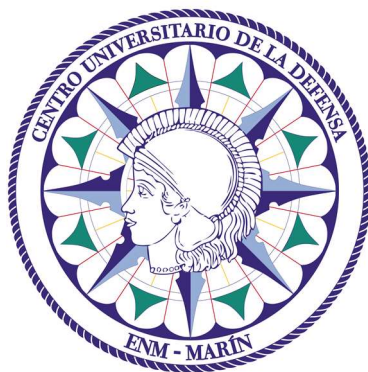




Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Protección de datos en el ámbito de las telecomunicaciones

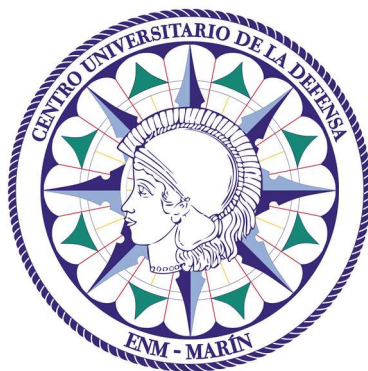
Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Francisco Javier Jiménez Ciudad

DIRECTORES: Aitor Sabino Atorrasagasti Morato
José Pablo González Coma

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Protección de datos en el ámbito de las telecomunicaciones

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

RESUMEN

El trabajo aborda el panorama de la protección de datos en telecomunicaciones, destacando el impacto positivo del Reglamento general de protección de datos (RGPD), aunque subraya que su implementación sigue siendo deficiente, especialmente en el ámbito transfronterizo y en grandes plataformas tecnológicas. A pesar de las multas impuestas, no siempre son disuasorias para las grandes empresas.

Además, el avance de tecnologías emergentes como la inteligencia artificial (IA) y el internet de las cosas, “*internet of things*” (*IoT*) ha introducido nuevas vulnerabilidades, lo que demanda la actualización constante de la normativa. El estudio también resalta el conflicto entre seguridad y privacidad en las comunicaciones, indicando que las medidas de seguridad no deben comprometer los derechos de los usuarios. A nivel empresarial, las grandes empresas han avanzado en la adopción de buenas prácticas, pero las pequeñas y medianas enfrentan dificultades para cumplir con las normativas.

Para mejorar la protección de datos en telecomunicaciones, se proponen varias recomendaciones. En primer lugar, avanzar hacia la armonización global de normativas liderada por la UE, con acuerdos internacionales basados en el RGPD para abordar las discrepancias legales entre países. En segundo lugar, reforzar la supervisión de las normativas actuales mediante sanciones proporcionales, controles estrictos y mecanismos que garanticen el cumplimiento. Además, se destacan campañas educativas masivas, utilizando redes sociales e “influencers”, para concienciar sobre los riesgos del mal uso de datos. Finalmente, se recomienda que las empresas inviertan en infraestructuras nacionales y sistemas de detección basados en IA y “*Machine learning*” (*ML*) y apoyar a las pequeñas y medianas Empresas (PYMES) con recursos, formación y herramientas adaptadas.

PALABRAS CLAVE

Protección de datos personales, privacidad, ciberseguridad, inteligencia artificial (IA), Reglamento general de protección de datos (RGPD).

AGRADECIMIENTOS

Me gustaría expresar en primer lugar mi más sincero agradecimiento por el apoyo y esfuerzo realizado en el seguimiento continuo del trabajo por parte de mis directores, el capitán jurídico D. Aitor Sabino Atorrasagasti Morato y D. José Pablo Gonzalez Coma.

En segundo lugar, me gustaría agradecer la colaboración realizada por parte del capitán de fragata D. Manuel Suarez García, D^a Virginia Gallardo Fernández y D^a Laura Méndez Dalmas destinados en el Cuartel General de la Armada, en la jefatura de sistemas de la información y telecomunicaciones (JECIS) dentro del grupo de seguridad de la información (GRUSEGINFO).

Finalmente, quiero agradecer al teniente de navío D. Francisco Javier Picón Sebastián destinado en la oficina del delegado de protección de datos del Ministerio de Defensa dentro del Gabinete Técnico de la Subsecretaría de Defensa por su asesoramiento en todos los aspectos relacionados con el trabajo.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	4
1 Introducción.....	5
1.1 Justificación del tema.....	5
1.2 Objetivos.	6
1.3 Metodología.	6
2 Estado del arte	8
2.1 Evolución histórica.	8
2.1.1 Evolución histórica de la protección de datos.	8
2.1.2 Conceptos clave.	8
2.1.3 Principales normas en el marco nacional e internacional.	9
2.2 Investigaciones y enfoques teóricos.....	11
2.2.1 Impacto de las tecnologías emergentes en la protección de datos.....	12
2.2.2 Herramientas y tecnologías actuales.....	13
2.2.3 Brechas en el conocimiento y oportunidades de investigación. [17].....	15
2.2.4 Desafíos y tendencias actuales.....	15
2.2.5 Teoría y enfoques relevantes en el ámbito de la protección de datos.....	17
2.2.6 Modelos de implementación.....	17
2.3 Situación actual y tendencia en la protección de datos.	19
2.3.1 Panorama global del sector.....	19
2.3.2 Estudio de casos recientes.	21
2.3.3 Retos y amenazas actuales.....	26
3 Implementación de la protección de datos en telecomunicaciones	32
3.1 Medidas técnicas y organizativas.....	32
3.1.1 Medidas técnicas.....	32
3.1.2 Medidas organizativas.	33
3.2 Evaluación de impacto relativa a la protección de datos (EIPD) [25].....	33
3.3 Gestión de Incidentes de Seguridad.....	35
3.3.1 Definición y tipología de incidentes.	35
3.3.2 Proceso de gestión de incidentes.	36
3.4 Sanciones por incumplir el RGPD y la LOPDGDD.....	37
4 Estudio Comparativo.....	39

4.1 Comparativa Internacional (UE, EEUU y Canadá).	39
4.1.1 Normativas en Europa.	39
4.1.2 Estados Unidos. La Ley de privacidad del consumidor de California [10].	39
4.1.3 Canadá. Ley de protección de información personal y documentos electrónicos. [30] ...	40
4.1.4 Comparativa general	40
4.2 Mejores Prácticas.	41
4.2.1 Cifrado de extremo a extremo.	41
4.2.2 Minimización de datos.	42
4.2.3 Transparencia y control para los usuarios.	43
4.2.4 Auditorías regulares y cumplimiento proactivo.	44
4.2.5 Gestión de los datos personales.	44
5 Resultados y Discusión	46
5.1 Análisis de los hallazgos	46
5.1.1 Regulaciones existentes en protección de datos y su aplicación en las comunicaciones.	46
5.1.2 Vulnerabilidades en el tratamiento de datos en comunicaciones digitales.	46
5.1.3 Tensión entre seguridad y privacidad.	46
5.1.4 Adopción de buenas prácticas de protección de datos.	46
5.2 Discusión crítica.	47
5.2.1 Evaluación de las políticas actuales.	47
5.2.2 Desafíos tecnológicos y su impacto.	47
5.2.3 Conflicto entre intereses comerciales y derechos de los usuarios	48
5.2.4 Recomendaciones para mejorar la protección de datos	48
6 Conclusiones y líneas futuras	51
6.1 Conclusiones	51
6.2 Líneas futuras.	52
Bibliografía.	53
Anexo I: Evolución de multas en España.	56
Anexo II: Sanciones por incumplimiento del RGPD.	57

ÍNDICE DE FIGURAS

Figura 2-1. Evolución normativa en protección de datos en España [13]	11
Figura 2-2. Data Protection Impact Assessment (DPIA) Data Wheel [14].....	12
Figura 2-3. Lista de herramientas disponibles en la web de la AEPD [16].....	14
Figura 2-4. Arquitectura propuesta para proteger datos y gestionar identidades de drones [19].....	16
Figura 2-5. Principios de la privacidad desde el diseño [20].....,	21
Figura 3-1. Ciclo de vida de respuesta a ciberincidentes [26].....	36
Figura 4-1. Panel de control de privacidad de Google [32].....	43
Figura A1-1. Evolución de multas impuestas en España. [28]	56
Figura A1-2. Multas superiores al millón de euros en resolución firme y ejecutiva. [28].....	56
Figura A1-3. Áreas con mayor importe global de multas. [28].....	56
Figura A2-1. Número de sanciones y cantidades acumuladas desde 2018. [31].....	57
Figura A2-2. Sanciones más altas por países. [31].....	57
Figura A2-3. Sanciones más altas por empresas. [31].....	58
Figura A2-4. Sanciones más altas por sectores. [31].....	58
Figura A2-5. Sanciones más altas por tipo de violación. [31].....	59

ÍNDICE DE TABLAS

Tabla 2-1. Resumen de las capas y protocolos de encriptación.....20

Tabla 2-2. Niveles de riesgo según el Reglamento de IA de la UE.....28

Tabla 3-1. Resumen de infracciones y multas de la LOPD y el RGPD. [27].....38

Tabla 4-1. Características principales de las aplicaciones de mensajería.....42

1 INTRODUCCIÓN

1.1 Justificación del tema.

En la era digital en la que vivimos, la protección de los datos personales se ha convertido en una piedra angular de las relaciones entre empresas y consumidores. Este fenómeno no es sólo resultado del crecimiento exponencial de la información digital, sino también de la cada vez mayor interconectividad de dispositivos y redes, evidente en las telecomunicaciones. Como facilitador de la comunicación y la transmisión de datos, la industria de las telecomunicaciones desempeña un papel clave en la protección de la privacidad y la seguridad de la información.

La progresiva dependencia de los servicios de telecomunicaciones, impulsada por tecnologías emergentes como el 5G, el Internet de las Cosas (*IoT*), y el “*Big Data*”, ha creado un aumento exponencial en la cantidad de datos que se recogen, procesan y transmiten a través de estas redes. Estos datos, que pueden contener desde información personal y de ubicación hasta hábitos de consumo y preferencias, son de gran valor tanto para las empresas como para los ciberdelincuentes. En este contexto, la protección de datos no es solo un asunto de cumplimiento legal, sino también un elemento clave para mantener la confianza del consumidor y la integridad del sistema de telecomunicaciones.

La implementación del Reglamento (UE) 2016/679 [1] [2] [3] (RGPD) del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ha marcado un antes y un después en la manera en que las empresas de telecomunicaciones deben manejar los datos personales. Esta regulación, que entró en vigor en mayo de 2018, ha establecido un marco legal riguroso que busca proteger los derechos de los ciudadanos sobre sus datos personales, imponiendo obligaciones claras a las empresas en términos de transparencia, consentimiento, y medidas de seguridad. Sin embargo, la rápida evolución tecnológica y las diferencias en la aplicación de regulaciones a nivel global plantean desafíos significativos para el sector.

Por otro lado, la importancia de la protección de datos en las telecomunicaciones no solo se limita a la perspectiva legal, sino que también tiene un impacto directo en la reputación de las empresas. Los incidentes de seguridad que resultan en brechas de datos pueden tener consecuencias devastadoras, no solo en términos de multas y sanciones, sino también en la pérdida de confianza por parte de los usuarios. Este es un factor crítico en un sector donde la confianza en la seguridad y la privacidad de las comunicaciones es fundamental para la relación con el cliente.

Además, la protección de datos en el ámbito de las telecomunicaciones es un tema de gran relevancia a nivel global, dado que muchas empresas del sector operan en múltiples países con diferentes marcos regulatorios. Esta diversidad normativa añade complejidad a la gestión de datos, lo que exige un enfoque integral y coordinado para garantizar la conformidad con las diferentes Leyes de protección de datos a nivel local e internacional.

La selección de este tema para el TFM se justifica, por tanto, por la necesidad de comprender en profundidad los desafíos a los que se enfrentan las organizaciones y las empresas de telecomunicaciones en relación con la protección de datos y las estrategias que se deben implementar para cumplir con las normativas vigentes y proteger la información de sus usuarios. Asimismo, es crucial explorar cómo las tecnologías emergentes están remodelando el panorama de la protección de datos y qué medidas pueden adoptarse para mitigar los riesgos asociados.

1.2 Objetivos.

El presente trabajo de fin de máster tiene como objetivo principal examinar en profundidad el marco normativo y las prácticas de protección de datos en el sector de las telecomunicaciones, con un enfoque particular en la adaptación a las normativas actuales y la implementación de medidas de seguridad efectivas. Para alcanzar este objetivo general, se plantean los siguientes objetivos específicos:

- a. **Analizar las normativas de protección de datos aplicables al sector de las telecomunicaciones.** Este objetivo busca realizar un análisis exhaustivo de las Leyes y regulaciones que afectan al sector, con especial atención al RGPD en Europa, así como a otras normativas relevantes a nivel global. Se examinarán los requisitos que estas normativas imponen a las empresas de telecomunicaciones y cómo estas empresas están respondiendo a dichos requisitos.
- b. **Evaluar las medidas de protección de datos adoptadas por las empresas de telecomunicaciones.** Este objetivo se centra en investigar las estrategias y tecnologías que las empresas de telecomunicaciones están implementando para proteger los datos personales de sus usuarios. Esto incluirá un análisis de las prácticas de seguridad de datos, como la encriptación, la anonimización, y las políticas de acceso y control de datos.
- c. **Identificar los principales desafíos en la implementación de la protección de datos en el sector de las telecomunicaciones.** En este apartado, se examinarán los desafíos a los que se enfrentan las empresas al intentar cumplir con las normativas de protección de datos, incluyendo dificultades técnicas, organizativas y regulatorias. Además, se analizarán los impactos de las nuevas tecnologías, como el 5G, el *IoT* y la IA en la protección de datos.
- d. **Proponer recomendaciones para mejorar la protección de datos en el sector de las telecomunicaciones.** A partir del análisis realizado, se buscará formular recomendaciones prácticas para las empresas de telecomunicaciones y los reguladores, con el fin de mejorar la protección de datos en el sector. Estas recomendaciones se basarán en las mejores prácticas identificadas durante la investigación y en las necesidades específicas del sector.

