de la información tradicional.
- Vulnerabilidades que se originan en entornos virtuales y funciones compartidas: como se mencionó en la sección anterior, se heredan las preocupaciones de privacidad de las tecnologías de virtualización, así como el riesgo de fuga de datos entre funciones compartidas entre diferentes segmentos, como las funciones de administración. Liquidez (AMF).
- la naturaleza dinámica de la función de gestión de la comunicación: si en generaciones anteriores la función de gestión de la red estaba prácticamente cableada, la posibilidad de actualizarla por software proporciona estabilidad, trazabilidad de la versión, actualizaciones de todas las partes, puertas traseras, Malware listo para usar y cosas así.

Los usuarios pueden perder el control: esto puede ocurrir en los flujos de datos, puede tener efectos transfronterizos, puede ocurrir en el ejercicio de los derechos. 5G utiliza un modelo de procesamiento distribuido dinámico donde se espera que los datos y el procesamiento se muevan en tiempo real a la ubicación física donde más se necesitan o se procesan de manera más eficiente (AEPD, 2020).

3.2.5. CUMPLIMIENTO DE LA LEY Y DESAFIOS DEL MINISTERIO DE TRANSPORTES Y TELECOMUNICACIONES RELACIONADOS CON 5G

3.2.5.1. Los desafíos relacionados con 5G para el Ministerio de Transportes y Telecomunicaciones

Los desafíos identificados a nivel nacional reflejan los beneficios y costos de aplicar las propuestas regulatorias, entre ellas que los operadores vienen desplegando infraestructura 4G desde 2014, con una tasa de crecimiento anual del 55% en antenas 4G, sin embargo, solo el 23% del país cuenta con cobertura local 4G servicio móvil, por lo que el Ministerio de Transportes y Comunicaciones pretende implementar la política de despliegue de infraestructura de telecomunicaciones para lograr una conexión más cercana y acceso a tecnología más avanzada a la tecnología 4G(MTC, 2019).

Asimismo, la gestión, uso y desarrollo del espectro radioeléctrico también debe sufrir una transformación, la demanda de más y mejores servicios de telecomunicaciones es cada vez mayor, por lo que se requieren mejoras tecnológicas para que la prestación de estos sea posible. El aumento del tráfico en las redes inalámbricas ha aumentado la demanda de espectro, lo que plantea la necesidad de optimizar las prácticas de gestión del espectro. Además, la ciudad de Lima y el país en su conjunto reflejan ineficiencias en la gestión pública, baja innovación tecnológica y poca planificación urbana; actualmente, con la necesidad de transmitir grandes cantidades de datos, así como la gran cantidad de conexiones simultáneas, los esfuerzos debe hacerse para aumentar la eficiencia y reducir el consumo de energía, y cada vez más datos que pasan a través de teléfonos, televisores y relojes inteligentes, además de que el desarrollo de Internet de las Cosas es cada vez más frecuente en la vida diaria de las personas (MTC, 2020).

Por ello, el Ministerio de Transportes y Comunicaciones (2019), Tiene como objetivo facilitar y facilitar el despliegue de infraestructura de telecomunicaciones para desarrollar nuevos servicios y tecnologías digitales a nivel nacional, con el objetivo de brindar servicios inclusivos e innovadores; ampliar los servicios de telecomunicaciones, principalmente en zonas rurales y áreas de interés social prioritario, a Ways incidir en la calidad de vida de los ciudadanos y promover una mayor inversión y desarrollo económico del país, garantizando así un marco normativo adecuado para su desarrollo. La Resolución Ministerial 917-20119 MTC/01.03 establece las soluciones técnicas o tipos de infraestructura que los operadores de comunicaciones y proveedores de infraestructura pasiva deberían estar más dispuestos a implementar para permitir la prestación eficiente de servicios de telecomunicaciones, tales como el despliegue de vallas publicitarias inteligentes y celdas pequeñas, y el uso de microtúbulos. Este se considera el inicio del desarrollo del despliegue de infraestructura para implementar la tecnología de quinta generación.

Por consiguiente, se necesitarán tecnologías de seguridad para proteger dispositivos y plataformas 5G e IoT de ataques de información y manipulación física, encriptar comunicaciones y enfrentar nuevos desafíos. Los estándares y protocolos en uso hoy en día no pueden manejar la enorme cantidad de tráfico de dispositivos inteligentes o móviles conectados simultáneamente a Internet. Además, se requiere una arquitectura bien definida para cumplir con los requisitos actuales que priorizan el bajo consumo de energía y los algoritmos optimizados. Establezca un marco de seguridad para una gran cantidad de dispositivos, establezca un entorno eficiente para estos dispositivos y mejore su seguridad (Martínez, 2017).

3.2.5.2. Autenticidad de la evidencia

A pesar de todos los beneficios que puede ofrecer la tecnología 5G, surgirían desafíos nuevos sobre privacidad y seguridad respecto a detectar objetos, autenticidad sobre las confidencialidades e integridad de cada dato personal intercambiado y recopilado, y autorización y no repudio. El dato personal y las informaciones generadas deberán mantenerse seguros durante todo el ciclo de vida. Los desafíos harían que la

implementación de nuevas tecnologías sea altamente vulnerable a distintas clases de ataques a la seguridad, generando un entorno inseguro. (MTC, 2020).

Por lo tanto, se deben implementar medidas de seguridad en la comunicación, como autentificar aplicaciones, autentificar y autorizar al usuario, disponibilidades de los servidores, las auditabilidades del sistema e integridad y confidencialidad, convirtiéndolo en el seguro protocolo. Al igual que OPC UA, proporciona nativa seguridad, incluida la autorización y autenticación a través de firmas, integridad y cifrado de datos; o sobre la versión SOAP, utiliza WSSecureConversation, una especificación de seguridades de servicios web generada por IBM (Nieny, 2021).

Cabe aclarar que, conforme al artículo 19 del Decreto Ley 29733, también se cuenta con medida de seguridad que garantice las seguridades de cada dato personal a través de encriptación, control de acceso, etc. o el artículo 21, que posee como objeto supervisar la seguridad de cada dato personal. Sin embargo, resulta que eso no es suficiente para esta nueva tecnología de telecomunicaciones.

3.2.5.3. Estandarización

En telecomunicaciones e informática, la estandarización de la comunicación es un sistema de reglas que permite que dos o más entidades en un sistema se comuniquen entre sí para pasar información. Estas reglas, o protocolos, definen la sintaxis, la semántica y los tiempos de comunicación, así como los posibles métodos de recuperación de errores. Estos pueden ser implementados por hardware, software o una combinación de ambos (MTC, 2020).

En cuanto a los protocolos empleados mayormente, Nieny (2021) describe y resume los siguientes en las normas del ámbito doméstico:

- *AllJoyn: Iniciado por AllSeen Alliance que consta de Haier, LG, Microsoft, Panasonic, Qualcomm, Sharp, Silicon Image,* Technicolor *y TP-Link.* Es un estándar de código abierto que facilita la comunicación entre dispositivos y aplicaciones y es aplicable a todo tipo de protocolos de capa de transporte.

- *HomePlug y HomeGrid:* Son protocolos de comunicación a través de la red eléctrica. Muchas marcas han adoptado esta técnica de comunicación. Según el producto adquirido, el tipo de encriptación varía y algunos dispositivos incluso transmiten información sin encriptar.
- *MFi (Made for iPhone/iPod/iPad):* es el protocolo de comunicación propio de Apple diseñado para interactuar con estos dispositivos. Los dispositivos Apple y los componentes de conexión contienen un chip que permite verificar la autenticidad del dispositivo y los cables de conexión.
- OCF *(Open Connectivity Foundation*): Es un protocolo promovido por empresas como Samsung, Intel, Microsoft, Qualcomm y Electrolux. Es un proyecto de código abierto que proporciona interconectividad con la filosofía "simplemente funciona". Gracias a una implementación de referencia (IoTivity) y un programa de certificación, el protocolo pretende garantizar la interoperabilidad de millones de dispositivos.
- Thread (*protocolo de red*): Fue creado por un grupo de empresas llamado Thread Group. Es una tecnología basada en la comunicación en red sobre IPv6 encriptada con AES. Por ello, y por la flexibilidad que aporta, es un protocolo muy seguro y preparado para el futuro.

Los protocolos mencionados son solo algunos de los más útiles que pueden ayudarnos a enfrentar los desafíos que enfrenta la tecnología 5G. Por otro lado, existen otras normas internacionales como la ISO 27001, que es una guía para mejorar los sistemas de gestión de información de datos personales. Asimismo, la Unión Internacional de Telecomunicaciones ITU-RM.2083 establece los requisitos de seguridad para las redes de comunicaciones móviles 5G.

3.2.5.4. Diálogo con los operadores

Todos los operadores deben tener un enfoque de la arquitectura de red que permita un control centralizado e inteligente o "programación" de la red a través de aplicaciones de software. También tiene como objetivo hacer que las redes sean tan ágiles y flexibles como el servidor virtualizado y la infraestructura de almacenamiento de los

centros de datos modernos. El objetivo es simplificar la gestión de la red proporcionando programabilidad para cambiar las características de toda la red, y debido a que está desacoplado del plano de datos, los ingenieros y administradores de red pueden responder rápidamente a las cambiantes necesidades comerciales. Como resultado, los operadores de red pueden administrar, configurar y optimizar rápida y fácilmente los recursos de la red utilizando procedimientos automatizados, dinámicos y no propietarios (MTC, 2020).

5G es una de las tecnologías inalámbricas más avanzadas jamás desarrolladas. Revolucionará todo el campo en el que se pueden utilizar redes inalámbricas para una comunicación eficiente. Aunque las especificaciones de 5G aún no están determinadas, se espera que la próxima generación de tecnología móvil beneficie en gran medida la innovación de IoT. Las redes 5G prometen ofrecer velocidades más rápidas, menor latencia y brindar soporte de red para un aumento masivo en el tráfico de datos de muchos dispositivos IoT diferentes (Nieny, 2021).