1.3 Metodología.

Para abordar los objetivos mencionados, este TFM ha utilizado una metodología que combina el análisis documental con el estudio de casos y la evaluación de medidas prácticas implementadas en el sector de las telecomunicaciones.

- a. **Revisión de documentación.** La primera fase del trabajo ha consistido en una revisión exhaustiva de la documentación existente sobre la protección de datos en las telecomunicaciones. Esta revisión incluye la evaluación de artículos científicos, informes técnicos, y estudios de caso que proporcionan una base sólida para el análisis posterior, prestando especial atención a la evolución de las normativas de protección de datos y su impacto en el sector.
- b. **Análisis normativo.** Análisis detallado de las normativas de protección de datos más relevantes para el sector de las telecomunicaciones, con un enfoque particular en el RGPD y otras Leyes internacionales. Este análisis incluye una evaluación de los requisitos legales que deben cumplir las empresas y cómo estas normativas afectan a sus operaciones diarias.
- c. **Estudio de casos.** Se han seleccionado varios casos de estudio de empresas de telecomunicaciones que han implementado medidas destacables en la protección de datos o que se han enfrentado a desafíos significativos en este ámbito. Estos estudios de caso permiten

identificar prácticas exitosas y lecciones aprendidas, proporcionando ejemplos concretos de cómo las empresas pueden mejorar su protección de datos.

- d. **Entrevistas con expertos.** Para complementar el análisis documental, se realizan entrevistas con expertos en protección de datos. Estas entrevistas proporcionan una visión práctica y actualizada sobre los desafíos y oportunidades en la protección de datos en telecomunicaciones.
- e. **Análisis comparativo.** Análisis comparativo de las políticas de protección de datos en diferentes regiones o países.
- f. **Elaboración de recomendaciones.** Finalmente, basado en los hallazgos obtenidos a través de la revisión de la bibliografía, el análisis normativo, los estudios de casos y las entrevistas, se formulan recomendaciones prácticas para mejorar la protección de datos en el sector de las telecomunicaciones. Estas recomendaciones están orientadas tanto a las empresas del sector como a los reguladores y otras partes interesadas.

2 ESTADO DEL ARTE

2.1 Evolución histórica.

2.1.1 Evolución histórica de la protección de datos.

La protección de datos es un campo que ha evolucionado significativamente en las últimas décadas, impulsado por el avance de la tecnología y el creciente reconocimiento de la importancia de la privacidad. Históricamente, la protección de datos surgió como una respuesta a las preocupaciones sobre la capacidad de las organizaciones para recopilar y procesar información personal a gran escala. A medida que las tecnologías de la información y la comunicación (TIC) se desarrollaron, la cantidad y el tipo de datos que podían recopilarse, almacenarse y analizarse aumentaron exponencialmente, lo que generó la necesidad de establecer normativas que protegieran la privacidad de los individuos.

La protección de datos personales es un derecho fundamental reconocido en el artículo 18.4 de la Constitución española de 1978. Desde sus inicios, la Constitución buscó proteger la intimidad personal y familiar limitando el uso de la informática para salvaguardar los derechos de los ciudadanos. Esto fue enfatizado en varias sentencias del Tribunal Constitucional como la STC 254/1993 [4] y la STC 292/2000 [5] declarando que la protección de datos es un derecho fundamental independiente, aunque relacionado con la intimidad. Asimismo, las personas tienen el poder de decidir sobre el acceso y uso de su información personal y el uso de datos personales debe respetar los principios de proporcionalidad y finalidad.

Uno de los primeros hitos en la historia de la protección de datos fue la adopción de la Ley de protección de datos de Suecia en 1973 [6], que es ampliamente reconocida como la primera legislación nacional dedicada a este tema. Esta Ley estableció un precedente al introducir principios como la transparencia en la recopilación de datos y la necesidad de obtener el consentimiento de las personas afectadas. Posteriormente, en 1981, el Convenio 108 del Consejo de Europa se convirtió en el primer tratado internacional legalmente vinculante sobre la protección de datos personales, estableciendo un marco para la protección de la privacidad en los países europeos.

Con el avance de internet y las telecomunicaciones en la década de 1990, se hizo evidente la necesidad de una normativa más robusta. La Directiva 95/46/CE [7] de la Unión Europea supuso un paso significativo en la armonización de las Leyes de protección de datos en los Estados miembros. Esto culminó en la adopción del Reglamento (UE) 2016/679 RGPD y la Directiva (UE) 2016/680 [8]. El RGPD corrigió las limitaciones de la Directiva 95/46/CE, reforzando la seguridad jurídica y garantizando que los estados miembros adapten su legislación para ofrecer coherencia y claridad.

El Reglamento de la Unión Europea establece un marco normativo uniforme para todos los Estados miembros con el fin de garantizar un alto nivel de protección de los datos personales en todos los sectores, incluyendo las telecomunicaciones. Introduce principios clave para el tratamiento de datos, como la transparencia, la minimización de datos, la exactitud y la integridad de los mismos.

Las empresas de telecomunicaciones que operan en la Unión Europea, o que manejan datos de ciudadanos europeos, deben cumplir con estas exigencias, independientemente de su sede. Esto incluye obtener el consentimiento explícito para el tratamiento de los datos personales y garantizar su seguridad a través de medidas técnicas y organizativas apropiadas, como el cifrado y la seudonimización.

2.1.2 Conceptos clave.

Protección de datos. La protección de datos se refiere al conjunto de políticas, procedimientos y tecnologías diseñados para garantizar la privacidad de los datos personales, protegerlos de accesos no autorizados, y cumplir con las regulaciones vigentes. En el contexto de las telecomunicaciones, esto implica proteger la gran cantidad de información personal que se transmite a través de redes de comunicación, incluyendo datos sensibles como localización, historial de llamadas, y patrones de uso de internet.

Privacidad. La privacidad es el derecho que tienen las personas a controlar la información sobre sí mismas y a decidir cómo se recopila, almacena y utiliza dicha información. En el sector de las telecomunicaciones, la privacidad se ve afectada por la cantidad masiva de datos que las empresas recopilan de los usuarios, lo que plantea importantes desafíos en términos de cómo se maneja y protege esta información.

Ciberseguridad. La ciberseguridad se refiere a la protección de los sistemas informáticos y las redes contra el acceso no autorizado, los ataques y el daño a los datos. En las telecomunicaciones, la ciberseguridad es fundamental para proteger las redes y los datos transmitidos a través de ellas, especialmente en un entorno en el que los ciberataques son cada vez más sofisticados y frecuentes.

Datos personales. Los datos personales son cualquier información relacionada con una persona física identificada o identificable. Esto incluye nombres, direcciones, números de teléfono, direcciones de correo electrónico, así como datos más sensibles como información bancaria, historial médico y comportamiento en línea. En el contexto de las telecomunicaciones, los datos personales incluyen tanto la información proporcionada directamente por los usuarios como la generada por el uso de los servicios.

Reglamento general de protección de datos. El RGPD es una regulación de la Unión Europea que establece un marco legal para la protección de los datos personales de los ciudadanos. Introduce conceptos como el consentimiento explícito, el derecho al olvido y la obligatoriedad de notificar a las autoridades y a los afectados en caso de una brecha de seguridad. Su implementación ha tenido un impacto significativo en el sector de las telecomunicaciones, obligando a las empresas a adoptar medidas más estrictas para proteger los datos de sus usuarios.

Anonimización y seudonimización. La anonimización es el proceso mediante el cual se eliminan o modifican los datos personales de manera que no puedan ser vinculados a una persona específica, incluso si se dispone de información adicional. La seudonimización, en cambio, implica sustituir los identificadores en los datos por seudónimos, de manera que los datos no puedan atribuirse a un individuo sin información adicional, la cual figura por separado y está sujeta a medidas técnicas y organizativas que garantizan que los datos no se atribuyan a una persona física identificada o identificable. Ambos procesos son cruciales en las telecomunicaciones para mitigar el riesgo de exposición de los datos personales.

2.1.3 Principales normas en el marco nacional e internacional.

Además del RGPD, la Directiva *ePrivacy* de la UE¹ [9], también conocida como la Directiva sobre privacidad y comunicaciones electrónicas, complementa el RGPD en el ámbito de las telecomunicaciones. Esta directiva regula el tratamiento de datos en las comunicaciones electrónicas, y cubre áreas como las cookies, el marketing directo y la confidencialidad de las comunicaciones. La revisión de esta directiva, conocida como el Reglamento *ePrivacy*, está en proceso de aprobación y busca modernizar la normativa para adaptarse a los nuevos desafíos tecnológicos, como el *IoT* y la IA.

Existen otras normativas internacionales que son relevantes en el ámbito de la protección de datos en telecomunicaciones. Entre ellas se incluyen la Ley de privacidad del consumidor de California, “*California Consumer Privacy Act*” (CCPA) [10], la Ley de protección de datos personales de Brasil, “*Lei Geral de Proteção de Dados*” (LGPD) [11], y la Ley de protección de la información personal de Japón [12].

La CCPA, que entró en vigor en enero de 2020, es una de las Leyes más estrictas de Estados Unidos en cuanto a la protección de datos personales. Aunque está enfocada principalmente en las empresas que operan en California, su influencia se ha extendido a nivel nacional e internacional, ya que muchas

¹ Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37)

empresas han adoptado sus principios como una buena práctica global. La *CCPA* otorga a los consumidores derechos amplios sobre sus datos personales, incluyendo el derecho a saber qué información se recopila, el derecho a eliminarla y el derecho a optar por no venderla.

La LGPD de Brasil, por otro lado, ha sido comparada frecuentemente con el RGPD debido a su estructura y principios similares. Implementada en 2020, la LGPD regula el tratamiento de datos personales en Brasil y ha establecido un marco para la protección de la privacidad en una de las economías más grandes de América. Esta Ley es particularmente relevante para las empresas de telecomunicaciones que operan en Brasil, ya que deben cumplir con requisitos estrictos sobre cómo recopilan, almacenan y comparten los datos de los usuarios.

En Asia, la Ley de protección de la información personal de Japón es un ejemplo importante de cómo las normativas de protección de datos están evolucionando en la región. Japón ha reforzado esta Ley en los últimos años para alinearse más estrechamente con los estándares internacionales, como el RGPD, lo que ha facilitado acuerdos de transferencia de datos entre la UE y Japón. Estas normativas reflejan una tendencia global hacia una mayor regulación en la protección de datos, que tiene un impacto directo en las empresas de telecomunicaciones que operan a nivel internacional.

El RGPD establece normas comunes para la protección de datos personales en la UE, respondiendo a los desafíos de la era digital, donde los flujos de información y el uso de datos personales han aumentado exponencialmente. A pesar de su aplicabilidad directa, el Reglamento requiere desarrollo y adaptación en cada país, incluyendo en España, para asegurar su plena implementación. El RGPD representa un marco legal avanzado que ha influido no solo en Europa, sino también en otras regiones del mundo, al establecer estándares altos para la protección de datos y al imponer sanciones severas por el incumplimiento.

A nivel legislativo, según la figura 2-1 [13], la primera Ley española que abordó este derecho fue la Ley Orgánica 5/1992, conocida como LORTAD (Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal). Esta Ley fue reemplazada por la Ley Orgánica 15/1999 para adaptarse a la Directiva 95/46/CE de la Unión Europea, que buscaba armonizar la protección de datos en toda Europa sin restringir la libre circulación de estos. Este marco europeo se complementa con el artículo 8 de la carta de los derechos fundamentales de la Unión Europea del 7 de diciembre del 2000 y el artículo 16.1 del tratado de funcionamiento de la Unión Europea de 1985.

La protección de datos en el ámbito de las telecomunicaciones en España y a nivel internacional es un aspecto clave en la regulación de la privacidad y la seguridad de la información. A nivel nacional, España cuenta con la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), que adapta el RGPD de la Unión Europea, y proporciona una regulación adicional en áreas específicas. En el sector de las telecomunicaciones, esta normativa es fundamental, ya que los operadores gestionan grandes volúmenes de datos sensibles sobre los usuarios, como información personal, geolocalización, comunicaciones y preferencias de consumo.

La LOPDGDD tiene como objetivo garantizar que los derechos fundamentales relacionados con la protección de los datos personales se respeten en todos los ámbitos, incluyendo las telecomunicaciones. Esta Ley se complementa con la Ley 11/2022, de 28 de junio, General de Telecomunicaciones (LGT), que tiene como objetivo actualizar el marco regulador de las telecomunicaciones en España. Entre sus aspectos más importantes, destaca la promoción de la conectividad digital, el despliegue de redes 5G, la protección de los usuarios y el fomento de la competencia en el sector. También aborda la ciberseguridad y el acceso universal a los servicios de telecomunicaciones, garantizando que todos los ciudadanos, independientemente de su ubicación, tengan acceso a estos servicios esenciales.

Uno de los puntos clave de la LOPDGDD, junto con el RGPD, es que otorga a los ciudadanos derechos reforzados sobre el uso de sus datos personales. Estos incluyen el derecho a acceder, rectificar, suprimir, y oponerse al tratamiento de sus datos, así como el derecho a la portabilidad y la limitación del tratamiento. Además, se introducen garantías especiales para los datos sensibles y medidas específicas

en el ámbito digital, como el derecho a la desconexión laboral, muy relevante en el entorno de las telecomunicaciones.

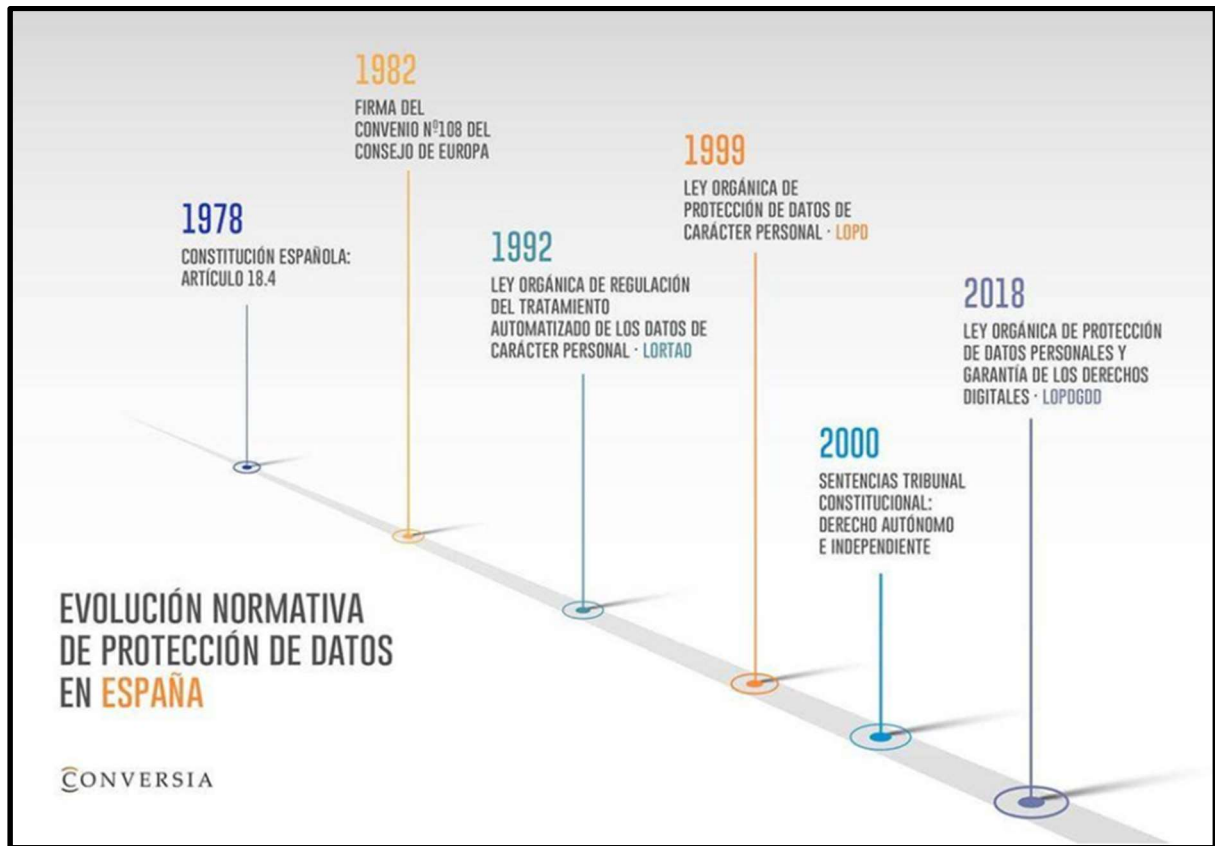


Figura 2-1. Evolución normativa en protección de datos en España. [13]

2.2 Investigaciones y enfoques teóricos.

En el ámbito académico, la protección de datos en telecomunicaciones ha sido objeto de numerosas investigaciones que abordan tanto los desafíos técnicos como los aspectos legales y éticos.

Un enfoque común en la investigación es el estudio de las técnicas de anonimización y seudonimización como mecanismos para proteger la privacidad de los usuarios sin comprometer la utilidad de los datos. Estas técnicas son fundamentales en las telecomunicaciones, donde los datos de los usuarios son esenciales para la operación y mejora de los servicios, pero al mismo tiempo deben protegerse para cumplir con las normativas de privacidad. Estudios recientes han explorado métodos avanzados de anonimización que buscan preservar la utilidad de los datos para el análisis, mientras minimizan el riesgo de identificación de individuos.

Otro tema importante es la gestión de incidentes de seguridad y las respuestas a las brechas de datos en las telecomunicaciones. Dado que este sector maneja datos sensibles a gran escala, las investigaciones han centrado su atención en el desarrollo de protocolos eficientes para la detección, respuesta y mitigación de incidentes de seguridad. Un estudio del “SysAdmin Audit, Networking and Security Institute” (SANS) con sede en Bethesda (Maryland, Estados Unidos) del año 2020 analiza cómo las empresas de telecomunicaciones pueden implementar estrategias proactivas para la ciberseguridad, destacando la importancia de la IA y el aprendizaje automático por su acrónimo en inglés “Machine Learning” (ML) en la detección de amenazas.

Además, la evaluación del impacto de privacidad, “Data Protection Impact Assessment” (DPIA) ha sido un área de creciente interés, particularmente en el contexto de las telecomunicaciones. DPIA es una

herramienta preventiva que permite a las empresas identificar y mitigar riesgos de privacidad antes de que se implementen nuevos procesos o tecnologías. Recientes investigaciones sobre *DPIA* han desarrollado marcos adaptados a telecomunicaciones para gestionar los riesgos específicos de este sector. Entre ellos se encuentra el modelo *DPIA* “*Data Wheel*”, según figura 2-2 [14], que ofrece una guía contextual para evaluar riesgos de privacidad, especialmente útil en sistemas interconectados.

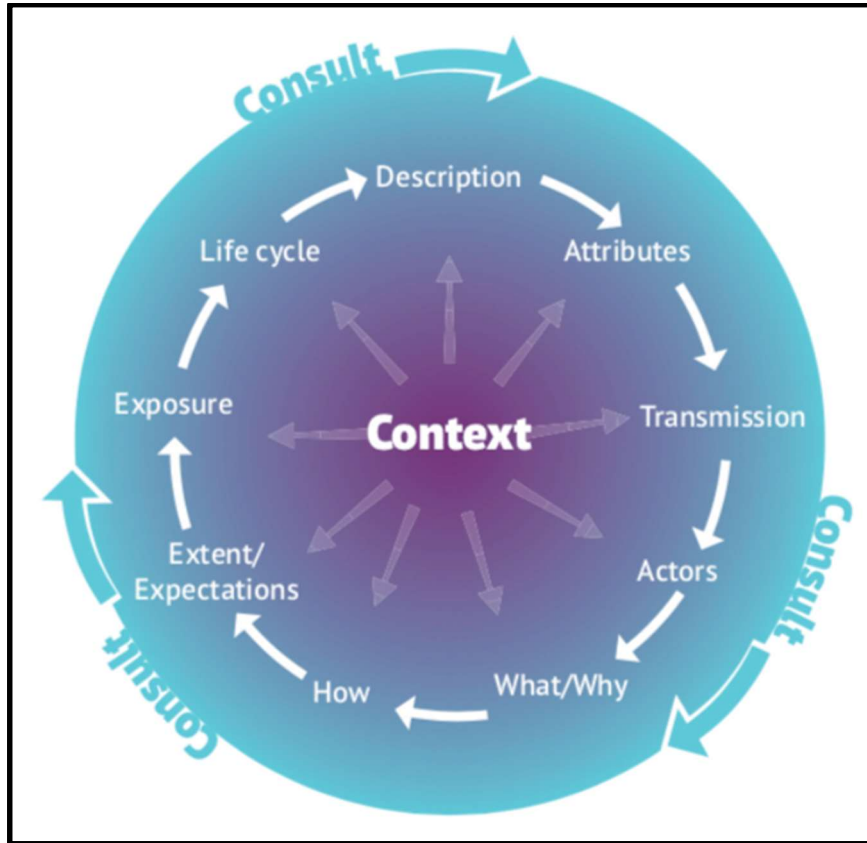


Figura 2-2. “Data Protection Impact Assessment Data Wheel”. [14]

Otro enfoque de la investigación es el uso de la IA y el *ML* en la protección de datos. La IA se utiliza cada vez más en telecomunicaciones para gestionar grandes volúmenes de datos y optimizar redes. Sin embargo, esto también plantea desafíos en términos de protección de datos, ya que los algoritmos de IA requieren acceso a datos personales para funcionar correctamente. Se han explorado los riesgos y beneficios del uso de IA en telecomunicaciones, sugiriendo que las empresas deben equilibrar la eficiencia tecnológica con la protección de la privacidad.

2.2.1 Impacto de las tecnologías emergentes en la protección de datos.

La quinta generación de redes móviles, conocida como 5G, representa un avance significativo en la velocidad y capacidad de las comunicaciones inalámbricas. Sin embargo, también plantea nuevos desafíos a las empresas de telecomunicaciones en términos de protección de datos [15]. El 5G permite conectar un número mucho mayor de dispositivos al mismo tiempo y a una velocidad mucho más rápida que las generaciones anteriores. Esto es especialmente relevante para el *IoT*, que abarca dispositivos como sensores, electrodomésticos inteligentes, cámaras de seguridad o incluso vehículos conectados. Al estar todos estos dispositivos comunicándose constantemente entre sí y con servidores, se genera y transmite una gran cantidad de datos.

Este aumento masivo en el tráfico de datos trae consigo grandes oportunidades, como hogares más inteligentes y ciudades más eficientes, pero también plantea importantes desafíos en términos de seguridad. Las empresas de telecomunicaciones se ven obligadas a adoptar medidas mucho más avanzadas para proteger estos datos, ya que cualquier vulnerabilidad podría ser explotada por ciberdelincuentes. Un ciberataque no solo podría comprometer la privacidad de los usuarios, sino que

también podría interrumpir sistemas esenciales conectados a la red, como el transporte, la salud, o la energía, lo que podría tener consecuencias graves. Por eso, la seguridad es una prioridad en el desarrollo y despliegue de redes 5G, para garantizar que esta tecnología sea segura y confiable para todos.

El *IoT* se refiere a la interconexión de dispositivos físicos que recopilan y transmiten datos a través de internet. Estos dispositivos, que van desde sensores y electrodomésticos hasta vehículos y sistemas industriales, generan una cantidad importante de datos personales y de comportamiento. En el ámbito de las telecomunicaciones, la gestión segura de estos datos es crítica. Los dispositivos *IoT* a menudo tienen capacidades de seguridad limitadas, lo que los hace vulnerables a ataques. Además, la recopilación masiva de datos por parte de estos dispositivos plantea preocupaciones sobre la privacidad, ya que los usuarios pueden no ser conscientes de la cantidad de información que se recopila y cómo se utiliza.

El uso de “*Big Data*” y analítica avanzada permite analizar grandes volúmenes de datos para extraer información valiosa sobre el comportamiento del usuario, optimizar redes y mejorar servicios. Sin embargo, el procesamiento de grandes cantidades de datos personales presenta riesgos significativos para la privacidad. La identificación de individuos a partir de datos anónimos es un riesgo potencial, y el uso de datos para la toma de decisiones automatizadas plantea preocupaciones sobre la igualdad y la discriminación. Las empresas deben implementar medidas adecuadas para garantizar que el uso de “*Big Data*” respete los principios de protección de datos, como el consentimiento informado y la minimización de datos.

La computación en la nube “*cloud computing*” permite a las empresas almacenar y procesar datos en servidores remotos, lo que ofrece flexibilidad y escalabilidad. Sin embargo, también plantea desafíos de seguridad y privacidad, especialmente en el sector de las telecomunicaciones, donde la confidencialidad de los datos es crítica. El uso de servicios en la nube puede implicar la transferencia de datos a través de fronteras internacionales, lo que requiere que las empresas cumplan con regulaciones de protección de datos en múltiples jurisdicciones. Además, la seguridad de los datos en la nube depende en gran medida de las medidas de seguridad implementadas por los proveedores de servicios en la nube, lo que hace necesario que las empresas seleccionen cuidadosamente a sus proveedores y establezcan acuerdos contractuales claros que garanticen la protección de los datos.

La IA y el *ML* se utilizan cada vez más en las telecomunicaciones para optimizar redes, personalizar servicios y mejorar la experiencia del usuario. Sin embargo, estos sistemas a menudo requieren el procesamiento de grandes cantidades de datos personales, lo que plantea desafíos en términos de privacidad y protección de datos. Además, los algoritmos de IA pueden tomar decisiones que afectan a los usuarios, lo que plantea cuestiones sobre la transparencia y la responsabilidad. Las empresas de telecomunicaciones deben asegurarse de que los sistemas de IA se diseñen y operen de manera que cumplan con las normativas de protección de datos y respeten los derechos de los usuarios.

2.2.2 Herramientas y tecnologías actuales.

En respuesta a los desafíos y tendencias actuales, se han desarrollado diversas herramientas y tecnologías para mejorar la protección de datos en el sector de las telecomunicaciones. Entre las más relevantes se encuentran:

1. Cifrado de extremo a extremo, “*End-to-End Encryption*” (*E2EE*). Esta tecnología asegura que los datos se cifren en el origen y solo se descifren en el destino, lo que impide que los intermediarios accedan a la información durante la transmisión. En las telecomunicaciones, el *E2EE* se ha convertido en un estándar para proteger las comunicaciones sensibles, especialmente en aplicaciones de mensajería y voz.

2. Soluciones de gestión de identidades y accesos, “*Identity and Access Management*” (*IAM*). Las soluciones *IAM* permiten a las empresas gestionar de manera segura las identidades digitales y controlar

el acceso a los recursos de la red. Estas herramientas son esenciales en telecomunicaciones, donde el acceso no autorizado a redes y datos puede tener consecuencias graves.

3. Sistemas de detección y respuesta ante amenazas “*Endpoint Detection and Response*” (*EDR*). Los sistemas *EDR* utilizan IA y análisis de comportamiento para detectar y responder a amenazas en tiempo real. Estos sistemas son cada vez más utilizados en telecomunicaciones para proteger las redes contra ciberataques avanzados.

4. Plataformas de cumplimiento normativo. Con la creciente complejidad de las normativas de protección de datos, las plataformas de cumplimiento normativo han surgido como herramientas clave para ayudar a las empresas de telecomunicaciones a cumplir con las Leyes de privacidad. En la *web* de la Agencia Española Protección de Datos (AEPD), según figura 2-3 [16], se encuentran a disposición de las empresas y profesionales que traten datos personales las siguientes herramientas para ayudar a cumplir con las obligaciones en materia de protección de datos: Facilita RGPD, Facilita EMPRENDE, Gestiona RGPD, Canal del DPD, Comunica-Brecha RGPD, Evalúa-Riesgo RGPD v2, Asesora Brecha y ValidaCripto RGPD.