3.2.5.5. Legislación nacional

El MTC, mediante El departamento adjunto a cargo del Ministerio de Comunicaciones es el departamento a cargo de la gestión del espectro radioeléctrico. En este sentido, es responsable de formular la política pública para el sector de las comunicaciones en el Perú. Según el artículo 2 de la Ley de Telecomunicaciones, la modernización y desarrollo de las telecomunicaciones es de interés nacional en el marco de la libre competencia. Asimismo, corresponde al Estado su promoción, dirección y control, de acuerdo con lo dispuesto en la Ley.

Asimismo, el artículo 58 de la Ley de Telecomunicaciones encomienda al MTC la administración, asignación de frecuencias y control del espectro radioeléctrico. Asimismo, en el artículo 75 del mismo cuerpo legal, se establece que además de las atribuciones previstas en su ley orgánica, son funciones del MTC formular políticas de telecomunicaciones en materia tales como seguimiento y control de los resultados de las mismas, gestionar el uso del espectro radioeléctrico, formular y aprobar El Plan Nacional

de Asignación de Frecuencias organiza el sistema de control, seguimiento y relevamiento del espectro radioeléctrico.

De igual forma, el artículo 199 del TUO de la Ordenanza establece que corresponde al Ministerio la gestión, atribución, asignación y control del espectro radioeléctrico y todo lo relativo al espectro radioeléctrico en general, así mismo el artículo 222 del mismo ordenamiento jurídico El artículo establece que el MTC debe velar por que el uso del Espectro radioeléctrico para los servicios de telecomunicaciones funcione adecuadamente y haga un uso razonable de dichos recursos.

En el marco de la Constitución de 1993, el artículo 65 establece que el Estado protege los intereses de los consumidores y usuarios. Para ello, garantiza el derecho a obtener información sobre los bienes y servicios disponibles en el mercado. El MTC, en el marco de sus atribuciones, utiliza todas las herramientas a su alcance para gestionar y gestionar el espectro radioeléctrico con el único fin de reducir la brecha de las telecomunicaciones, que frena la equidad económica y social del país, las desigualdades facilitadas por la tecnología, ya sea en educación, salud, seguridad, etc.

Según el artículo 66 de la Constitución Política del Perú, los recursos naturales renovables y no renovables son propiedad del Estado. En esa línea, el literal e. El artículo 3 de la Ley N° 26821 Ley Orgánica de Aprovechamiento Sustentable de los Recursos Naturales considera al espectro como uno de los recursos naturales existentes en el país, todos los componentes de la naturaleza que pueden ser utilizados por el ser humano para satisfacer sus necesidades y disponibles en el mercado tienen disponibilidad actual o valor potencial (MTC, 2020).

Tal como indica Martel (2020), Intentar simplificar la implementación de los sistemas de protección de datos significa burocracia para las empresas y los controladores de datos personales. Atrás queda la exigencia de la directiva de que los supervisores puedan tratar datos personales con notificación previa, pero incorpora en sus disposiciones obligaciones y principios directamente relacionados con el gobierno corporativo, los modelos de gestión de riesgos y el cumplimiento normativo, que ya se exigen en otros

ámbitos del derecho. como la prevención de riesgos laborales o el compliance penal. Sobre esta base, se introducen nuevos principios de protección de datos personales, tales como:

- Transparencia en el tratamiento de los datos, responsabilidad activa en el cumplimiento de los principios y su certificación.
- Protección de datos por diseño o responsabilidad activa como modelo predeterminado global para el cumplimiento de la preservación de la privacidad integrado en el diseño del sistema informático
- Protección de datos por defecto, es decir, la obligación de tratar únicamente los datos personales necesarios para cada finalidad específica por defecto, y la obligación de evaluar el impacto previamente.

3.2.5.6. Posibles próximos pasos en el futuro inmediato

Según Nieny (2021), el Proyecto de Internet de las cosas (*IoT*), las áreas de ataque de *IoT* son las siguientes:

- Interfaz web insegura
- Autenticación/autorización insuficiente
- Servicios web inseguros
- Falta de cifrado de transmisión.
- Asuntos privados
- Interfaz de nube insegura
- Interfaz móvil insegura
- Configuración de seguridad insuficiente
- El software/firmware no es seguro
- poca seguridad personal

Por consiguiente, se necesitan tecnologías de seguridad para proteger los dispositivos y plataformas de IoT de ataques de información y manipulación física, encriptar sus comunicaciones y enfrentar nuevos desafíos. Los estándares y protocolos actualmente en uso no pueden manejar el alto volumen de tráfico de dispositivos inteligentes o móviles conectados simultáneamente a Internet. Para cumplir con los requisitos actuales de bajo

consumo de energía o algoritmos optimizados, se requiere una arquitectura bien definida para admitir una gran cantidad de dispositivos. Establecer un marco de seguridad para crear un entorno eficiente y mejorar la seguridad de estos dispositivos (Martel, 2020).

Para cada ataque a la tecnología, existe al menos una solución posible. La implementación de todas estas soluciones individualmente generaría una sobrecarga significativa y degradaría el rendimiento. Los estándares y protocolos actualmente en uso no pueden manejar el alto volumen de tráfico de dispositivos inteligentes o móviles conectados simultáneamente a Internet. Para cumplir con los requisitos actuales, se requiere una arquitectura bien definida que admita una gran cantidad de dispositivos (Duque & Gómez, 2020).

La solución al problema presentado permite abordar la situación de seguridad y privacidad de los datos personales, surgiendo como una propuesta de desarrollo de modelos para diseñar arquitecturas de red eficientes y más seguras, se consideran todas las capas de las arquitecturas 5G e IoT, ya que cada dominio presenta diferentes riesgos de seguridad, así que usa diferentes técnicas de seguridad (Nieny, 2021).

3.2.5.7. Influir en la fijación de estándares en el 3GPP

3GPP en la versión 13 (2016) introdujo una nueva interfaz de radio dedicada a comunicaciones masivas de tipo máquina (mMTC), llamada Internet de las cosas de banda estrecha (NB-IoT), que opera en espectro celular con licencia y funciona con sistema LTE / LTE-A compatible. Las características específicas de NB-IoT incluyen la aplicación de tecnología de mejora de cobertura, que se espera que brinde una mayor confiabilidad de conexión en áreas de cobertura extendida en comparación con los sistemas 4G actuales. Dado que NB-IoT también se concibe como un futuro estándar 3GPP para IoT basado en 5G, el análisis de tales tecnologías parece crucial (Martel, 2020).

CAPÍTULO III.

RESULTADOS

3.1. RESULTADOS DE LA APLICACIÓN DEL CUESTIONARIO

Tabla1

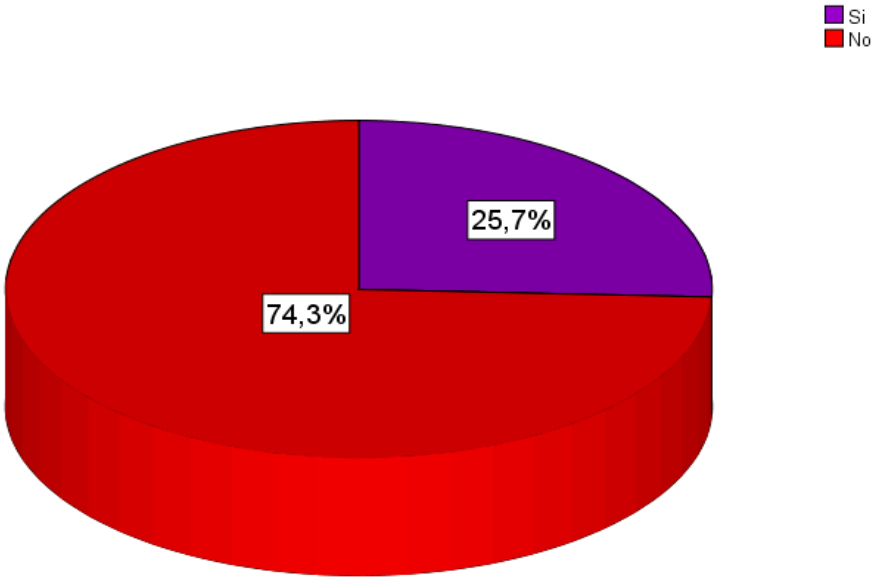
Considera usted ¿Qué las leyes implementadas en Perú protegen los datos personales de los usuarios de la tecnología 5G?.

		Frecuencia	Porcentaje
Válido	Si	18	25,7
	No	52	74,3
	Total	70	100,0

Fuente: Elaboración propia

Figura1

Considera usted ¿Qué las leyes implementadas en Perú protegen los datos personales de los usuarios de la tecnología 5G?



Fuente: Elaboración propia

Conforme se percibe en la Tabla 1 y Figura 1, los resultados de una encuesta a 70 usuarios de tecnología 5G mostraron que el 74,3% de las leyes vigentes e implementadas de Perú no protegen los datos personales de los usuarios de tecnología 5G, mientras que el 25,7% de las leyes vigentes e implementadas de Perú protegen los datos personales. Proteger los datos personales de los usuarios de la tecnología 5G. Por lo tanto, concluyó que las leyes vigentes y aplicadas no protegen los datos personales de los usuarios de la tecnología 5G en Perú en el 2021.

Tabla2

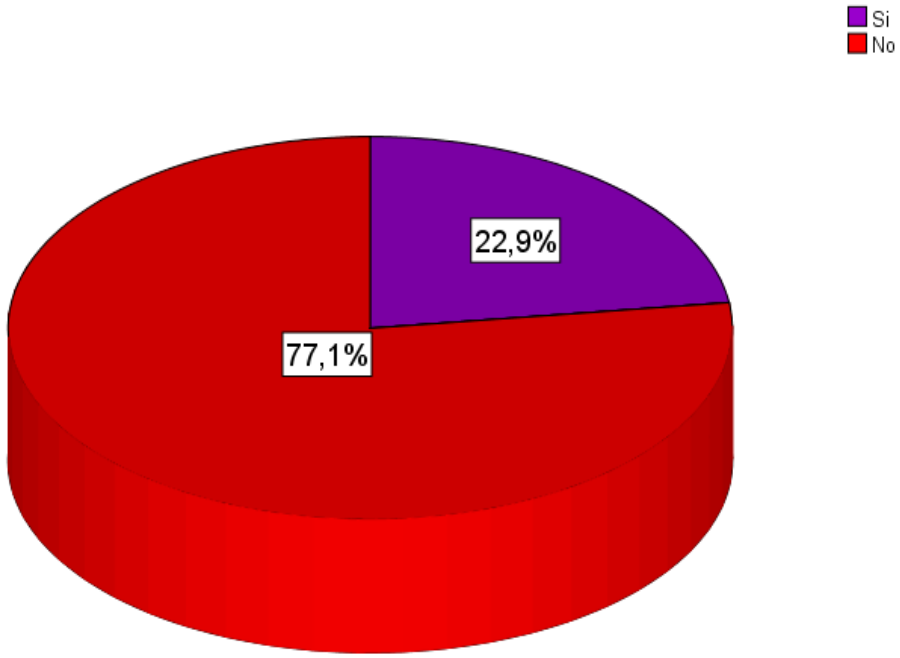
Cree usted ¿Qué existen leyes peruanas que le protejan a los usuarios de la tecnología 5G frente a los riesgos de los contenidos en las plataformas sociales?