5. “*Blockchain*”: Aunque tradicionalmente está asociado con las criptomonedas, la tecnología “*Blockchain*” se está explorando como una herramienta para asegurar el intercambio de datos en telecomunicaciones. Su capacidad para proporcionar un registro inmutable y transparente de transacciones lo convierte en una opción atractiva para la protección de datos en redes distribuidas.

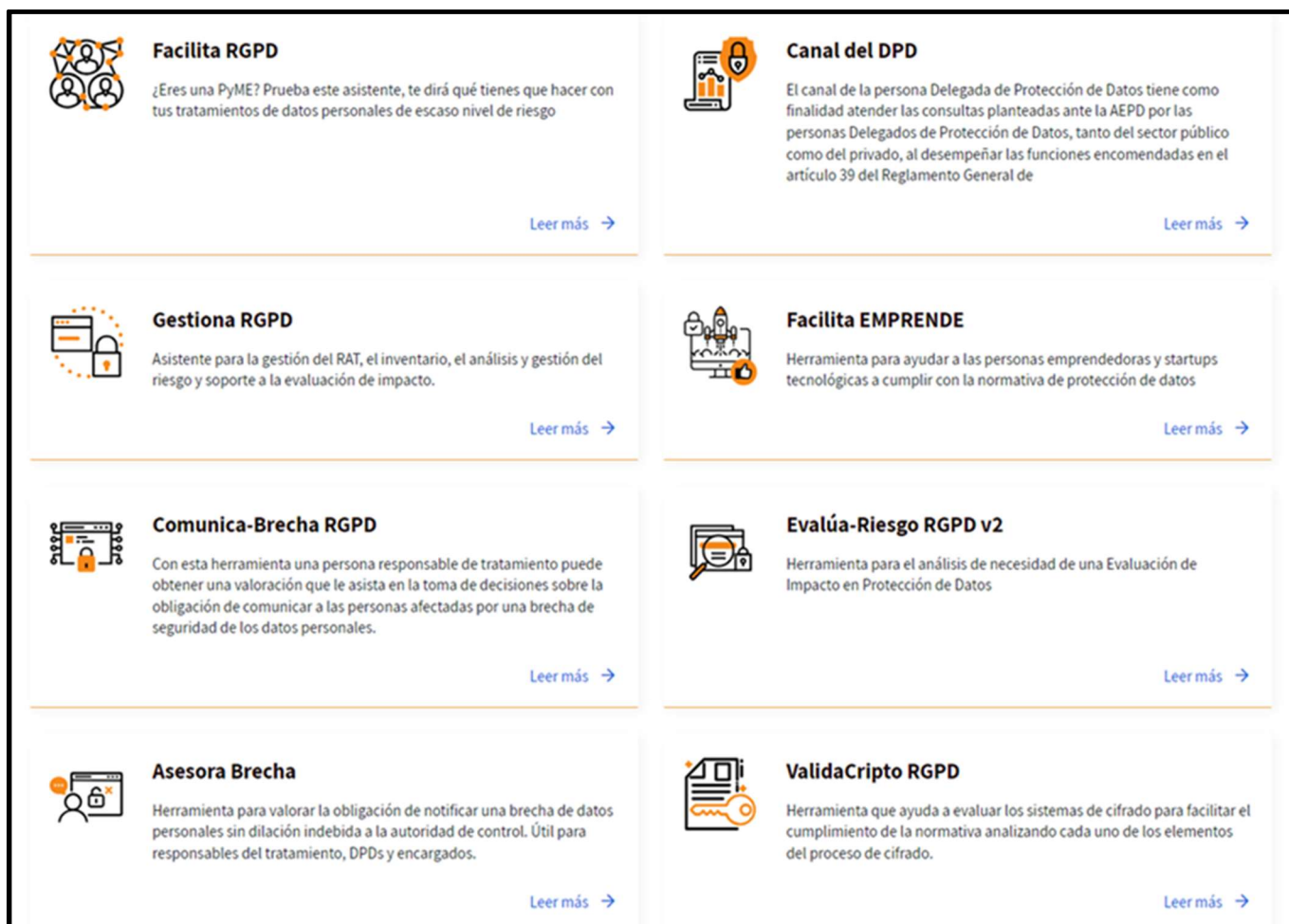


Figura 2-3. Lista de herramientas disponibles en la *web* de la AEPD. [16]

2.2.3 Brechas en el conocimiento y oportunidades de investigación. [17]

A pesar de los avances significativos en la protección de datos en telecomunicaciones, todavía existen brechas en el conocimiento que representan oportunidades de investigación. Una de estas brechas es la protección de datos en el contexto de las redes 5G e *IoT*. Aunque se han realizado estudios sobre la seguridad en 5G, la integración con *IoT* introduce nuevos riesgos que aún no están completamente solucionados. Actualmente, se están llevando a cabo investigaciones para abordar los desafíos de seguridad que surgen con la convergencia de las redes 5G y el *IoT*.

Estas investigaciones se enfocan en crear soluciones específicas para proteger los datos en entornos altamente interconectados, teniendo en cuenta la vulnerabilidad de muchos dispositivos *IoT* y la complejidad de las infraestructuras 5G. Se están desarrollando protocolos de seguridad que combinan criptografía avanzada con técnicas de autenticación ligera, adecuados para dispositivos con recursos limitados. Además, se exploran tecnologías como “*blockchain*” para garantizar la trazabilidad y la integridad de los datos, así como la aplicación de IA para la detección proactiva de amenazas en tiempo real.

Otra área que requiere más investigación es la efectividad de las técnicas de anonimización y seudonimización. Si bien estas técnicas son esenciales para la protección de la privacidad, existe un debate sobre su capacidad para prevenir la identificación, especialmente cuando se combinan con “*Big Data*” y técnicas avanzadas de análisis.

Además, la interacción entre la IA y la privacidad sigue siendo un área relativamente nueva y poco explorada. Dado el papel creciente de la IA en telecomunicaciones, es crucial investigar cómo se puede desarrollar y utilizar la IA de manera que respete los principios de protección de datos, evitando sesgos y garantizando la transparencia en la toma de decisiones automatizadas.

Finalmente, la convergencia de las normativas internacionales de protección de datos representa una oportunidad de investigación importante. A medida que las empresas de telecomunicaciones operan globalmente, necesitan navegar por un panorama regulatorio complejo. La investigación en este campo podría enfocarse en desarrollar marcos y directrices que faciliten el cumplimiento normativo de las Leyes de protección de datos. Esto incluiría herramientas y estrategias que permitan a las empresas gestionar eficazmente los riesgos asociados al tratamiento de datos personales en redes 5G e *IoT*, garantizando tanto la seguridad como la privacidad. Además, sería clave abordar la interoperabilidad de estas normativas con estándares internacionales, fomentando una protección de datos sólida a nivel global.

2.2.4 Desafíos y tendencias actuales.

El sector de las telecomunicaciones se enfrenta a desafíos específicos en la protección de datos debido a la naturaleza global y compleja de sus operaciones. Uno de los mayores retos es la implementación de normativas de protección de datos en un entorno que debe cumplir con diversas regulaciones internacionales y estándares de seguridad. Esto implica desarrollar estrategias de gestión que garanticen la privacidad y la integridad de los datos, alineándose con marcos legales como el RGPD en Europa, y adaptándose a las particularidades legales de cada región donde operan las empresas del sector.

Otro desafío importante es la seguridad de las redes 5G. A medida que las redes 5G se despliegan globalmente, ofrecen velocidades más rápidas y conectividad mejorada, lo que permite el crecimiento del *IoT*. Sin embargo, estas redes también amplían la superficie de ataque para los ciberdelincuentes, lo que requiere nuevas estrategias de protección de datos. Una de las investigaciones recientes que explora la seguridad de redes 5G usando “*Blockchain*” es un estudio del “*Institute of Electrical and Electronics Engineers*” (IEEE) con sede en la ciudad de New York. Esta investigación propone un sistema basado

en “*Blockchain*” para proteger datos y gestionar identidades de drones, mitigando riesgos de ataques como el de tipo *Sybil*² y controlando el acceso a datos sensibles. [18] [19]

La investigación presenta un método para identificar ataques en redes de drones conectados, conocidos como internet de las cosas voladoras, por sus siglas en inglés “*Internet of Flying Things*” (*IoFT*). Estos ataques tal y como se observan en la figura 2-4 [19], consisten en que un solo atacante suplante varias identidades de nodos en la red, generando posibles amenazas a la integridad de los datos y la seguridad del sistema. Este método introduce un enfoque basado en *ML* para mejorar la detección de estos ataques, aprovechando características de señal y patrones de comportamiento.

La investigación se centra en detectar anomalías de identidad mediante el uso de datos físicos de capa de red, como el “*Time Difference of Arrival*” (*TDoA*) y la “*Received Signal Strength Difference*” (*RSSD*). Esto permite diferenciar entre nodos legítimos y falsos sin necesidad de autenticar continuamente las identidades, reduciendo así el consumo de energía y aumentando la eficiencia. Además, el modelo propuesto realiza simulaciones que confirman la efectividad del método al aplicar algoritmos de clasificación en entornos de *IoFT*, demostrando su aplicabilidad a redes de drones que requieren alta movilidad y seguridad.

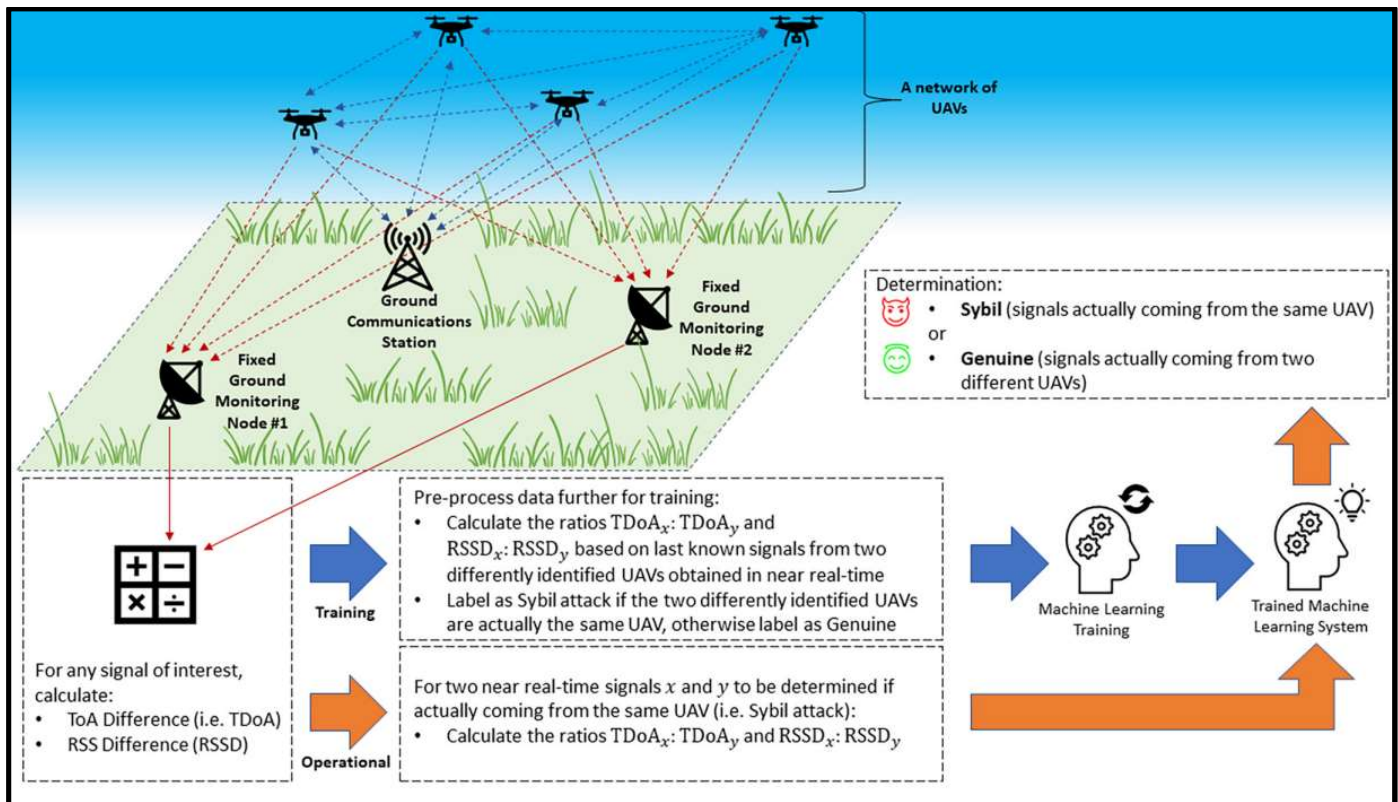


Figura 2-4. Arquitectura propuesta para proteger datos y gestionar identidades de drones. [19]

La gestión de datos en la nube también representa un desafío clave. Con el aumento del uso de la computación en la nube por parte de las empresas de telecomunicaciones, resulta crítico garantizar la seguridad de los datos almacenados y procesados en los servidores. Los estudios han señalado la

² Un ataque *Sybil* es un tipo de ataque en redes y sistemas descentralizados donde un atacante crea múltiples identidades falsas (o nodos) para ganar influencia o controlar el sistema. En contextos como el *Blockchain* y redes 5G, este tipo de ataque es particularmente peligroso, ya que permite al atacante comprometer la integridad y la seguridad de los datos que se manejan en la red.

importancia de seleccionar proveedores de servicios en la nube que cumplan con las normativas de protección de datos y que ofrezcan garantías robustas de seguridad.

2.2.5 Teoría y enfoques relevantes en el ámbito de la protección de datos.

Enfoque de la protección de la información. El enfoque de la protección de la información se centra en cómo se debe proteger la información desde su creación hasta su destrucción. Este enfoque es fundamental para entender los principios que guían la protección de datos en telecomunicaciones, ya que las empresas deben implementar políticas y tecnologías que aseguren la confidencialidad, integridad y disponibilidad de la información a lo largo de su ciclo de vida. En este contexto, se emplean diversos modelos, como el modelo de confidencialidad, integridad y disponibilidad, “*confidentiality, integrity and availability*” (CIA) que proporciona un marco para garantizar la seguridad de los datos.

Enfoque del consentimiento informado. Este enfoque sostiene que los individuos deben tener el control sobre cómo se recopilan, usan y comparten sus datos personales. El consentimiento informado es un principio clave del RGPD, que exige que las empresas obtengan un consentimiento explícito de los usuarios antes de recopilar y procesar sus datos. En las telecomunicaciones, donde los datos se recopilan constantemente, esta teoría es esencial para garantizar que los usuarios sean conscientes de cómo se manejan sus datos y que tienen el poder de revocar su consentimiento en cualquier momento.

Enfoque de gestión de riesgos en ciberseguridad. La gestión de riesgos en ciberseguridad implica la identificación, evaluación y mitigación de los riesgos asociados a la protección de datos y la seguridad de la información. Este enfoque es particularmente relevante en el sector de las telecomunicaciones debido a la creciente amenaza de ciberataques. Las empresas de telecomunicaciones deben implementar estrategias de gestión de riesgos que incluyan medidas preventivas, como la encriptación de datos y la implementación de “*firewalls*”, así como planes de respuesta a incidentes para minimizar el impacto de posibles brechas de seguridad.

Teoría de la responsabilidad proactiva. Introducida por el RGPD, la teoría de la responsabilidad proactiva establece que las organizaciones no solo deben cumplir con las normativas de protección de datos, sino que también deben ser capaces de demostrar este cumplimiento. Esto significa que las empresas de telecomunicaciones deben mantener registros detallados de cómo protegen los datos, realizar evaluaciones de impacto de privacidad cuando sea necesario, y estar preparadas para responder a auditorías por parte de las autoridades de protección de datos.

Enfoque de privacidad por diseño. Este enfoque sostiene que la protección de la privacidad debe integrarse en el diseño de los sistemas y procesos desde el principio, en lugar de añadirse como una medida correctiva. En el sector de las telecomunicaciones, esto implica que las redes y los servicios deben diseñarse teniendo en cuenta la privacidad de los usuarios, garantizando que los datos personales estén protegidos en todas las etapas del procesamiento.

2.2.6 Modelos de implementación.

Modelo de seguridad multicapa. Este modelo se basa en la implementación de múltiples capas de seguridad para proteger los datos en las telecomunicaciones. Cada capa de seguridad actúa como una barrera que debe superarse para acceder a los datos, lo que aumenta la dificultad para los atacantes y reduce el riesgo de brechas de seguridad. Las capas pueden incluir la encriptación de datos, la autenticación de usuarios, el monitoreo de redes, y la segmentación de la red. Este enfoque es esencial en las telecomunicaciones, donde los datos viajan a través de redes públicas y privadas y son susceptibles a diferentes tipos de amenazas.

Los algoritmos de cifrado sólidos son esenciales para garantizar la seguridad de los datos. Utilizan funciones matemáticas complejas y claves criptográficas para cifrar y descifrar la información, lo que dificulta a los atacantes obtener acceso a los datos protegidos. La fortaleza del cifrado no solo depende del algoritmo utilizado, sino también de la gestión segura de las claves. Es vital que las claves se generen, almacenen y roten de manera segura, limitando el acceso únicamente a personal autorizado.

El cifrado de extremo a extremo asegura que los datos estén protegidos desde su origen hasta su destino. Solo el destinatario final puede descifrar los datos, lo que impide que cualquier intermediario, como proveedores de servicios o atacantes, acceda a la información. Algunos servicios como “*WhatsApp*” utilizan este enfoque para proteger las comunicaciones.

Las técnicas de enmascaramiento de datos y tokenización añaden una capa adicional de seguridad. El enmascaramiento reemplaza los datos sensibles con valores ficticios, mientras que la tokenización sustituye los datos sensibles por símbolos de identificación únicos que conservan toda la información esencial de los datos sin comprometer su seguridad. Ambas prácticas son útiles en entornos donde se comparten o procesan datos, asegurando que la información original no pueda ser explotada por atacantes.

La protección de los datos durante su transmisión es tan importante como su almacenamiento seguro. Existen protocolos como “*Hypertext Transfer Protocol Secure*” HTTPS y “*Virtual Private Network*” (VPN) que establecen canales de comunicación cifrados, asegurando que la información no pueda ser interceptada ni manipulada durante su traslado a través de redes públicas o privadas.

Las soluciones de prevención de datos, “*Data Loss Prevention*” (DLP) también ayudan a prevenir la fuga de información confidencial mediante la inspección de contenido, el control de acceso y el cifrado. Estas soluciones detectan posibles riesgos de pérdida de datos y aplican políticas de seguridad para mitigar las vulnerabilidades, ayudando a las organizaciones a proteger la integridad de su información.

La evaluación de impacto de privacidad es una herramienta utilizada para identificar y mitigar los riesgos de privacidad asociados con el procesamiento de datos personales. En el sector de las telecomunicaciones, es particularmente relevante debido a la gran cantidad de datos que se procesan y a los riesgos inherentes a las tecnologías emergentes como el 5G y el *IoT*. La realización de una evaluación de impacto de privacidad permite a las empresas identificar posibles vulnerabilidades en sus sistemas y procesos y tomar medidas para mitigarlas antes de que se produzcan problemas de privacidad.

El modelo de gestión de incidentes de seguridad se centra en la identificación, respuesta y recuperación ante incidentes de seguridad que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos. En las telecomunicaciones, un incidente de seguridad puede tener consecuencias amplias, afectando no solo a la empresa sino también a sus usuarios. El modelo incluye la detección proactiva de amenazas, la implementación de procedimientos de respuesta rápida, y la recuperación y análisis posterior para prevenir futuros incidentes.

El enfoque “*Zero Trust*” se basa en la premisa de que ninguna parte de la red es completamente segura, y, por lo tanto, todas las solicitudes de acceso deben ser verificadas y autenticadas de manera rigurosa. Este enfoque es especialmente relevante en el contexto de las telecomunicaciones, donde las redes están constantemente expuestas a amenazas internas y externas. Implementar un enfoque “*Zero Trust*” implica segmentar la red, aplicar políticas de acceso estrictas, y monitorear continuamente todas las actividades en la red para detectar y responder a posibles amenazas.

2.3 Situación actual y tendencia en la protección de datos.

2.3.1 Panorama global del sector.

La protección de datos en el ámbito de las telecomunicaciones se ha convertido en un tema de máxima prioridad a nivel mundial debido al creciente volumen de datos que se generan y manejan, así como al aumento de la complejidad de los ciberataques. Las telecomunicaciones, que abarcan desde la telefonía móvil y fija hasta las redes de datos, son fundamentales en la infraestructura digital global. Este sector maneja información altamente sensible, lo que lo convierte en un objetivo clave para los ciberataques y plantea importantes desafíos en términos de protección de datos.

En el panorama global, las regulaciones de protección de datos han experimentado un notable avance, impulsado principalmente por la adopción del Reglamento general de protección de datos en la Unión Europea en 2018. El Reglamento ha establecido un estándar riguroso que ha influido en otras legislaciones alrededor del mundo.

A nivel de telecomunicaciones, estas normativas tienen un impacto significativo. Las empresas del sector deben asegurar que sus procesos de recopilación, almacenamiento y tratamiento de datos cumplen con las exigencias legales de las diferentes jurisdicciones en las que operan. Esto incluye la implementación de medidas de seguridad robustas, como la encriptación de datos y la gestión de consentimientos, así como la preparación para la notificación rápida en caso de brechas de seguridad.

La encriptación de datos convierte la información legible en un formato codificado que solo puede ser descifrado mediante una clave o algoritmo específico, lo que asegura que, incluso si los datos son interceptados durante su transmisión, no puedan ser leídos por personas no autorizadas.

Existen dos tipos principales de encriptación, encriptación simétrica, en la que la misma clave se utiliza tanto para cifrar como para descifrar los datos, y encriptación asimétrica, que emplea una clave pública para cifrar y una clave privada para descifrar, lo que añade una capa extra de seguridad. Además, las empresas deben gestionar adecuadamente las claves de cifrado, asegurando que estas estén protegidas y actualizadas regularmente para evitar vulnerabilidades.

En el ámbito de las telecomunicaciones, la encriptación se aplica en diferentes capas de la red. Cada capa tiene su propio enfoque y protocolos para garantizar la seguridad de los datos en tránsito. Los diferentes protocolos de encriptación que existen aparecen resumidos en la tabla 2-1 y son los siguientes:

Encriptación a nivel de aplicación: en este nivel, la encriptación se aplica directamente a los datos que se están transmitiendo. Los datos se cifran antes de ser enviados a través de la red y se descifran en el destino final. Es particularmente útil cuando se quiere proteger la información de manera específica, independientemente de la red que se utilice.

Encriptación en capa de transporte: “*Transport Layer Security/Secure Sockets Layer*” (*TLS/SSL*). Esta encriptación se utiliza para proteger las comunicaciones entre dos puntos de la red, como entre un navegador web y un servidor. Se asegura de que los datos no sean interceptados o alterados durante el tránsito. El protocolo criptográfico *TLS* es el sucesor de *SSL* y es el protocolo más común para cifrar la comunicación en línea, como en las conexiones “*HyperText Transfer Protocol Secure*” (*HTTPS*). Aunque *SSL* es menos utilizado hoy en día, *SSL* fue el predecesor de *TLS* y todavía es conocido en algunos contextos, aunque es menos seguro que *TLS*.

El objetivo de *HTTPS* es asegurar que los datos transmitidos estén protegidos frente a posibles interceptaciones y ataques, como el de tipo “*man-in-the-middle*”, en el cual un atacante intercepta y

altera la comunicación. Al emplear *HTTPS*, la información se cifra antes de ser enviada, lo que impide que cualquier tercero no autorizado pueda leerla.

Además, *HTTPS* garantiza la autenticidad del servidor, permitiendo a los usuarios confirmar que están accediendo a un sitio web legítimo y no a uno falso creado con el fin de robar datos. En los navegadores actuales, los sitios que utilizan *HTTPS* se identifican con un candado verde en la barra de direcciones, lo que indica que la conexión es segura.

Encriptación en capa de red: en el nivel de red, los paquetes de datos se cifran directamente. Este tipo de encriptación es utilizada en redes privadas y para la creación de redes privadas virtuales “*Virtual Private Network*” (*VPN*). Protege toda la comunicación entre dispositivos de red, incluso si atraviesa varias redes intermedias. “*Internet Protocol Security*” (*IPsec*) cifra los paquetes de datos IP y puede usarse en *VPNs* para asegurar las conexiones entre dos puntos remotos, como una oficina y una red corporativa. *IPsec* asegura que todos los paquetes, sin importar su tipo o la aplicación que los genere, estén cifrados mientras atraviesan la red.

Encriptación en capa de enlace de datos: a nivel de la capa de enlace de datos, la encriptación se utiliza para proteger la comunicación entre dispositivos en una red local, como redes Wi-Fi. Esto es importante para evitar que los atacantes puedan interceptar o manipular los datos dentro de una red local. “*Wi-Fi Protected Access*” (*WPA/WPA2*): estos protocolos protegen las redes inalámbricas, asegurando que la información transmitida entre dispositivos (como entre un teléfono y un router) esté cifrada. WPA2 es el estándar más seguro y utiliza el cifrado *Advanced Encryption Standard* (*AES*).

Encriptación en capa de enlace físico: la encriptación de la capa física se utiliza para proteger los datos a nivel de enlace, especialmente cuando se transmite información a través de redes cableadas o de alta velocidad. El protocolo “*Media Access Control Security*” (*MACsec*) cifra los datos que se transmiten a través de enlaces en redes de alta velocidad. Asegura que los datos estén protegidos entre dispositivos conectados directamente, como switches o routers.

Capa de la Red	Protocolo de Encriptación	Descripción
Aplicación.	Cifrado de aplicaciones web.	Cifra los datos en la capa de la aplicación (correo electrónico, servicios web).
Transporte.	TLS, SSL.	Protege la comunicación entre un servidor y un cliente (ejemplo <i>HTTPS</i>).
Red.	IPsec.	Cifra los paquetes IP en la capa de red, protegiendo toda la comunicación a través de la red (ejemplo <i>VPNs</i>).
Enlace de datos.	WPA, WPA2.	Cifra los datos transmitidos en redes inalámbricas, protegiendo la comunicación en redes Wi-Fi.
Física.	MACsec.	Cifra los datos transmitidos a través de enlaces físicos, asegurando la transmisión en redes de alta velocidad.

Tabla 2-1. Resumen de las capas de red y protocolos de encriptación.

Las organizaciones también deben tener en cuenta los datos generados por tecnologías emergentes como el *IoT* y las redes 5G. Estas tecnologías generan un volumen masivo de datos, lo que aumenta el riesgo de infracciones de la privacidad si no se implementan adecuadamente las medidas de seguridad necesarias. En este contexto, el cumplimiento normativo ya no es suficiente; las empresas deben adoptar enfoques proactivos para la protección de datos, incorporando los principios funcionales de la privacidad desde el diseño “*Privacy by Design*” de sus sistemas y productos, según aparece en la figura 2-5 [20]

Principios Fundacionales de la Privacidad desde el Diseño
1. Proactivo, no reactivo; Preventivo, no correctivo
2. La privacidad como configuración predeterminada
3. Privacidad incorporada en la fase de diseño
4. Funcionalidad total: pensamiento “todos ganan”
5. Aseguramiento de la privacidad en todo el ciclo de vida.
6. Visibilidad y transparencia
7. Enfoque centrado en el sujeto de los datos

Figura 2-5. Principios de la privacidad desde el diseño. [20]

Esto implica integrar la protección de la privacidad en el diseño de sistemas desde el principio, en lugar de agregar medidas de seguridad después de que se han desarrollado los productos. Es especialmente relevante en la era del *IoT*, donde los dispositivos conectados recopilan y transmiten datos continuamente. Los estudios recientes en España han subrayado la importancia de este enfoque para prevenir problemas de privacidad y cumplir con las normativas de protección de datos de manera proactiva.