		Frecuencia	Porcentaje
Válido	Si	16	22,9
	No	54	77,1
	Total	70	100,0

Fuente: Elaboración propia

Figura2

Cree usted ¿Qué existen leyes peruanas que le protejan a los usuarios de la tecnología 5G frente a los riesgos de los contenidos en las plataformas sociales?



Fuente: Elaboración propia

De acuerdo con la Tabla 2 y Figura 2 de resultados de haber encuestado a 70 usuarios que cuenten con la tecnología 5G, se alcanzó que el 77,1% considera que no existen leyes peruanas que le protegen a los usuarios de la tecnología 5G de los contenidos que se distribuye a través de las plataformas sociales, en tanto el 22,9% considera que si existen leyes peruanas que le protegen a los usuarios de la tecnología 5G de los contenidos que se distribuye a través de las plataformas sociales. Por lo que se concluye que no existen leyes peruanas que le protegen a los usuarios de la tecnología 5G de los contenidos que se distribuye a través de las plataformas sociales en Perú, 2021.

Tabla3

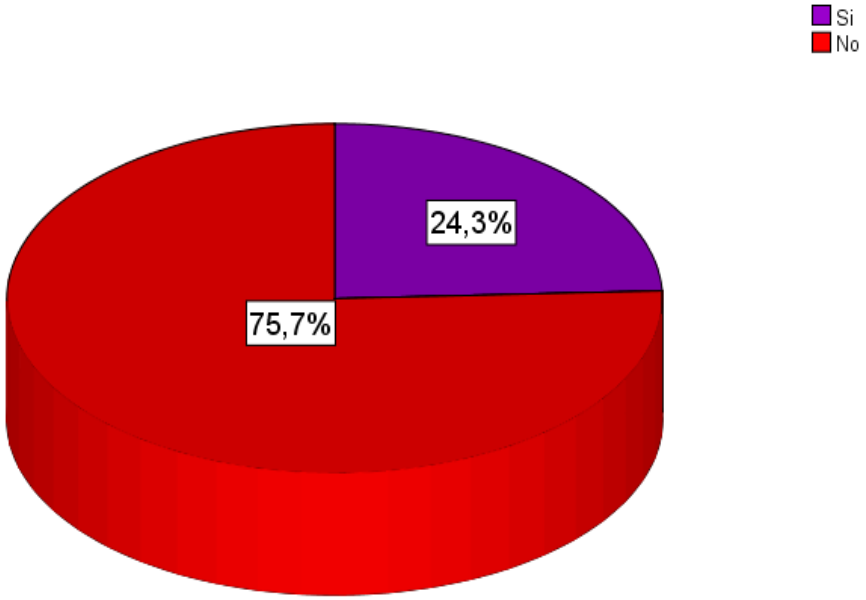
Cree usted ¿Qué, los operadores de servicios de tecnología 5G cuentan con profesionales de seguridad informática para hacer frente a la fuga de datos personales?

		Frecuencia	Porcentaje
Válido	Si	17	24,3
	No	53	75,7
	Total	70	100,0

Fuente: Elaboración propia

Figura3

Cree usted ¿Qué, los operadores de servicios de tecnología 5G cuentan con profesionales de seguridad informática para hacer frente a la fuga de datos personales?



Fuente: Elaboración propia

Según a la Tabla 3 y Figura 3 de resultados de haber encuestado a 70 usuarios que cuenten con la tecnología 5G, se alcanzó que el 75,7% de los operadores de servicios de tecnología 5G no cuentan con profesionales de la seguridad informática para hacer frente a la ciberdelincuencia, no obstante, el 24,3% de los operadores de servicios de tecnología 5G si cuentan con profesionales de la seguridad informática para hacer frente a la ciberdelincuencia. Se concluye que los operadores de servicios de tecnología 5G no cuentan con profesionales de la seguridad informática para hacer frente a la ciberdelincuencia en Perú, 2021.

Tabla4

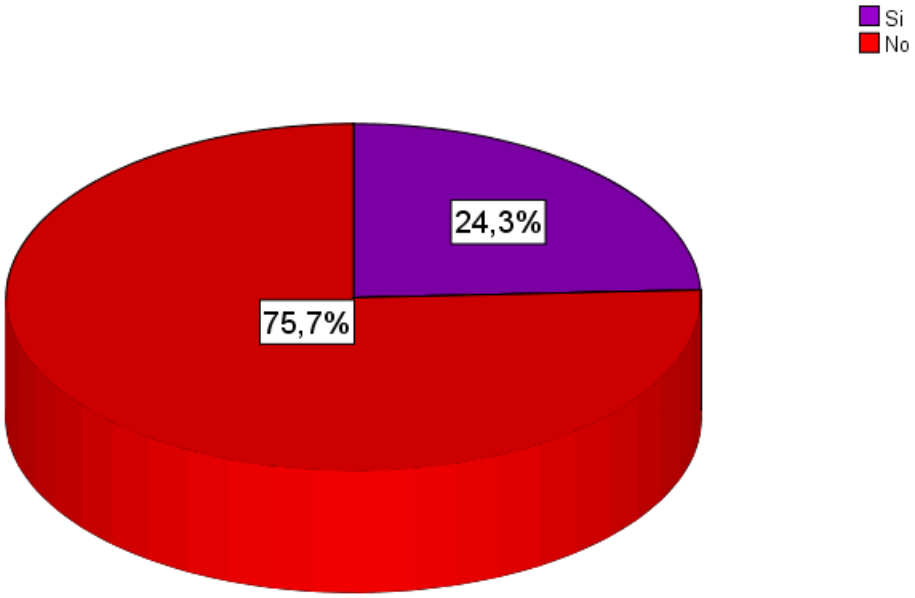
Según usted ¿Las empresas de telecomunicaciones que venden tecnología 5G cuentan con profesionales de seguridad informática para hacer frente a la fuga de datos personales?

		Frecuencia	Porcentaje
Válido	Si	17	24,3
	No	53	75,7
	Total	70	100,0

Fuente: Elaboración propia

Figura4

Según usted ¿Las empresas de telecomunicaciones que venden tecnología 5G cuentan con profesionales de seguridad informática para hacer frente a la fuga de datos personales?



Fuente: Elaboración propia

Acorde a la Tabla 4 y Figura 4 de resultados de haber encuestado a 70 usuarios que cuenten con la tecnología 5G, se obtuvo que el 75,7% de las empresas de telecomunicaciones que venden tecnología 5G no cuentan con profesionales de seguridad informática para frente a la ciberdelincuencia, por otro lado, el 24,3% de las empresas de telecomunicaciones que venden tecnología 5G si cuentan con profesionales de seguridad informática para frente a la ciberdelincuencia. Se concluye que las empresas de telecomunicaciones que venden tecnología 5G no cuentan con profesionales de seguridad informática para frente a la ciberdelincuencia en Perú, 2021.

Tabla5

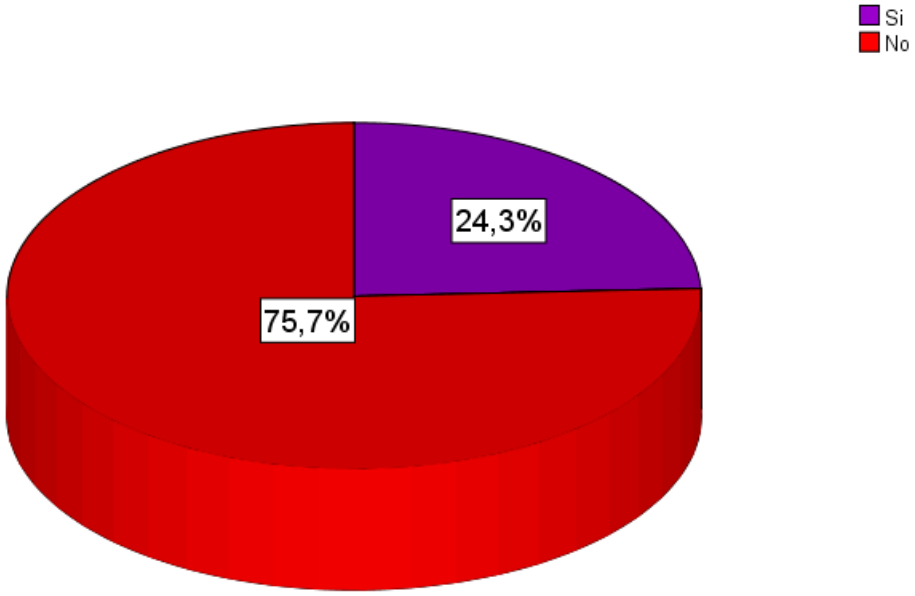
Según usted ¿Los proveedores de tecnología 5G cuentan con profesionales de seguridad informática para hacer frente a la fuga de datos personales?

		Frecuencia	Porcentaje
Válido	Si	17	24,3
	No	53	75,7
	Total	70	100,0

Fuente: Elaboración propia

Figura5

Según usted ¿Los proveedores de tecnología 5G cuentan con profesionales de seguridad informática para hacer frente a la fuga de datos personales?