La conciencia del usuario sobre la privacidad es un área de creciente interés. A medida que los consumidores se vuelven más conscientes de sus derechos de privacidad, las empresas de telecomunicaciones se enfrentan a la presión de ser transparentes sobre cómo recopilan y utilizan los datos personales. Mantener una comunicación clara y transparente con los usuarios es esencial para generar confianza y cumplir con las expectativas de privacidad.

A pesar del avance en las normativas y la creciente conciencia sobre la importancia de la protección de datos, el sector de las telecomunicaciones sigue enfrentando desafíos importantes. Las diferencias entre las legislaciones de protección de datos a nivel internacional pueden complicar la operación global de las empresas de telecomunicaciones, ya que deben cumplir con regulaciones a menudo incompatibles o contradictorias. Además, la rápida evolución de las tecnologías de la información y la comunicación plantea constantemente nuevos riesgos que las legislaciones existentes no siempre están preparadas para abordar.

2.3.2 Estudio de casos recientes.

Para comprender mejor la situación actual de la protección de datos en telecomunicaciones, es útil analizar casos recientes de empresas que se han enfrentado a desafíos significativos o que han

implementado medidas destacables en este ámbito. A continuación, se presentan cuatro estudios de caso representativos.

Caso 1. Brecha de Seguridad en “Verizon” (2017)³.

En 2017, “*Verizon Communications Inc*”, una de las principales empresas de telecomunicaciones en Estados Unidos, experimentó una brecha de seguridad significativa que expuso los datos personales de varios millones de clientes. La causa del incidente fue una configuración incorrecta en la nube de “*Amazon Web Services*” (AWS), utilizada por un proveedor externo contratado por “*Verizon*”.

La brecha reveló información como nombres, direcciones y números de teléfono, pero lo más preocupante fue que los “*Personal Identification Number*” (PIN) de cuenta también se vieron comprometidos, lo que podría haber permitido a los atacantes acceder a las cuentas de los clientes. Este incidente subrayó la importancia de la gestión segura de los datos en la nube, especialmente en un sector como las telecomunicaciones, donde se maneja información crítica.

Como respuesta, “*Verizon*” reforzó sus políticas de seguridad, especialmente en lo que respecta a la colaboración con proveedores externos. Este caso pone de manifiesto la necesidad de implementar controles estrictos y continuos sobre cómo se configuran y manejan los datos en plataformas de terceros, así como la importancia de las auditorías regulares de seguridad.

Según estándares como el “*International Organization for Standardization and International Electrotechnical Commission*” ISO/IEC 27001 [21] o el “*National Institute of Standards and Technology (NIST) Cybersecurity Framework*”, los controles que se deberían implementar, para garantizar la seguridad de los datos manejados en plataformas de terceros y evitar este tipo de brechas de seguridad son los siguientes: gestión de la relación con proveedores, gestión de configuración de sistemas, auditorías y monitoreo continuo, protección de datos, gestión de incidentes de seguridad y concienciación y capacitación

Uno de los aspectos clave es la gestión de la relación con proveedores, lo que incluye establecer acuerdos contractuales claros que detallen las obligaciones de seguridad y cumplimiento normativo, como el RGPD o el CCPA. Además, es necesario realizar evaluaciones previas para identificar riesgos antes de formalizar la relación y mantener un monitoreo continuo de las actividades del proveedor, asegurando que cumplan con las políticas de seguridad establecidas.

La configuración adecuada de los sistemas es otro pilar esencial. Esto implica adoptar controles de acceso basados en roles, asegurando que cada usuario solo tenga los permisos mínimos necesarios, y realizar un “*hardening*”⁴ de los sistemas para eliminar configuraciones predeterminadas o deshabilitar servicios innecesarios. Asimismo, es crucial llevar a cabo pruebas regulares de vulnerabilidad que permitan identificar y corregir configuraciones débiles o susceptibles a ataques.

Las auditorías y el monitoreo continuo son indispensables para detectar y prevenir amenazas. La realización de auditorías de seguridad regulares permite comprobar que los proveedores cumplen con los estándares requeridos, mientras que el monitoreo en tiempo real ayuda a identificar actividades sospechosas o anómalas en las plataformas de terceros. También es importante revisar de manera periódica los registros de actividad para analizar posibles incidentes y fortalecer los controles.

³ <https://www.upguard.com/breaches/verizon-cloud-leak>

⁴ “*hardening*”: es el proceso de asegurar un sistema, red o aplicación mediante la eliminación de vulnerabilidades y la configuración de ajustes de seguridad más estrictos.

La protección de los datos requiere la implementación de medidas como el cifrado, tanto en tránsito como almacenados, garantizando que se cumplan los estándares de seguridad actuales. Además, la clasificación de los datos sensibles facilita su tratamiento con niveles de protección adecuados, y el uso de herramientas de prevención de pérdida de datos como pueden ser el bloqueo del envío de datos confidenciales por correo o USB, la identificación de datos sensibles en la red o dispositivos y no enviar información a servicios en la nube no autorizados, ayuda a evitar filtraciones accidentales o malintencionadas.

Por último, gestionar de manera eficiente los incidentes de seguridad es esencial. Es necesario contar con un plan de respuesta a incidentes específico para situaciones relacionadas con proveedores, asegurando notificaciones rápidas ante cualquier brecha de seguridad y realizando revisiones post-incidentes para identificar la causa raíz y mejorar los controles. Complementariamente, la concienciación y capacitación de los proveedores, a través de formaciones y simulacros de seguridad, refuerza el cumplimiento de las políticas establecidas y eleva el nivel general de protección de los datos.

Caso 2. Incidente de protección de datos de Rikunabi (2019)⁵.

El incidente de protección de datos de Rikunabi, una plataforma japonesa de búsqueda de empleo, se produjo en 2019 cuando se reveló que la empresa vendió información personal de los usuarios sin su consentimiento. Rikunabi utilizó un algoritmo que predecía la probabilidad de que los candidatos rechazaran una oferta de trabajo y vendió estos datos a las empresas que utilizaban su plataforma, violando la normativa de protección de datos en Japón. Aproximadamente 8,000 usuarios se vieron afectados por esta práctica, lo que generó una fuerte crítica pública y repercusiones legales.

Como resultado del incidente, el gobierno japonés y la agencia de protección de información personal intervinieron, ordenando a Rikunabi mejorar sus prácticas de gestión de datos y revisar sus políticas de privacidad. Además, la empresa matriz de Rikunabi, “*Recruit Holdings*”, emitió disculpas públicas y comenzó a trabajar en un plan de compensación para los usuarios afectados. La situación dejó en evidencia la falta de transparencia en el manejo de datos personales y puso en tela de juicio la ética de las empresas en el uso de algoritmos predictivos.

Este caso también provocó un mayor examen sobre el uso de la IA y los algoritmos en la toma de decisiones que afectan a las personas, lo que llevó a Japón a reforzar su legislación de protección de datos. La situación de Rikunabi se convirtió en un referente importante para la discusión global sobre privacidad y el manejo de información personal en el entorno digital.

Para fortalecer su legislación sobre protección de datos, Japón implementó en 2020 importantes enmiendas a la Ley de protección de la información personal “*Act on the Protection of Personal Information*” (APPI), adoptando un enfoque más riguroso hacia el manejo de datos personales, especialmente en contextos donde se utiliza IA para la toma de decisiones automatizadas. Entre los cambios más importantes se encuentra la implementación de medidas que exigen a las empresas obtener el consentimiento explícito de los individuos antes de procesar sus datos personales con fines automatizados. Además, se reforzó la regulación sobre la transferencia de datos a terceros países, alineándola con las prácticas globales de protección de datos, como las que establece el RGPD.

Comparando la legislación japonesa con el RGPD, hay áreas donde se podrían hacer mejoras adicionales. Por ejemplo, el RGPD tiene disposiciones más estrictas respecto a la transparencia y la toma

⁵ <https://law.asia/data-dojo/>

de decisiones automatizadas, exigiendo que los individuos tengan derecho a no ser sujetos a decisiones basadas únicamente en el procesamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos o les afecten significativamente. Aunque las enmiendas de la *APPI* abordan algunas de estas preocupaciones, el RGPD establece de manera más explícita los derechos de los ciudadanos en cuanto a la automatización, proporcionando también un mecanismo para la evaluación de impacto en la privacidad cuando se implementan tecnologías que afectan de forma significativa la privacidad de los individuos.

Desde mi punto de vista, una mejora potencial en la normativa japonesa podría ser la implementación de un sistema más robusto de evaluación de impacto de la IA en la privacidad. Aunque Japón ha dado pasos importantes, una evaluación anticipada de los riesgos de privacidad y las implicaciones éticas de los algoritmos utilizados en la toma de decisiones podría ayudar a mitigar los posibles impactos negativos de la automatización. Además, fortalecer las normativas sobre derechos de los usuarios frente a decisiones automatizadas, como el derecho a la explicación de decisiones algorítmicas, podría ser un paso hacia un enfoque más transparente y equitativo.

En resumen, la legislación de protección de datos en Japón ha dado pasos significativos para enfrentar los desafíos que presenta el uso de la IA y los algoritmos, pero aún existen áreas donde se podría tomar como modelo el RGPD para garantizar una mayor protección de los derechos de privacidad y promover la confianza en el manejo de datos personales.

Caso 3. Sanción a *Vodafone* por incumplimiento en la protección de datos (2021). [22]

Vodafone España se enfrentó a una sanción en marzo de 2021 de más de 8 millones de euros por la AEPD debido a múltiples infracciones relacionadas con el incumplimiento de la Ley de protección de datos y el RGPD. Esta sanción se derivó de 191 quejas recibidas entre abril de 2018 y septiembre de 2019, donde los usuarios denunciaron que la empresa seguía enviando comunicaciones publicitarias a pesar de haber ejercido su derecho de oposición al tratamiento de sus datos personales. Durante una inspección, la AEPD constató que *Vodafone* no estaba realizando un monitoreo continuo de los tratamientos de datos que llevaba a cabo, lo que llevó a la conclusión de que existían fallos significativos en sus protocolos de protección de datos.

La AEPD determinó que *Vodafone* no había implementado las medidas organizativas y técnicas necesarias para evitar que se produjeran estas infracciones. En particular, se señaló que existían deficiencias en la gestión de las solicitudes de oposición de los usuarios, lo que resultó en que muchos clientes seguían recibiendo publicidad no deseada. La situación fue agravada por la evidencia de que *Vodafone* había transferido datos personales a terceros en el extranjero, específicamente a Perú, sin cumplir con las condiciones requeridas para la transferencia internacional de datos según el RGPD.

Esta sanción subraya la importancia de que las empresas, especialmente las que manejan grandes volúmenes de datos personales, implementen sistemas robustos de cumplimiento normativo y protección de datos. *Vodafone* reconoció la necesidad de mejorar sus procedimientos internos y ha tomado medidas alineadas con el RGPD para rectificar las deficiencias identificadas por la AEPD.

Entre estas medidas adoptó sistemas avanzados de cifrado para proteger la información personal tanto en tránsito como almacenados, asegurando su confidencialidad frente a accesos no autorizados. Asimismo, estableció controles de acceso más estrictos basados en el principio de mínimo privilegio, limitando el acceso a los datos personales únicamente a empleados y sistemas que lo requirieran estrictamente.

También implementó auditorías automatizadas y herramientas de monitoreo continuo para detectar posibles anomalías en el tratamiento de datos, acompañadas de procedimientos de registro detallado para garantizar la trazabilidad de todas las operaciones. Estas acciones se complementaron con evaluaciones periódicas de impacto para identificar y mitigar riesgos en el uso de datos personales, así como con programas de formación para su personal, enfocados en el cumplimiento normativo y la gestión ética de los datos.

Caso 4. Incidente de Seguridad en “T-Mobile” (2021)⁶.

En agosto de 2021, *T-Mobile* en Estados Unidos fue víctima de un ciberataque que resultó en el robo de datos personales de más de 50 millones de personas, incluidos clientes actuales, antiguos y potenciales. Los datos robados incluían nombres, fechas de nacimiento, números de seguro social y licencias de conducir, lo que lo convierte en uno de los incidentes de seguridad más graves en el sector de telecomunicaciones en los últimos años.

Este ataque fue realizado mediante una vulnerabilidad en los servidores de “*T-Mobile*”, lo que permitió a los atacantes acceder a información altamente sensible. A pesar de que la empresa había implementado múltiples capas de seguridad, los “*hackers*” lograron eludirlas, lo que puso en evidencia las limitaciones de las defensas de seguridad tradicionales frente a ataques cada vez más sofisticados.

Tras el incidente, “*T-Mobile*” se comprometió a realizar una revisión completa de sus políticas y sistemas de seguridad, incluyendo la adopción de tecnologías más avanzadas como la IA para detectar y prevenir amenazas en tiempo real. También se centraron en mejorar su transparencia con los clientes, informándoles detalladamente sobre el incidente y las medidas para proteger sus datos en el futuro.

Este caso resalta la importancia de mantener una vigilancia continua y actualizar constantemente las medidas de seguridad para hacer frente a las amenazas emergentes. Además, subraya la necesidad de que las empresas de telecomunicaciones no solo cumplan con las normativas de protección de datos, sino que también vayan más allá, adoptando prácticas innovadoras y proactivas en ciberseguridad que incluyen tecnologías avanzadas como la IA y el *ML* para la detección y prevención de amenazas en tiempo real.