Fuente: Elaboración propia

De acuerdo a la Tabla 5 y Figura 5 de resultados producidos conforme a la encuesta empleada a 70 usuarios que cuenten con la tecnología 5G, se alcanzó que el 75,7% de las empresas de telecomunicaciones y proveedores de tecnología 5G no cuentan con profesionales de seguridad informática para frente a la ciberdelincuencia, por otra parte el 24,3% de las empresas de telecomunicaciones y proveedores de tecnología 5G si cuentan con profesionales de seguridad informática para frente a la ciberdelincuencia. Se concluye que las empresas de telecomunicaciones y proveedores de tecnología 5G no cuentan con profesionales de seguridad informática para frente a la ciberdelincuencia en Perú, 2021.

Tabla6

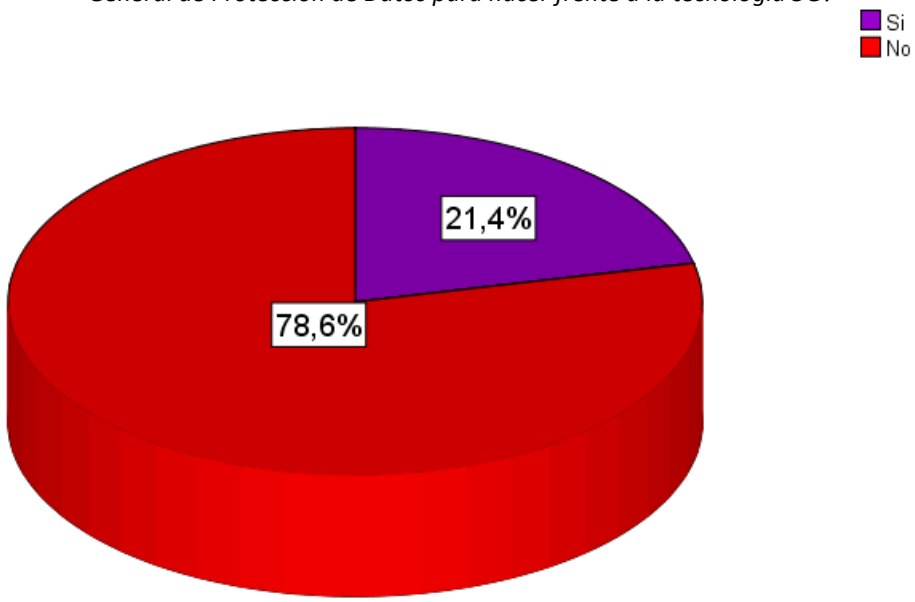
Cree usted ¿Qué, Perú ha implementado normas conforme a las recomendaciones del Reglamento General de Protección de Datos para hacer frente a la tecnología 5G?.

		Frecuencia	Porcentaje
Válido	Si	15	21,4
	No	55	78,6
	Total	70	100,0

Fuente: Elaboración propia

Figura6

Cree usted ¿Qué, Perú ha implementado normas conforme a las recomendaciones del Reglamento General de Protección de Datos para hacer frente a la tecnología 5G?



Fuente: Elaboración propia

Acorde a la Tabla 6 y Figura 6 Los resultados basados en una encuesta a 70 usuarios con tecnología 5G arrojaron que el 78,6% de los usuarios no manejaban la tecnología 5G de acuerdo con los estándares de implementación propuestos del Reglamento General de Protección de Datos, en cambio, el 21,4% si lo habían hecho. El Reglamento de Protección de Datos propone implementar estándares para tratar con la tecnología 5G. Concluyó que en 2021 Perú no implementó los estándares recomendados por el Reglamento General de Protección de Datos, que trata sobre la tecnología 5G.

Tabla7

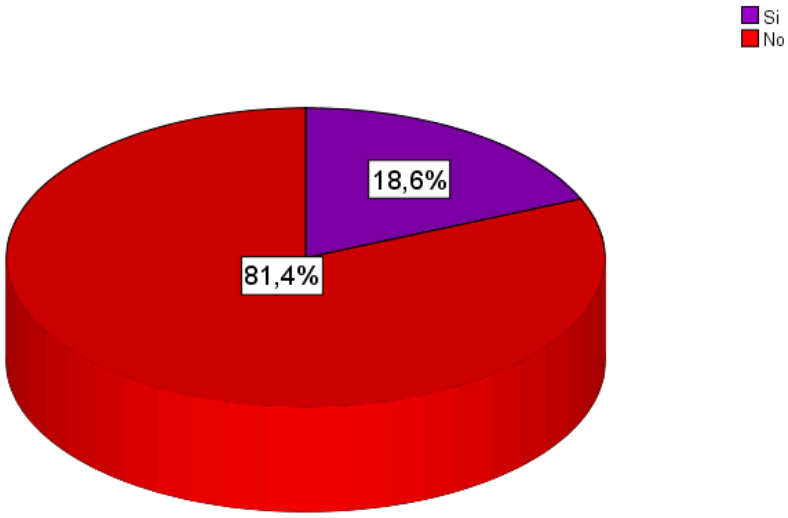
Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G, informan a sus usuarios con precisión la finalidad del tratamiento de sus datos?

		Frecuencia	Porcentaje
Válido	Si	13	18,6
	No	57	81,4
	Total	70	100,0

Fuente: Elaboración propia

Figura7

Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G, informan a sus usuarios con precisión la finalidad del tratamiento de sus datos?



Fuente: Elaboración propia

Conforme a la Tabla 7 y Figura 7 de resultados originados conforme a la encuesta empleada a 70 usuarios que cuenten con la tecnología 5G, se halló que el 81,4% de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no informan con precisión a los usuarios de la finalidad del tratamiento de sus datos, frente a los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G que informan con precisión a los usuarios de la finalidad del tratamiento de datos. datos. Concluyó que los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no informaron con precisión a sus usuarios la finalidad del tratamiento de sus datos en Perú en 2021.

Tabla8

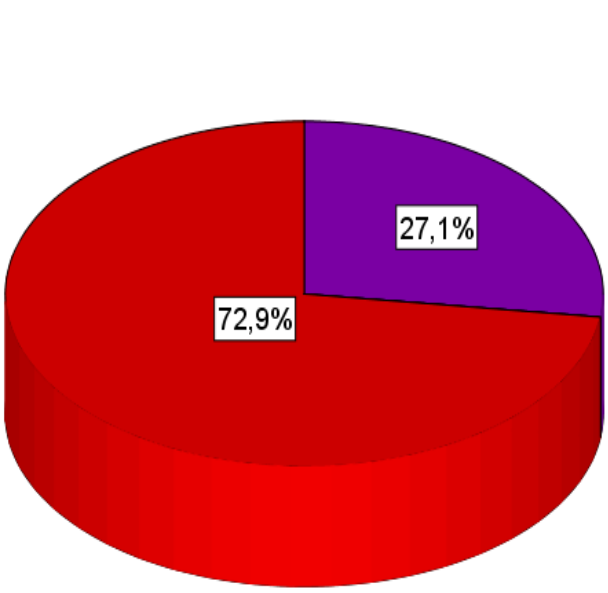
Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G llevan un registro de las actividades realizadas con los datos de sus usuarios brindados?

		Frecuencia	Porcentaje
Válido	Si	19	27,1
	No	51	72,9
	Total	70	100,0

Fuente: Elaboración propia

Figura8

Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G llevan un registro de las actividades realizadas con los datos de sus usuarios brindados?



Fuente: Elaboración propia

De acuerdo a la Tabla 8 y Figura 8 de resultados producidos conforme a la encuesta empleada a 70 usuarios que cuenten con la tecnología 5G, se obtuvo que el 72,9% de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no llevan un registro de las actividades realizadas con los datos de sus usuarios, frente al 18,6% de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G si llevan un registro de las actividades realizadas con los datos de sus usuarios. Se concluye que los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no llevan un registro de las actividades realizadas con los datos de sus usuarios en Perú, 2021.

Tabla9

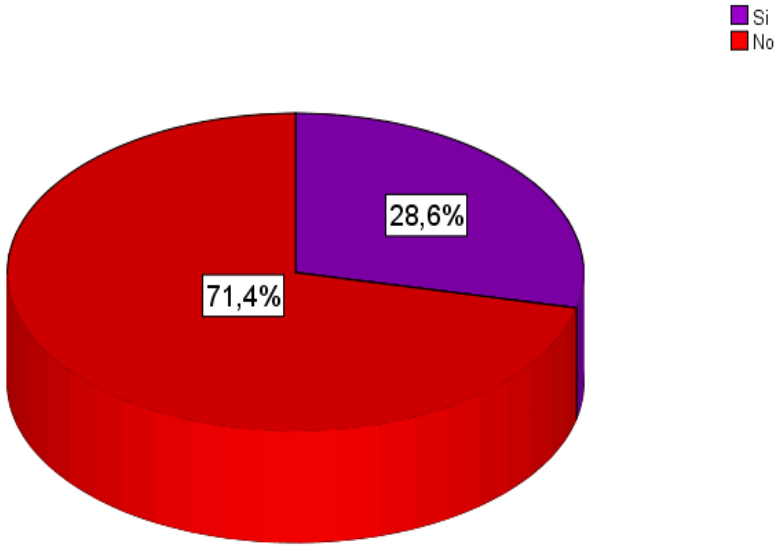
Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios?

		Frecuencia	Porcentaje
Válido	Si	20	28,6
	No	50	71,4
	Total	70	100,0

Fuente: Elaboración propia

Figura9

Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios?



Fuente: Elaboración propia

Conforme a la Tabla 9 y Figura 9 de resultados obtenidos conforme a la encuesta empleada a 70 usuarios que cuenten con la tecnología 5G, se alcanzó que el 71,4% de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios, mientras que el 28,6% de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G si notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios. Se concluye que, de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios en Perú, 2021.

Tabla10

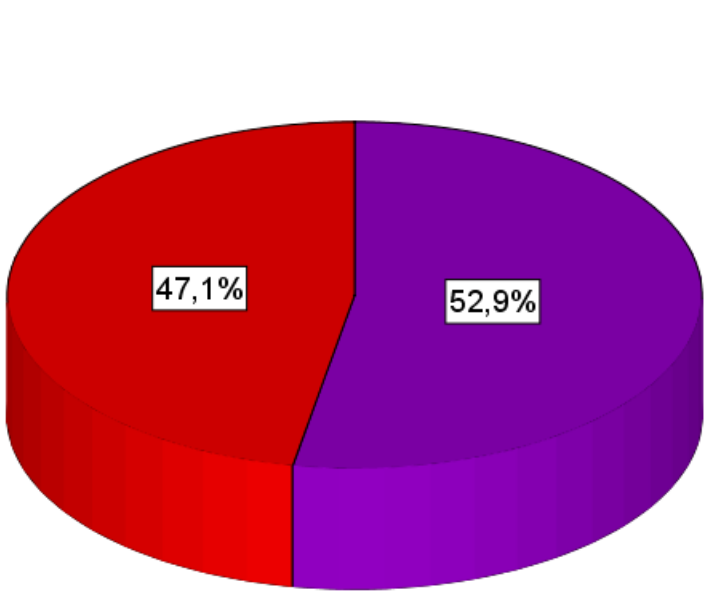
Según usted ¿Se deben modificar las leyes peruanas sobre protección de datos personales para hacerlas más eficientes frente a la ciberdelincuencia para los usuarios de tecnología 5G?

		Frecuencia	Porcentaje
Válido	Si	37	52,9
	No	33	47,1
	Total	70	100,0

Fuente: Elaboración propia

Figura10

Según usted ¿Se deben modificar las leyes peruanas sobre protección de datos personales para hacerlas más eficientes frente a la ciberdelincuencia para los usuarios de tecnología 5G?



Fuente: Elaboración propia

Según a la Tabla 10 y Figura 10 de resultados generados conforme a la encuesta empleada a 70 usuarios que cuenten con la tecnología 5G, se obtuvo que el 52,9%consideran que si deben modificar las leyes peruanas sobre protección de datos para hacerlas más eficientes frente a la ciberdelincuencia para los usuarios de tecnología 5G, por otro lado el 47,1% consideran que no deben modificar las leyes peruanas sobre protección de datos para hacerlas más eficientes frente a la ciberdelincuencia para los usuarios de tecnología 5G. Se concluye que, si deben modificar las leyes peruanas sobre protección de datos para hacerlas más eficientes frente a la ciberdelincuencia para los usuarios de tecnología 5G en Perú, 2021.

3.2. RESULTADOS DE LA APLICACIÓN DE LA ENTREVISTA

De haber entrevistado a tres especialistas sobre los alcances jurídicos de la legislación nacional e internacional sobre protección de datos personales en la implementación de la tecnología 5G en Perú, respecto al **objetivo general:** Analizar los alcances jurídicos de la legislación sobre protección de datos personales en la implementación de la Tecnología 5G en Perú, 2021, la entrevistada Abogada Salas (2022) especialista en Derechos del Consumidor y protección de Datos sostuvo que:

> De cara a los avances tan progresivos y rápidos que traen consigo la utilización de Tecnología 5G, en cuanto al ámbito nacional, se deberá considerar el aumento en la protección legal de los derechos de los ciudadanos y de sus datos personales, al ser que esta nueva tecnología evidentemente involucra una mayor utilización, disponibilidad y almacenamiento de datos, a través por ejemplo de la geolocalización.

En la misma línea, la segunda entrevistada Abogada Valdivia (2022) con respeto a lo mencionado manifiesta que:

> La legislación en protección de datos personales resultará especialmente aplicable y necesaria a fin de proteger a las personas cuya información sea gestionada por medio de tecnología 5G, pues la cantidad de datos que se pueden recopilar por medio de esta red, a través del uso de distintos dispositivos, permite una captación de información mucho más invasiva y, por ende, más específica sobre el titular de los datos personales.

Por último, el tercer entrevistado Abogado Zegarra (2022) especialista en derechos de consumidor y seguridad de datos afirma:

> La legislación en materia de datos personales deberá ser de uso y aplicación directa en los avances que tengan las redes tecnológicas. Al ser la más reciente la Tecnología 5G, implica un mayor riesgo de tratamiento en los datos personales de

las personas. Por consiguiente, será necesario la adición de ciertas medidas en la legislación nacional.

De igual modo con respecto al objetivo específico 1: Describir el nivel de entendimiento de las personas de la tecnología 5G en las implicancias y riesgos puede generar sobre sus datos personales en Perú, 2021, la entrevistada Abogada Salas (2022) especialista en Derechos del Consumidor y protección de Datos manifestó que:

> El concepto que tiene la ciudadanía de esta tecnología 5G va dirigido únicamente, o al menos lo que es más escuchado, a la velocidad con la cual se logra avanzar en el navegador a través de un dispositivo, o descargar archivos y demás. Como se conoce, abarca mucho más que la anterior gama tecnológica; a través de esta tecnología se puede tener acceso a datos personales desde el uso o envío en ambientes compartidos, utilización de dispositivos LoT, dependencia de tecnología iCloud, etc. Y de esta forma los usuarios de esta tecnología podrían encontrarse en desconocimiento de lo que realmente abarca.

Asimismo, la segunda entrevistada Abogada Valdivia (2022) con respeto a lo mencionado asegura que:

> Se debe a un amplio desconocimiento de los ciudadanos en relación con la importancia de la información personal en la economía actual. Los datos personales son el primer insumo de las compañías para establecer planes comerciales y diseñar productos y servicios para sus consumidores, los cuales, ignorando esto, se encuentran plenamente dispuestos a proporcionar información personal a cambio de obsequios o por la obtención de beneficios gratuitos sin cuestionar el destino de su información. A esto se suma la poca educación en tecnologías de la información que recibe la ciudadanía.

De igual, el tercer entrevistado Abogado Zegarra (2022) especialista en derechos de consumidor y protección de datos declara que :

> No, los ciudadanos en su gran mayoría desconocen de la implicancia y riesgo que representa el buen y/o inadecuado tratamiento de sus datos personales. Recordemos que esta es la herramienta más usada por el sector empresarial y político para determinar el comportamiento de los usuarios, consumidores o población en general. Uno de los riesgos más evidentes es la geolocalización lo que permitiría a las áreas de marketing identificar donde ubicar su publicidad y que pueda ser recibida por usuarios preseleccionados.

De la misma, con respecto al objetivo específico 2: Analizar la responsabilidad de los operadores de servicios, empresas de telecomunicaciones y proveedores de la tecnología 5G en la manipulación de los datos personales de los usuarios en Perú, 2021, la entrevistada Abogada Salas (2022) especialista en Derechos del Consumidor y protección de Datos asevera que:

> Desde hace unos años se viene generando una cultura de aplicación e implementación de la legislación sobre la Protección de Datos Personales cada vez más consciente, sin embargo, los operadores de servicios, empresas de telecomunicaciones y proveedores de la tecnología 5G deberán prestar particular atención a partir de la aplicación de esta nueva tecnología y las novedades que conlleva. La responsabilidad en la manipulación de los datos personales de sus usuarios considero no puede tomarse como algo estático por parte de las empresas proveedoras, puesto que los avances tecnológicos avanzan día a día y estoy segura de que la regulación sobre el tema también lo hará.

De la misma manera, la segunda entrevistada Abogada Valdivia (2022) con respeto a lo mencionado sostiene que:

> Los operadores de telecomunicaciones y proveedores de servicios de tecnología 5G tienen mucha claridad sobre las implicancias del uso de esta red por la evidente naturaleza del manejo de su propio negocio; sin embargo, no cuentan con incentivos suficientes para asumir proactivamente la responsabilidad de

> informar sobre las particularidades de la red 5G en la afectación a la privacidad de los titulares de datos personales.

Al respecto, considero que debemos distinguir el rol de los operadores, que ponen la red al orden de las personas, del rol de los proveedores de servicios que utilizan la red 5G y efectúan el tratamiento de datos personales ya sea por encargo o como responsables del mismo. Solo en este último caso se verán afectados por la normativa y asumirán las obligaciones que de esta se derivan. Los proveedores de redes de telecomunicaciones no asumen un rol de tratamiento, y, por ende, las implicancias del uso dicha tecnología en la privacidad de sus usuarios no exige el cumplimiento de la LPDP.

Por tanto, el tercer entrevistado Abogado Zegarra (2022) especialista en derechos de consumidor y protección de datos declara:

> Las empresas de telecomunicaciones, operadores de servicios y proveedores de servicios si tienen conocimiento sobre la responsabilidad y rol que tienen frente a los datos personales. Sin embargo, no es un tema que sea de suma preocupación por desconocimiento sobre el ente que regula el procedimiento de datos personales y desconocimiento respecto de las multas a las cuales pueden ser acreedoras. Por otro lado, debe tenerse claro que las empresas de servicios tienen mayor incidencia en el procedimiento de datos que a diferencia de los proveedores de servicio tienen mayor flujo de datos.

De igual forma con respecto al objetivo específico 3: Explicar los alcances jurídicos del Reglamento General de Protección de Datos (RGPDP) sobre la seguridad de los datos personales en la tecnología 5G en la legislación en Perú, 2021, la entrevistada Abogada Salas (2022) especialista en Derechos del Consumidor y protección de Datos afirma que:

> El RGPDP si bien es cierto se encuentra dentro de los parámetros de lo que está actualmente siendo visto por la regulación de la materia, eventualmente y como comentaba párrafos arriba, va a tener que mutar y actualizarse de la mano con las nuevas figuras digitales que vengan naciendo y aplicando en nuestro territorio.

En la misma línea, la segunda entrevistada Abogada Valdivia (2022) con respeto a lo mencionado sostiene que:

> El RGDP tiene injerencia en el tratamiento de datos personales en el territorio nacional, es importante considerar que el RGDP cuenta con disposiciones que habilitan su aplicación extraterritorial, y permiten que las instituciones europeas exigir el cumplimiento de los estándares de tratamiento previstos por dicha norma a responsables de tratamiento que se encuentren fuera de la UE o que realicen su tratamiento fuera de la misma, siempre que tal tratamiento involucre los datos de residentes de la UE. En ese caso, las medidas de seguridad exigibles por la RGPD serían plenamente exigibles por los tribunales europeos, aun así, el tratamiento se haya generado en Perú

Por último, el tercer entrevistado Abogado Zegarra (2022) especialista en derechos de consumidor y seguridad de datos firma:

> El RGPDP tiene actuación del elemento de tratamiento de datos personales en el territorio nacional, también lleva consigo aplicación extraterritorial como fuera y dentro de la Unión Europea cumpliendo los estándares de dichas disposiciones. En mi opinión con el paso de los años el RGPDP va a tener que actualizarse a las nuevas tecnológicas digitales las cuales vayan a ser aplicables al territorio peruano tarde o temprano.