Estas tecnologías permiten identificar patrones anómalos en el tráfico de datos o en el comportamiento de los usuarios, lo que ayuda a predecir y neutralizar ataques antes de que ocurran. Además, se están implementando sistemas de autenticación más robustos, como la biometría y la autenticación multifactor, que añaden capas adicionales de seguridad para el acceso a los sistemas.

La autenticación multifactor combina diferentes tipos de factores para verificar la identidad de un usuario, generalmente están agrupados en tres categorías principales, algo que sabes, como contraseñas o *PIN*, algo que tienes, como tarjetas inteligentes o dispositivos móviles que generan códigos únicos y algo que eres, como datos biométricos, huellas dactilares, reconocimiento facial o de iris. También se incluyen factores emergentes, como la ubicación geográfica que utiliza la ubicación física del usuario como un criterio para verificar su identidad. Se basa en la detección de la dirección IP, el GPS del dispositivo o torres de telefonía móvil para determinar si el acceso se está realizando desde un lugar autorizado.

Otra práctica clave es el uso de técnicas de segmentación de red, que aíslan las distintas áreas de una infraestructura para limitar la propagación de un ataque en caso de que ocurra. Asimismo, las empresas

⁶ <https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers>

están adoptando enfoques de seguridad “*Zero Trust*”, donde cada acceso es evaluado y autenticado sin presuponer confianza en ningún usuario o dispositivo, incluso dentro de la red interna.

Estas medidas se complementan con el uso de análisis de comportamiento avanzado y simulaciones de ciberataques como pruebas de penetración o ejercicios de “*Red Team*” para evaluar constantemente la resiliencia de los sistemas frente a amenazas emergentes. Este enfoque proactivo no solo permite a las empresas cumplir con las normativas, sino que también fortalece su capacidad de respuesta ante un panorama de amenazas en constante evolución.

2.3.3 Retos y amenazas actuales.

El sector de las telecomunicaciones se enfrenta a numerosos retos y amenazas en lo que respecta a la protección de datos. A continuación, se detallan algunos de los más significativos:

a) Ciberamenazas y brechas de seguridad.

Uno de los mayores desafíos para las empresas de telecomunicaciones es la creciente sofisticación de las ciberamenazas. Dado que este sector maneja grandes volúmenes de datos sensibles, cualquier brecha de seguridad puede tener consecuencias devastadoras, tanto para la empresa afectada como para sus clientes. Los atacantes utilizan técnicas avanzadas como el “*phishing*” dirigido, el “*ransomware*” y los ataques de “*zero-day*” para comprometer los sistemas de telecomunicaciones.

El “*phishing*” es una técnica de ciberataque en la que los atacantes intentan engañar a los usuarios para que revelen información confidencial, como contraseñas, números de tarjetas de crédito o datos personales. Esto se logra a menudo mediante correos electrónicos o mensajes falsos que parecen provenir de fuentes legítimas, como bancos o servicios en línea, solicitando que el usuario haga clic en un enlace que lo redirige a un sitio *web* fraudulento. Los métodos de “*phishing*” han evolucionado con el tiempo e incluyen variaciones como el “*spear phishing*”, que se dirige a individuos específicos, y el “*whaling*”, que se enfoca en ejecutivos de alto nivel.

El “*ransomware*” es un tipo de “*malware*” que encripta los archivos de un sistema o dispositivo y exige un rescate para restaurar el acceso a los datos. Este tipo de ataque puede afectar a individuos y organizaciones, bloqueando el acceso a información crítica hasta que se pague una suma de dinero, generalmente en criptomonedas, para recibir la clave de descifrado. Los ataques de “*ransomware*” pueden causar pérdidas financieras significativas y daño a la reputación de las empresas. En muchos casos, los atacantes utilizan técnicas de ingeniería social para propagar el “*ransomware*”, como correos electrónicos de “*phishing*” que incitan al usuario a abrir un archivo adjunto infectado.

Un ataque “*zero-day*” se refiere a una vulnerabilidad de software que es desconocida para el fabricante y, por lo tanto, no tiene un parche o solución disponible en el momento en que se explota. El término “*zero-day*” proviene del hecho de que los desarrolladores tienen cero días para arreglar la vulnerabilidad antes de que sea aprovechada por atacantes maliciosos. Estas vulnerabilidades son especialmente peligrosas, ya que pueden ser utilizadas para llevar a cabo ataques antes de que se implemente una solución, lo que permite a los “*hackers*” acceder a sistemas, robar información o instalar *malware* sin ser detectados.

La gestión de la seguridad en un entorno de red tan complejo requiere un enfoque integral que combine medidas preventivas, como la segmentación de la red y la autenticación multifactor, con tecnologías de detección y respuesta, como los sistemas de detección y respuesta ante amenazas conocidos como “*Endpoint Detection and Response*”.

Los ciberataques a empresas y ciudadanos en España han mostrado un crecimiento constante [23]. Según el Instituto Nacional de Ciberseguridad (INCIBE), en 2023 se gestionaron 83.517 incidentes de

ciberseguridad, lo que representa un aumento del 24 % respecto al año anterior. De estos, más de 22.000 afectaron a empresas privadas, incluidas PYMES y autónomos. Los incidentes más comunes fueron los fraudes en línea, que representaron 28.258 casos, seguidos de ataques de “*phishing*” (14.261 incidentes) y “*malware*”, que afectaron a más de 26.200 sistemas. También se detectaron 621 casos de “*ransomware*”, en los que ciberdelincuentes bloquearon sistemas para pedir rescates económicos

INCIBE también informó que más de 4 millones de dispositivos en España presentaron vulnerabilidades críticas, lo que aumenta el riesgo de ataques. Además, destaca que sectores clave como energía, transporte y finanzas son especialmente vulnerables debido a su valor estratégico.

Esta tendencia subraya la importancia de invertir en medidas preventivas, como la actualización de sistemas, la capacitación en ciberseguridad y la implementación de políticas de protección adecuadas para las empresas de todos los tamaños.

b) Análisis del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, Reglamento de Inteligencia Artificial (RIA) [24] en relación con el RGPD.

El cumplimiento de las normativas de protección de datos es otro desafío importante. Las empresas de telecomunicaciones que operan a nivel internacional deben cumplir con una variedad de Leyes y regulaciones, que a menudo difieren de un país a otro. Por ejemplo, mientras que el RGPD en Europa es conocido por su rigor, otras regiones pueden tener requisitos menos estrictos o más fragmentados.

Este mosaico regulatorio crea complejidades adicionales para las empresas, que deben adaptar sus prácticas de protección de datos a cada jurisdicción sin comprometer la eficiencia operativa. La falta de armonización entre las normativas también puede aumentar el riesgo de incumplimiento involuntario, lo que podría resultar en sanciones severas y daños a la reputación.

Este tipo de sanciones pueden alcanzar hasta 20 millones de euros o el 4 % de la facturación anual global de la empresa, lo que sea mayor. Esta sanción tiene como objetivo garantizar el cumplimiento estricto de las normativas y subraya la gravedad de las infracciones relacionadas con la privacidad y la seguridad de los datos. Además de las sanciones financieras, las empresas también se pueden enfrentar a prohibiciones temporales o definitivas sobre el procesamiento de datos, lo que podría paralizar sus operaciones.

Para abordar este desafío, algunas empresas están invirtiendo en plataformas de cumplimiento normativo que les ayudan a gestionar las diferencias entre las regulaciones y a automatizar la aplicación de políticas de protección de datos.

Estas plataformas integran funciones para automatizar procesos relacionados con la recopilación, almacenamiento, y manejo de datos personales, garantizando la transparencia y el cumplimiento.

Algunas de las plataformas más utilizadas como “*IBM Data Privacy Passports*” y “*OneTrust Data Discovery*” utilizan IA y ML para identificar y clasificar datos sensibles, asegurando que su uso cumpla con el RGPD. Otras herramientas como “*Privitar*” y “*BigID*” ofrecen también soluciones avanzadas de anonimización y seudonimización, permitiendo el procesamiento seguro de información sin comprometer la privacidad. Por otro lado, tecnologías como “*Azure Purview*” y “*Google Cloud Data Loss Prevention (DLP)*” detectan vulnerabilidades, comprueban continuamente el flujo de datos y alertando sobre posibles incumplimientos. Estas tecnologías no solo refuerzan la seguridad y privacidad, sino que también promueven la confianza en la adopción de soluciones de IA en sectores sensibles al garantizar la transparencia y el cumplimiento normativo.

El RIA de 2024 garantiza el uso ético y seguro de la IA en la Unión Europea. La normativa clasifica los sistemas de IA niveles de riesgo según lo señalado en la tabla 2-2 y prohíbe aquellos considerados de riesgo inaceptable, como la vigilancia masiva indiscriminada, imponiendo obligaciones estrictas para sistemas de riesgo alto. Aunque se alinea con los principios fundamentales RGPD, surgen tensiones entre ambos marcos. Mientras el RGPD protege la privacidad y los derechos individuales sobre los datos personales, el RIA fomenta el desarrollo de sistemas que a menudo requieren grandes volúmenes de datos para funcionar eficazmente, lo que podría aumentar el riesgo de vulneración de la privacidad.

Nivel de Riesgo	Descripción	Ejemplos
Riesgo mínimo o nulo	Aplicaciones de IA que no presentan riesgos significativos para los derechos fundamentales de las personas.	IA en videojuegos, chatbots informativos, recomendadores de música o productos sin impacto significativo.
Riesgo limitado	Aplicaciones de IA que tienen un riesgo bajo, pero que requieren ciertas medidas de transparencia y supervisión.	IA en servicios de atención al cliente, herramientas de filtrado de contenido, sistemas de marketing.
Riesgo alto	Aplicaciones de IA que pueden afectar gravemente los derechos y libertades de las personas, pero que están permitidas bajo condiciones estrictas.	Reconocimiento facial en espacios públicos, IA en decisiones automatizadas en crédito o contratación, vehículos autónomos.
Riesgo inaceptable	Aplicaciones de IA que representan un peligro claro para los derechos humanos y la seguridad, y se prohíben.	Sistemas de puntuación social, IA para manipulación masiva o vigilancia masiva indiscriminada.

Tabla 2-2. Niveles de riesgo según el RIA de la UE.

La transparencia en los sistemas de IA de alto riesgo es un punto crítico. El RIA exige que estos sistemas tengan capacidad de *ML* para ser entendido de manera clara y comprensible por los humanos y cuenten con documentación adecuada. Sin embargo, la complejidad de muchos algoritmos dificulta el desglose para proporcionar una información clara y comprensible, como exige el RGPD en relación con el tratamiento de datos personales. Por otro lado, el uso masivo de datos para entrenar modelos de IA puede entrar en conflicto con el principio de minimización del RGPD, que establece que solo deben recopilarse y procesarse los datos estrictamente necesarios para cumplir con un propósito específico, evitando excesos o usos innecesarios.

También se cuestiona la proporcionalidad del uso de sistemas de IA en áreas como la vigilancia y la seguridad, donde los fines legítimos podrían justificar prácticas que rozan la línea de la privacidad intrusiva. Por ejemplo, tecnologías como el reconocimiento facial, reguladas estrictamente por el RGPD, son identificadas en el RIA como riesgo alto, pero no prohibidas completamente. Esto plantea dudas sobre si la protección de datos personales está suficientemente garantizada frente a los intereses comerciales o de seguridad pública.

El RIA de la Unión Europea establece requisitos específicos para los sistemas de IA de riesgo alto, como transparencia, evaluaciones de impacto y documentación detallada. Sin embargo, su interacción

con el RGPD plantea desafíos importantes, especialmente en relación con principios como la minimización de datos, la finalidad y la transparencia.

Por ejemplo, según el artículo 5 del RGPD se exige que solo se recopilen y procesen los datos estrictamente necesarios para un propósito específico, mientras que muchos sistemas de IA requieren grandes volúmenes de datos para su aprendizaje, lo que puede violar este principio. La IA también se enfrenta a dificultades para cumplir con el principio de finalidad, dado que los modelos suelen usar datos recolectados inicialmente para otros fines, y esto puede contradecir la normativa del RGPD sobre procesamiento de datos con propósitos claramente definidos desde el inicio.

Otro aspecto clave es la transparencia. Aunque el RGPD exige que las personas sean informadas de manera clara y comprensible sobre cómo se procesan sus datos, los algoritmos complejos de IA suelen ser difíciles de explicar, lo que puede ir en contra de lo desarrollado en el artículo 12 del RGPD.

Los algoritmos de IA pueden impedir el cumplimiento de los requisitos de capacidad que un sistema de *ML* debe cumplir para ser entendido y explicado de manera clara por los humanos. Esta limitación puede restringir la capacidad de los usuarios para comprender cómo se toman las decisiones automatizadas que afectan directamente a sus vidas. En un mundo donde las decisiones basadas en IA tienen un impacto significativo, la falta de transparencia puede generar desconfianza y dudas sobre la justicia y legalidad de estos sistemas.

Para afrontar esta situación, la integración de normativas como el RIA y el RGPD resulta fundamental. La adaptación de ambas regulaciones podría requerir la implementación de soluciones prácticas que aseguren que el uso de IA no comprometa derechos fundamentales ni cree riesgos innecesarios para la privacidad. Una de las medidas clave sería la realización de evaluaciones de impacto conjunto. Las empresas deben llevar a cabo evaluaciones para identificar y mitigar riesgos relacionados con la privacidad y el uso de la IA. Este proceso debe incluir la valoración de la proporcionalidad en el uso de datos y la minimización de los mismos antes de la implementación de sistemas automatizados, asegurando que estos sistemas no excedan lo necesario para alcanzar sus objetivos.

Además, se requiere la implementación de mecanismos de gobernanza de datos. Estos sistemas deben ser capaces de gestionar los datos personales de forma segura, incorporando controles estrictos de acceso, medidas de anonimización o seudonimización, y herramientas para la monitorización constante del cumplimiento normativo. Esto no solo protege los datos, sino que también permite que las organizaciones mantengan una gestión transparente y responsable de la información que manejan.