Para finalizar con respecto al objetivo específico 4: Proponer la implementación de una modificatoria de las leyes peruanas que normaliza la seguridad de datos frente a la tecnología 5G en Perú, 2021, la entrevistada Abogada Salas (2022) especialista en Derechos del Consumidor y protección de Datos sostiene que:

> Considero que se debe primero hacer un análisis exhaustivo de los ejes donde se puede ver implicado el tratamiento y transferencia de datos personales en el contexto de la T5G, y en base a eso el subsecuente análisis de la regulación a modificarse o implementarse de manera específica a fin de velar por la protección de este tipo de data y de sus titulares.

De igual manera, la segunda entrevistada Abogada Valdivia (2022) con respeto a lo mencionado asegura que:

> Considero que no hay necesidad de una normativa distinta, pues el cambio en la tecnología solo exacerba riesgos aumentando la incidencia de estos por la enorme cantidad de data que se procesaría por medio de estas redes. No se generan nuevos riesgos a la privacidad. En el contexto peruano, considero que, al generarse una más alta incidencia de afectaciones a la privacidad, nuestra DPA necesita tener los recursos materiales que le permitan una apropiada difusión de la relevancia de la privacidad, sus potenciales afectaciones y los derechos de los ciudadanos para su protección, así como para fiscalizar y sancionar con mayor celeridad a los proveedores de servicios que utilicen esta tecnología.

Por último, el tercer entrevistado Abogado Zegarra (2022) especialista en derechos de consumidor y protección de datos sostiene:

> La legislación actual no amerita la modificación de la norma, puesto que lo contemplado en la LPDP y su reglamento se presta con flexibilidad para hacer frente al dinamismo de la tecnología. Siendo apropiado que el ente rector eduque a los ciudadanos respecto de las implicancias que tiene la innovación tecnológica en el uso y tratamiento de sus datos personales, como lo es el caso de la Tecnología 5G.

3.3. DISCUSIÓN DE RESULTADOS

En esta parte se describen los resultados descriptivos de la investigación conforme de haber encuestado a 3 especialistas y 70 usuarios de la Tecnología 5G de Arequipa, obteniendo por resultados para el objetivo general: donde se obtuvo que el 74,3% de las leyes existentes e implementadas en Perú no protege los datos personales de los usuarios de la tecnología 5G, mientras que el 25, 7% de las leyes existente e implementadas en Perú si protege los datos personales de los usuarios de la tecnología 5G. Por lo que concluye que las leyes existentes e implementadas no protegen los datos personales de los usuarios de la tecnología 5G en Perú, 2021. Sin embargo, discrepa con Adachi y Nakajima (2000) Quienes en su investigación demostraron que para el año 2000 llegó la tercera generación

de redes móviles, las cuales intentaron brindar conexión con terminales móviles a través de Internet, y el mercado comenzó a ser conocido como aplicaciones dedicadas a la comunicación entre teléfonos móviles, con mayor carga y descarga. rapidez y posibilidad de intercambiar mensajes a través de WhatsApp, correo o diferentes aplicaciones que simplifican la comunicación y acercan a las personas, según su uso. Asimismo, concuerda con (Pérez, 2009) Para el 2010, cuando lleguen las redes móviles de cuarta generación, sus núcleos actualmente están compuestos por elementos de red, que básicamente se refieren a hardware dedicado a funciones específicas en las redes móviles, con cargas financieras y operativas, dijo. Muy grande y actualmente, las necesidades tecnológicas han llegado al límite de su funcionalidad. La cantidad de datos que utilizan los terminales móviles es mayor, y con la revolución de las redes 5G se utiliza el concepto de virtualización de redes, donde cada elemento de la red estará alojado virtualmente en un servidor que gestiona el funcionamiento de dichos elementos. Sin embargo, siempre existirá el risego latente de emplear nuevas tecnologías que generen riesgos legales, en este caso frente a los datos personales, por consiguiente será necesario la aplicación del concepto sobre el dinamismo del derecho.

Seguidamente Se presentó una discusión de resultados relacionada con el objetivo específico 1, en el que el 81,4% de los operadores de servicios, telecomunicaciones y proveedores de tecnología 5G no informaron con precisión a los usuarios sobre el propósito de su procesamiento de datos, en comparación con el 18,6% de los operadores de servicios, telecomunicaciones y proveedores de tecnología 5G. proveedores, si informan con precisión a los usuarios de las finalidades para las que se tratan sus datos. Concluyó que los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no informaron con precisión a sus usuarios las finalidades del tratamiento de sus datos en el Perú, 2021. Así mismo, se concuerda con los resultados de Rodríguez (2019) quien refiera que conforme con 3GPPP, el 5G aparece oficialmente en el 2018, pero su nacimiento se remonta al 2008, junto al proyecto *"5Gmobiles communication systems based on beam-divisionmultiple access and realys with grooup cooperation"*. La compañía de telecomunicaciones pionera en alcanzar velocidades 5G fue la sueca Ericsson; seguidamente, Huawei realizó un acuerdo con el operador ruso *Megafon* durante el 2014

para la estandarización de la tecnología 5G. Asimismo, países de la Unión Europea, como Alemania e Inglaterra, al igual que compañías tecnológicas como NTTD, Samsung Electronics, Nokia y Alcatel han estado invirtiendo mucho en pruebas de laboratorio para obtener datos críticos que ayuden a dar vida a la tecnología. Como resultado, se han formado alianzas estratégicas entre operadores de telefonía móvil, universidades y empresas de telecomunicaciones en diferentes países, incluidos proyectos como NGMN Alliance, Mobile Cloud Network, 5GNOW y el más famoso METIS2020, que probablemente sentarán las bases funcionales de 5G, con niveles de rendimiento estimados de 1000 veces más tráfico que el tráfico actual, 10 000 millones de dispositivos conectados, tasas de datos de usuario alcanzables de 10 a 100 veces más altas, reducción de latencia 5 veces mayor que la del tráfico actual, hasta un aumento en la integridad de los datos y la duración de la batería 10 veces. Si bien nuestra legislación actual si contempla el ejercicio obligatorio de solo recopilar aquellos datos personales que guarden una finalidad para lo cual fueron solicitados, es claro que (y no solo en nuestro país) existe una brecha de comunicación con quienes adquieren o reciben productos o servicios, ya que el caso expuesto solo evidencia que la implementación de nuevas tecnologías genera un vacio para todos respecto de la manera en la que se recopila los datos personales.

En la misma línea se presentó la discusión de resultados relacionados al objetivo específico 2, donde el 71,4% de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios, mientras que el 28,6% de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G si notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios. Se concluye que, de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G no notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios en Perú, 2021. Concuerda con los resultados de Talens (2019) quien manifiesta que se trata de un derecho reconocido prácticamente en todos los ordenamientos jurídicos, pero entender el fundamento del derecho de protección de datos necesita de forma obligatoria acercarse al derecho a la intimidad y privacidad, pues estos

experimentaron su desarrollo jurídico paralelo al desarrollo de las nuevas tecnologías. Empezando a hablar sobre privacidad se debe remontar hasta finales del siglo XIX en Estados Unidos, donde dos jóvenes abogados de Boston publicaron en 1890 un artículo en la Harvard Law Review; en este, Samuel Warren y Louis Brandeis se refirieron a la privacidad como derecho a "que se nos deje en paz", estableciendo las bases de lo que hoy se conoce en el sistema jurídico como los "asuntos de relevancia pública", impidiendo la publicación de aquello que resulte de interés general o público, siendo una suerte de presunción a favor del control individual sobre la información personal. Por consiguiente, es de carácter obligatorio idear nuevas maneras para que los responsables (titular del banco de datos, encargado de tratamiento y un tercero) del dato personal comuniquen a sus usuarios o potenciales usuarios sobre el tratamiento de estos.

Así mismo, se presentó la discusión de resultados relacionados al objetivo específico 3, se obtuvo que el 52,9%consideran que, si deben modificar las leyes peruanas sobre protección de datos para hacerlas más eficientes frente a la ciberdelincuencia para los usuarios de tecnología 5G, por otro lado, el 47,1% consideran que no deben modificar las leyes peruanas sobre protección de datos para hacerlas más eficientes frente a la ciberdelincuencia para los usuarios de tecnología 5G. Se concluye que, si deben modificar las leyes peruanas sobre protección de datos para hacerlas más eficientes frente a la fuga de datos personales para los usuarios de tecnología 5G en Perú, 2021. De igual modo concuerda con los resultados de Vinelli (2021) quien manifiesta que la coyuntura de Perú, evidencian en su técnica legislativa la incorporación de disposiciones específicas contra el ciberdelito a través de leyes especiales. Por el contrario, en demás países de la región tomaron la decisión de incluir disposiciones sobre ciberdelincuencia en sus códigos penales. En ocasiones, el ciberdelito se concentra en el nombre que se destina a resguardar jurídicamente cada medio electrónico o la protección de datos e información, y dentro del capítulo que trata sobre crímenes de informática, sin embargo, demás naciones persiguen el estándar técnico-legislativo conservadores, enfocándose en la creación de "eficiencias equivalentes", con lo cual se ha revisado parcialmente el código, adaptando caracteres clásicos delictivos para que pueda ser aplicado para combatir ciberataques. Siendo evidente la preocupación de los encuestados es necesario y urgente iniciar con la

implementación de nuevas figuras legislativas o mejores interpretaciones para combatir contra la fuga de datos personales.

Por último, se presentó la discusión de resultados relacionados al objetivo específico 4, se obtuvo que el 78,6% de los usuarios encuestados consideran que no se ha implementado normas conforme a las recomendaciones del Reglamento General de Protección de Datos para hacer frente a la tecnología 5G, por otro lado, el 21,4% si ha implementado normas conforme a las recomendaciones del Reglamento General de Protección de Datos para hacer frente a la tecnología 5G. Se concluye que no se ha implementado normas conforme a las recomendaciones del Reglamento General de Protección de Datos para hacer frente a la tecnología 5G en Perú, 2021. Por último, se concuerda con los resultados de Celin (2019) quien manifiesta que el término *IoT* se acuñó por primera vez por el pionero de la tecnología británica Kevin Ashton en una presentación realizada en 1999 para la multinacional Procter & Gamble, describiendo un sistema donde los objetos en el mundo físico podrían conectarse a internet mediante sensores para la automatización de acopio de datos, propugnando su aplicación hacia la cadena de suministro. De igual modo se concuerda con Gartner (2017) quien señala que para el 2017 se conectaron 8,400 millones de dispositivos, evidenciando un crecimiento del 31% en comparación al 2016, pasando a la enorme cifra de 20,415 millones de dispositivos habilitados para el 2020; asimismo, la cantidad de dispositivos conectados en todo el mundo pasará de 20,35 billones en 2017 a 75,44 billones para el 2025, evidenciando con ello que el impacto de las tecnologías de *IoT* resulta creciente y sustancial. Resultando evidente que el crecimiento exponencial que tendra esta actualización en el rubro de telecomunicaciones debe ser considerada en agenda de gobierno como lo fue en otros paises como españa; con la finalida de garantizar la adecuada protección de los datos personales de todos los peruanos.

CONCLUSIONES

Primero. - Relacionado al objetivo específico 1. Se describió el nivel de conocimiento de las personas sobre tecnología 5G en las implicancias y riesgos que puede generar sobre sus datos personales, habiéndose complementado el análisis dogmático con una entrevista donde los entrevistados coincidieron en su mayoría que los usuarios no conocen el concepto sobre la tecnología 5G, su implicancia y riesgos que contrae el uso adecuado o inadecuado de los datos personales. Asimismo, el 77,1% de los encuestados indicaron que no existen leyes peruanas que protegen a los usuarios de la tecnología 5G de los contenidos que se distribuye a través de las plataformas sociales por el contrario solo el 16% de encuestados indicaron que, si existen leyes que protegen a los usuarios de la Tecnología 5G, advirtiéndose que hay un pequeño grupo de personas que si conocen la existencia de las leyes que protegen los datos personales. Por lo que se concluye que en su mayoría los usuarios de la tecnología 5G desconocen la existencia de normas que protegen los datos personales de los contenidos que se distribuye a través de las plataformas sociales en Perú.

Segundo. - Relaciona al objetivo específico 2. Se analizó la responsabilidad de Procesamiento de datos personales del usuario por parte de operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G. Complementado con las diversas fuentes y una entrevista, los entrevistados explican que las empresas de telecomunicaciones y proveedoras de servicios tienen conocimiento respecto a la responsabilidad, implicancia y manejo sobre los datos personales. Pero, estas empresas deberán de mejorar el tratamiento seguro y regulado de los datos personales. Además, los 70 usuarios encuestados indicaron que los operadores (75,7%) y empresas de telecomunicaciones (75,7%) de servicios de Tecnología 5G no cuentan con profesionales de seguridad informática para hacer frente a la ciberdelincuencia. Por lo que se concluye que los operadores de servicios de tecnología, proveedores de tecnología 5G y las empresas de telecomunicaciones que venden tecnología 5G no cuentan con profesionales de la seguridad informática para hacer frente a la ciberdelincuencia en Perú, 2021.

Tercero. - Relacionado al objetivo específico 3. Se explicó los alcances jurídicos del RGPDP sobre la seguridad de los datos personales en la tecnología 5G en la manipulación de los datos personales de los usuarios siendo que al haberse complementado con fuentes y una entrevista, la mayoría de los entrevistados concordaron que el RGPDP tiene una ejecución directa sobre el tratamiento de los datos personales dentro de Perú y fuera. Es por ello, que el RGPDP tiene que adecuarse y actualizarse de acuerdo con el avance de las tecnologías digitales en el Perú. Además, el 78,6% de los encuestados sostuvieron que Perú no ha implementado normas conforme a las recomendaciones del Reglamento General de Protección de Datos para hacer frente a la tecnología 5G. Por lo que se concluye, que en la legislación peruana no se han implementado los lineamientos conforme al RGPDP y que como consecuencia las empresas dedicadas a la distribución de tecnología 5G , no informan a sus usuarios exactamente con el propósito de procesar sus datos y no llevan un registro de las actividades realizadas con los datos de sus usuarios, por último, no notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios en Perú.

Cuarto. – Referido al objetivo específico 4. Se propuso la implementación de una modificatoria en las normas peruanas que regulan la protección de datos personales frente a la tecnología 5G. Complementando las fuentes con una entrevista donde la mayoría coincide que no se debería modificar la normativa contemplado en la RGPDP, por lo contrario, se debería de revisar y analizar los lineamientos de la normativa en base a ello si se amerita se podría modificar o implementar a la normativa de RGPDP. Además, el 52,9% de los usuarios encuestados indicaron que, si debiera modificarse las leyes peruanas sobre protección de datos. Por lo que se concluye que, la normativa contemplada en la RGPDP debería de revisarse y analizarse y en base a ello modificarse las leyes peruanas sobre protección de datos personales frente a la tecnología 5G en Perú.

Quinto. - Respecto al objetivo general. Se analizó los alcances jurídicos sobre legislación en seguridad de información personales en la implementación de la Tecnología 5G en Perú. Complementado las fuentes revisadas con una entrevista donde la mayoría coincide al indicar que se deben reforzar las normas referido a la protección de los datos

personales de los ciudadanos en base a las normas internacionales. Asimismo, los 70 usuarios encuestados indicaron en su mayoría (74,3%) que las leyes existentes e implementadas en Perú no protegen la información privada de los usuarios de la Tecnología 5G. Por lo que se concluye que las normas existentes no protegen las informaciónes personales de los usuarios de la tecnología 5G en Perú. De modo que los alcances jurídicos de la legislación nacional no son suficientes para dar la seguridad a los individuos respecto a la protección de sus datos personales, a pesar de que en derecho comparado existan ya avances al respecto.

RECOMENDACIONES

Primero. – Se recomienda, a los pocos operadores de la tecnología 5G y empresas de telecomunicación emplear estrategias de orientación e información con la finalidad de informar y poner en conocimiento las obligaciones de los usuarios y los riesgos de la tecnología 5G. Por otro lado también se recomienda al Ministerio de Transportes y Comunicaciones difundir los beneficios y riesgos de la tecnología 5G de manera pública por los canales de señal abierta.

Segundo. – Se recomienda a los operadores y empresas de telecomunicaciones, contratar personal capacitado en ciberseguridad y seguridad de datos personales a efectos de hacer un mal uso y proceso de datos personales.

Tercero. - Se recomienda a los legisladores complementar las normas referido a la protección de datos personales, en el sentido de que, si el ataque a la privacidad es producto de los nuevos desarrollos tecnológicos, es lógico que los mecanismos tradicionales de protección existentes son insuficientes y debe ser vista como una nueva dimensión.

Cuarto. - Se recomienda a los legisladores fortalecer los estándares reales sobre seguridad de datos personales, incluyendo nuevas modalidades en delitos informáticos perpetrados a partir de la tecnología 5G y que las empresas u operadores sean responsables solidariamente si no han informado respecto a los riesgos.

Quinto. – Se recomienda a partir de los resultados, a los legisladores proponer iniciativas legales con fines de modificar o implementar leyes que protejan los datos personales del usuario sobre tecnología 5G en el Perú.

REFERENCIAS BIBLIOGRÁFICAS

Adachi, F., & Nakajima, N. (2000). Challenges of Wireless Communications, IMT-2000 and Beyond. *IECE TRANS. FUNDAMENTALS, E83-A*(7), 1300-1308. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.29.7502&rep=rep1&type=pdf

AEPD. (mayo de 2020). *Introducción a las tecnologías 5G y sus riesgos para la privacidad.* Agencia Española Protección de Datos: https://www.aepd.es/es/documento/nota-tecnica-privacidad-5g.pdf

Bigelow, S. J. (17 de junio de 2023). *Data privacy (information privacy)*. Techtarget: https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy

Brevo. (17 de june de 2023). *Privacy Policy Personal Data Protection*. Brevo: https://www.brevo.com/legal/privacypolicy/

Celín Barraza, A. (2019). *Modelo de implementación de ciberseguridad para sistemas IoT en el marco de rees 5G.* Universidad Tecnológica de Pereira, Pereira. https://repositorio.utp.edu.co/server/api/core/bitstreams/4ba4ae57-fe91-4853-b841-21c52e403a96/content

CEPAL. (2020). *Gestión de datos de investigación.* Comisión Económica para América Latina y el Caribe. https://biblioguias.cepal.org/c.php?g=495473&p=3390849

Chen, X., Xing, L., Qiu, T., & Li, Z. (2017). An auction-based spectrum leasing mechanism for mobile maccro-femtocell networks of IoT. *Sensors, 17*(2). https://doi.org/https://doi.org/10.3390/s17020380

Compliance Aspekte. (5 de october de 2022). *Difference Between Data Protection and Data Security*. Compliance Aspekte: https://compliance-aspekte.de/en/blog/data-protection-vs-data-security/

Data Privacy Manager. (17 de june de 2023). *5 things you need to know about Data Privacy [Definition & Comparison]*. Data Privacy Manager: https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/

Duque Giraldo, J., & Gómez Flórez, L. (2020). *Derecho a la Protección de Datos personales en la era digital: Comparativo entre las legislaciones de EE. UU, China, España y Brasil con la de Colombia.* Universidad Autónoma Latinoamericana. http://52.170.20.67:8080/bitstream/123456789/1489/1/unaula_rep_pre_der_2020_derecho_proteccion_datos_personales.pdf

EDPB. (2023). *Data protection guide*. The European Data Protection Board: https://edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en

Gartner. (2017). *Las aplicaciones de consumo representarán el 63 % del total de aplicaciones de IoT en 2017.* Gartner, Egham.

Ironpaper. (2016). *Internet of Things Market Statistics - 2016.* Ironpaper, New York. https://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics

Kaspersky. (2018). *Kaspersky Lab presenta su pronóstico de ciberseguridad del 2018 para América Latina.* Kaspersky Lab . https://latam.kaspersky.com/blog/kaspersky-lab-presenta-su-pronostico-de-ciberseguridad-del-2018-para-america-latina/12142/

Liu, X., He, D., & Jia, M. (2017). 5G-based wideband cognitive radio system design with cooperative spectrum sensing. *Physical Communication, 25*(2), 539-545. https://doi.org/https://doi.org/10.1016/j.phycom.2017.09.010

Martel Silva, B. (2020). *Impactos y recomendaciones para el despliegue de las redes 5G en el mercado peruano.* Pontificia Universidad Católica del Perú, Lima. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/18883/MARTEL_SILVA_BORIS_PABLO_IMPACTOS_&_RECOMENDACIONES_PARA_EL_DESPLIEGUE_DE_LAS_REDES_5G.pdf?sequence=1

Martínez Martínez, D. (2017). Unificación de la protección de datos personales en la Unión Europea: Desafíos e implicaciones. *El profesional de la información, 27*(1), 185-194. https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/63285/38571

Miron, A. (22 de August de 2022). *5 Simple Steps to Improve Data Security Compliance*. Polar an IBM Compañy: https://www.polar.security/post/5-simple-steps-to-improve-data-security-compliance

MTC. (2019). *Resolución Ministerial 917-2019 MTC/01.03.* Ministerio de Transportes y Comunicaciones, Lima. https://cdn.www.gob.pe/uploads/document/file/388737/RM_N__917-2019-MTC-01.03.pdf

MTC. (2020). *Estrategias de gestión de espectro radioléctrico: Hacia el desarrollo de nuevas tecnologías y servicios digitales.* Ministerio de Transportes y Comunicaciones, Lima. https://cdn.www.gob.pe/uploads/document/file/469863/Tecnologia_5g__1_.pdf

Nieny Hodar, J. (2021). Desafíos de la tecnología 5G en el ámbito de la ciberseguridad. *Cuaderno de Difusión Pensamiento de Estado Mayor* (45), 79-103. https://revistaensayosmilitares.cl/index.php/cuadernos/article/view/237/216

Pérez Conde, C. (2009). *17392 - Seguridad en sistemas informáticos, 2008/ 2009.* Universitat de Valencia, Valencia.

Reflecfiz. (2 de february de 2023). *The Complete List of Data Security Standards*. Reflecfiz: https://www.reflectiz.com/blog/data-security-standards/

Rodríguez Roncancio, I. (2019). *Nuevos desafíos en seguridad para 5G.* Universidad ECCI, Bogotá. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6830/Nuevos%20desaf%c3%ados%20en%20seguridad%20para%205G.pdf?sequence=1&isAllowed=y

Salas Medina, S. (20 de Octubre de 2022). Alcances de la Legislación Nacional e Internacional sobre la protección de datos personales en la implementación de la Tecnología 5G, Perú 2021. (C. Z. Alvarez Valencia, & K. A. Llerena Ramos, Entrevistadores) Arequipa, Perú.

Salas Medina, S. (20 de Octubre de 2022). Describir el nivel de conocimiento los usuarios de la tecnología 5G en las implicancias y riesgos puede generar sobre sus datos personales. (C. Z. Álvarez Valencia, & K. A. Llerena Ramos, Entrevistadores)

Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Appl. Sci., XII*, 1-22. https://doi.org/10.3390/app12041927

Stouffer, C. (26 de may de 2023). *What is data privacy and why is it important?* LifeLock: https://lifelock.norton.com/learn/identity-theft-resources/what-is-data-privacy-and-why-is-it-important#

Talens Ortiz, Á. (2019). *La protección de datos personales como un derecho fundamental en la era de la tecnología y su protección en el ordenamiento jurídico español.* Universidad de Jaén. https://tauja.ujaen.es/bitstream/10953.1/10829/1/TFG_Alvaro_Talens_2805_.pdf

Valdivia Romero, Á. (20 de Octubre de 2022). Alcance de la Legislación Nacional e Internacional sobre protección de datos personales en la implementación de la Tecnología 5G, Perú 2021. (A. V. Claudia Zarina, & K. A. Llerena Ramos, Entrevistadores)

Valdivia Romero, Á. M. (20 de Octubre de 2022). Describir el nivel de conocimiento los usuarios de la tecnología 5G en las implicancias y riesgos puede generar sobre sus datos personales. (C. Z. Álvarez Valencia, & K. A. Llerena Ramos, Entrevistadores)

Zegarra Torres, R. O. (20 de Octubre de 2022). Describir el nivel de conocimiento los usuarios de la tecnología 5G en las implicancias y riesgos puede generar sobre sus datos personales. (C. Z. Álvarez Valencia, & K. A. Llerena Ramos, Entrevistadores)

Zegarra Torres, R. O., & Llerena Ramos, K. A. (20 de Octubre de 2022). Alcances de la Legislación Nacional e Internacional sobre protección de datos personales en la implementación de la tecnología 5G, Perú 2021. (C. Z. Alvarez Valencia, & K. A. Llerena Ramos, Entrevistadores)

ANEXOS

Anexo 01: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA SEMIESTRUCTURADA

Título: "ALCANCES JURÍDICOS DE LA LEGISLACIÓN NACIONAL E INTERNACIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES EN LA IMPLEMENTACIÓN DE LA TECNOLOGÍA 5G, PERÚ 2021".

Entrevistado: ……..……..

Profesión: ……..……..

Institución: ……..……..

OBJETIVO GENERAL

Analizar los alcances de la legislación sobre protección de datos personales en la implementación de la Tecnología 5G en Perú, 2021.

Preguntas:

1. Según Ud. ¿Cuáles son los alcances jurídicos de la legislación nacional e internacional sobre la protección de datos personales en la implementación de la Tecnología 5G en Perú, 2021? sustentar su respuesta.

……

……

……

OBJETIVO ESPECÍFICO 1

Describir si los usuarios de la tecnología 5G conocen las implicancias que puede generar sobre sus datos personales.

Preguntas:

2. Considera Ud. ¿Qué los usuarios de la tecnología 5G conocen las implicancias que puede generar sobre sus datos personales? sustentar su respuesta.

   ……

   ……

   ……

OBJETIVO ESPECÍFICO 2

Explicar el nivel conocimiento y responsabilidad de los operadores de servicios y empresas de telecomunicaciones y proveedores de la tecnología 5G en la manipulación de los datos personales de los usuarios.

Preguntas:

3. Según Ud. ¿Los operadores de servicios y empresas de telecomunicaciones y proveedores de la tecnología 5g conocen y saben cuál es su responsabilidad en la manipulación de los datos personales de sus usuarios? sustentar su respuesta.

   ……

   ……

   ……

OBJETIVO ESPECÍFICO 3

Explicar los alcances del Reglamento General de Protección de Datos (RGPDP) sobre la seguridad de los datos personales en la tecnología 5G en la legislación peruana.

Preguntas:

4. Según Ud. ¿Cuáles son los alcances jurídicos del RGPDP sobre la seguridad los datos personales en la tecnología 5g en la legislación peruana? sustentar su respuesta.

   ……

   ……

   ……

OBJETIVO ESPECÍFICO 4

Proponer la modificatoria de las normas peruanas que regulan la protección de datos frente a la tecnología 5G.

Preguntas:

5. Considera Ud. ¿Que, es necesario la modificatoria de las normas peruanas que regulan la protección de datos frente a la tecnología 5G, de ser afirmativo indique que norma en específico? sustentar su respuesta.

   ……

   ……

   ……

Cuestionario

"ALCANCES JURÍDICOS DE LA LEGISLACIÓN NACIONAL E INTERNACIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES EN LA IMPLEMENTACIÓN DE LA TECNOLOGÍA 5G, PERÚ 2021".

Instrumentos de recolección de datos

Sres.

Gracias por responder el cuestionario.

Como parte de mi tesis en la Universidad Católica San Pablo, estoy realizando una investigación acerca de la "ALCANCES JURÍDICOS DE LA LEGISLACIÓN NACIONAL E INTERNACIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES EN LA IMPLEMENTACIÓN DE LA TECNOLOGÍA 5G, PERÚ 2021", que consiste en el desarrollo de un cuestionario que no tardará más de cinco minutos en completarla, esta información será de gran valor para el desarrollo de mi investigación.

Los datos que en ella se consignen se tratarán de forma anónima

Por favor marcar con una (X) la alternativa que corresponda con su opinión aplicando la siguiente valoración:

1	2
Si	No

Nº	PREGUNTA	1	2
Alcances Jurídicos de la legislación sobre la protección de datos personales			
Usuarios de la tecnología 5G			
1	Considera usted ¿Qué las leyes existentes e implementadas en Perú protege los datos personales de los usuarios de la tecnología 5G?		
2	Cree usted ¿Qué existen leyes peruanas que le protegen a los usuarios de la tecnología 5G de los contenidos que se distribuye a través de las plataformas sociales?		
Responsabilidad de los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G			
3	Cree usted ¿Qué, los operadores de servicios de tecnología 5G cuentan con profesionales de la seguridad informática para hacer frente a la ciberdelincuencia?		
4	Según usted ¿Las empresas de telecomunicaciones que venden tecnología 5G cuentan con profesionales de seguridad informática para frente a la ciberdelincuencia?		
5	Según usted ¿Las empresas de telecomunicaciones y proveedores de tecnología 5G cuentan con profesionales de seguridad informática para frente a la ciberdelincuencia?		
Alcances Jurídicos de la RGPDP			
6	Cree usted ¿Qué, Perú ha implementado normas conforme a las recomendaciones del Reglamento General de Protección de Datos para hacer frente a la tecnología 5G?		
7	Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G, informan a sus usuarios con precisión la finalidad del tratamiento de sus datos?		
8	Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G llevan un registro de las actividades realizadas con los datos de sus usuarios?		
9	Según usted ¿Los operadores de servicios, empresas de telecomunicaciones y proveedores de tecnología 5G notifican de manera inmediata sobre toda brecha de seguridad o violación a los datos personales de sus usuarios?		
Modificatoria de las normas			
10	Según usted ¿Se deben modificar las leyes peruanas sobre protección de datos para hacerlas más eficientes frente a la ciberdelincuencia para los usuarios de tecnología 5G?		