Otro elemento fundamental de la IA es la necesidad de que un sistema de *ML* sea comprensible y pueda ser explicado de forma clara a los humanos. Las empresas deben trabajar en el desarrollo de modelos más transparentes y explicables, lo que implica el uso de tecnologías de IA interpretables y metodologías que permitan auditar los algoritmos. Esto garantizará que se pueda verificar su alineación con principios fundamentales como la igualdad y la no discriminación. La transparencia en los modelos no solo es esencial para el cumplimiento normativo, sino también para la confianza de los usuarios en los sistemas automatizados.

A lo largo de este proceso, es importante considerar la compatibilidad entre normativas. Las guías emitidas por la AEPD y otras autoridades europeas ofrecen directrices claras para armonizar el cumplimiento del RGPD con el desarrollo ético y legal de sistemas de IA. Estas guías se enfocan en proteger los derechos fundamentales de los usuarios, asegurando que los sistemas de IA operen dentro de un marco legal que respete la privacidad y garantice una base legal sólida para el tratamiento de los datos personales.

En este contexto, el análisis del RIA en relación con el RGPD subraya la necesidad de adaptar continuamente los sistemas de IA al marco legal europeo. No solo es necesario cumplir con el RIA y el RGPD, sino también garantizar la confianza y la seguridad en el manejo de los datos personales. Los avances tecnológicos deben ir acompañados de una constante revisión de las prácticas y normativas que regulan la IA, para que esta no comprometa los derechos y la privacidad de los ciudadanos.

En conclusión, aunque tanto el RIA como el RGPD comparten objetivos comunes en cuanto a ética y protección de derechos fundamentales, es fundamental encontrar un equilibrio más claro entre ambas normativas. Esto permitirá evitar contradicciones y garantizar que el desarrollo de la IA no perjudique los derechos de privacidad de los ciudadanos, protegiendo al mismo tiempo la innovación tecnológica en el ámbito europeo.

c) Protección de datos en redes 5G.

La implementación de redes 5G representa tanto una oportunidad como un desafío para la protección de datos. Si bien las redes 5G ofrecen velocidades de conexión más rápidas y menor latencia, también introducen nuevas preocupaciones de seguridad. La arquitectura descentralizada de 5G, con más puntos de acceso y dispositivos conectados, amplía la superficie de ataque y dificulta la protección integral de los datos. Además, las redes 5G facilitan la proliferación de dispositivos *IoT*, que a menudo carecen de las capacidades de seguridad necesarias para proteger adecuadamente los datos que manejan.

La protección de los datos en las redes 5G consiste en implementar medidas avanzadas de seguridad que aborden los desafíos específicos de esta tecnología, como la arquitectura descentralizada, la proliferación de dispositivos *IoT* y la expansión de la superficie de ataque. Esto implica adoptar un enfoque de seguridad por diseño, donde la privacidad y la protección de datos se integran desde la concepción y desarrollo de las redes.

Entre las estrategias clave se encuentran la segmentación de la red mediante “*Network Slicing*”, que permite aislar diferentes flujos de tráfico y reducir el riesgo de accesos no autorizados, y la virtualización de funciones de red, “*Network Functions Virtualization*” (*NFV*) como firewalls, routers o balanceadores de carga, separándolos del hardware físico, cuyo objetivo principal es desplegar y gestionar funciones de red de forma flexible y eficiente, optimizando recursos mediante virtualización en servidores estándar y facilitando la implementación de mecanismos de seguridad adaptables y escalables.

Asimismo, es esencial fortalecer la protección de dispositivos *IoT* mediante el cifrado de datos, la autenticación robusta y la actualización constante de sus protocolos de seguridad. De esta manera, las redes 5G buscan garantizar la confidencialidad, integridad y disponibilidad de la información, a pesar de los retos que supone su infraestructura avanzada.

En un mundo donde los consumidores son cada vez más conscientes de sus derechos de privacidad, las empresas de telecomunicaciones deben esforzarse por mantener la confianza de sus clientes. Esto implica no solo cumplir con las normativas de protección de datos, sino también ser transparentes sobre cómo se manejan los datos personales.

Los clientes esperan que las empresas expliquen claramente qué datos recopilan, cómo se utilizan y con quién se comparten. La falta de transparencia puede llevar a la desconfianza y al rechazo de los servicios, lo que a su vez puede afectar negativamente a la reputación y al éxito comercial de la empresa.

Para abordar este desafío, algunas empresas están adoptando enfoques innovadores como el desarrollo de paneles de privacidad donde los clientes pueden gestionar sus preferencias de datos y revisar cómo se están utilizando sus datos. Además, las empresas deben estar preparadas para responder

a las solicitudes de los clientes en relación con sus derechos de acceso, corrección y eliminación de datos de manera eficiente y oportuna.

d) Evolución tecnológica rápida.

El ritmo acelerado de la evolución tecnológica en el sector de telecomunicaciones representa otro reto significativo para la protección de datos. Nuevas tecnologías como la IA, el *ML* y el “*Big Data*” están transformando la forma en que se manejan y protegen los datos, pero también introducen nuevos riesgos.

Para mantenerse al día con estos avances tecnológicos, las empresas de telecomunicaciones deben invertir en investigación y desarrollo, así como en la formación continua de su personal. También deben colaborar estrechamente con los proveedores de tecnología para asegurar que las soluciones adoptadas cumplen con los más altos estándares de protección de datos.

En resumen, la situación actual de la protección de datos en el sector de las telecomunicaciones está marcada por un entorno regulatorio en constante evolución, la rápida adopción de nuevas tecnologías y el incremento de las ciberamenazas. Aunque las empresas de telecomunicaciones han avanzado significativamente en la implementación de medidas de protección de datos, siguen enfrentando desafíos complejos que requieren un enfoque proactivo y estratégico para garantizar la seguridad y la privacidad de los datos en un panorama cada vez más conectado y globalizado.

3 IMPLEMENTACIÓN DE LA PROTECCIÓN DE DATOS EN TELECOMUNICACIONES

La protección de datos en el ámbito de las telecomunicaciones es una cuestión crítica, dado el volumen y la sensibilidad de la información transmitida a través de redes y sistemas de comunicación. La implementación de medidas efectivas de protección de datos en este contexto no solo responde a exigencias legales, sino también a la necesidad de preservar la confianza del usuario y asegurar la integridad de los datos manejados. Este apartado aborda las principales estrategias de implementación de la protección de datos, destacando las medidas técnicas y organizativas, la evaluación de impacto de privacidad y la gestión de incidentes de seguridad.

3.1 Medidas técnicas y organizativas.

La implementación efectiva de la protección de datos en telecomunicaciones requiere una combinación equilibrada de medidas técnicas y organizativas. Estas medidas tienen como objetivo garantizar que los datos personales sean tratados de manera segura y en cumplimiento con el RGPD y otras normativas relevantes.

3.1.1 Medidas técnicas.

Las medidas técnicas incluyen todas aquellas herramientas y procedimientos tecnológicos diseñados para proteger los datos personales durante su transmisión, almacenamiento y procesamiento. Algunas de las medidas técnicas más relevantes en el ámbito de las telecomunicaciones son:

- a) **Cifrado.** El cifrado es una de las medidas técnicas más esenciales en la protección de datos en telecomunicaciones. Mediante el uso de algoritmos criptográficos, los datos son transformados en un formato ilegible para cualquiera que no tenga la clave de descifrado. El cifrado asegura que incluso si los datos son interceptados durante la transmisión, no podrán ser comprendidos ni utilizados indebidamente. En telecomunicaciones, es común el uso de cifrado de extremo a extremo para proteger la confidencialidad de los mensajes y llamadas.
- b) **Control de acceso.** La implementación de sistemas de control de acceso es fundamental para limitar quién puede acceder a los datos personales. Esto incluye la autenticación de usuarios, la gestión de permisos y la monitorización de accesos. En telecomunicaciones, es crucial que solo el personal autorizado pueda acceder a datos sensibles, y que existan registros detallados de todos los accesos realizados.
- c) **Anonimización.** Esta técnica reduce el riesgo de identificación de individuos a partir de los datos. La anonimización transforma los datos de tal manera que la persona ya no es identificable. Cuando los datos están anonimizados no es aplicable el RGPD.
- d) **Seudonimización.** La seudonimización reemplaza los identificadores directos con seudónimos, manteniendo una referencia que permite la identificación bajo condiciones controladas. En telecomunicaciones, estas técnicas son especialmente útiles para el análisis de grandes volúmenes de datos sin comprometer la privacidad de los usuarios.
- e) **Seguridad de las redes:** En el ámbito de las telecomunicaciones, asegurar la integridad y confidencialidad de las redes es crucial. Esto implica el uso de “firewalls”, “intrusion detection system” (IDS), y protocolos de seguridad para redes inalámbricas, como “Wi-Fi Protected Access 3” (WPA3), que protejan las comunicaciones contra accesos no autorizados y ciberataques.

3.1.2 Medidas organizativas.

Además de las medidas técnicas, es fundamental implementar medidas organizativas que aseguren un tratamiento adecuado de los datos personales dentro de la organización. Estas incluyen:

- a) **Políticas de protección de datos.** Establecer políticas claras y accesibles sobre cómo deben ser tratados los datos personales en la organización. Estas políticas deben incluir procedimientos para la recogida, almacenamiento, uso, y eliminación de datos, y deben ser conocidas y comprendidas por todos los empleados.
- b) **Capacitación y concienciación.** Los empleados deben recibir formación continua sobre las mejores prácticas en protección de datos y seguridad de la información. En telecomunicaciones, donde se manejan grandes volúmenes de datos sensibles, es crucial que el personal esté capacitado para identificar y responder a posibles amenazas a la seguridad de los datos.
- c) **Gestión de riesgos.** Implementar un enfoque proactivo de gestión de riesgos que incluya la identificación, evaluación, y mitigación de posibles amenazas a la privacidad y seguridad de los datos. Esto puede implicar la realización de auditorías regulares, la revisión de procedimientos y la implementación de mejoras continuas en las prácticas de protección de datos.

3.2 Evaluación de impacto relativa a la protección de datos (EIPD) [25].

El artículo 35 del RGPD establece la obligación de realizar una evaluación de impacto relativa a la protección de datos (EIPD) cuando un tratamiento de datos pueda implicar un riesgo alto para los derechos y libertades de las personas. Esto suele ocurrir cuando el tratamiento de datos presenta características que lo hacen potencialmente invasivo, sin la adecuada mitigación de riesgos.

Este tipo de riesgos suelen estar relacionados con el tratamiento de grandes volúmenes de datos sensibles o la utilización de nuevas tecnologías. Por ejemplo, se considera que existe un riesgo alto cuando se realizan tratamientos de datos personales sensibles a gran escala relativos a la salud, origen racial o étnico, opiniones políticas, creencias religiosas, vida sexual o datos biométricos que están sujetos a una protección reforzada sin medidas adecuadas de seguridad.

En este caso, la AEPD recomienda llevar a cabo EIPD para identificar y mitigar los riesgos antes de que se lleve a cabo el tratamiento, con el fin de proteger los derechos de los afectados. Si se identifican riesgos no mitigables, el responsable del tratamiento debe consultar a la AEPD antes de proceder con el tratamiento.

La evaluación de impacto de privacidad es un proceso que permite identificar y mitigar los riesgos asociados al tratamiento de datos personales, especialmente cuando se utilizan nuevas tecnologías o se implementan procesos que pueden afectar significativamente la privacidad de los individuos. En el sector de las telecomunicaciones, la realización de esta evaluación es particularmente relevante debido a la gran cantidad de datos sensibles que se manejan y a la rapidez con la que evoluciona la tecnología.

El principal objetivo de una evaluación de impacto de privacidad es identificar y controlar los riesgos para los derechos y las libertades de las personas, asociados a un tratamiento de datos. Este proceso permite a las organizaciones:

- a) **Identificar riesgos potenciales.** Se pueden identificar posibles riesgos para la privacidad antes de que se materialicen, lo que permite a la organización tomar medidas preventivas.
- b) **Cumplir con la normativa.** Es un requisito legal en algunos casos bajo el RGPD, especialmente cuando el tratamiento de datos implica un riesgo alto para los derechos y libertades de las personas. Esto incluye el uso de tecnologías nuevas o la realización de perfiles de individuos a gran escala.
- c) **Fomentar la confianza.** Al demostrar un compromiso con la protección de datos mediante la realización de evaluaciones de impacto, las organizaciones pueden aumentar la confianza de los usuarios y otras partes interesadas, lo que es esencial en un sector tan sensible como el de las telecomunicaciones.

La realización de una evaluación de impacto de privacidad implica varias etapas clave:

- 1) **Descripción del tratamiento.** Proporcionar una descripción clara y detallada del tratamiento de datos previsto, incluyendo la finalidad del tratamiento, los tipos de datos que se recopilarán, y las tecnologías que se utilizarán.
- 2) **Evaluación de la necesidad y proporcionalidad.** Analizar si el tratamiento es necesario y si se realiza de manera proporcional en relación con los fines que se persiguen. Esto incluye considerar si los objetivos podrían lograrse mediante otros medios que impliquen menos riesgos para la privacidad.
- 3) **Identificación y evaluación de riesgos.** En esta etapa, se identifican los posibles riesgos para la privacidad de los individuos y se evalúa la probabilidad y el impacto de estos riesgos.
- 4) **Medidas para mitigar los riesgos.** Una vez identificados los riesgos, se deben proponer medidas específicas para mitigarlos. Esto puede incluir cambios en el diseño del sistema, la implementación de medidas de seguridad adicionales, o la modificación de políticas organizativas.
- 5) **Consulta con las partes interesadas.** En algunos casos, puede ser necesario consultar con las partes interesadas, como los representantes de los interesados o las autoridades de protección de datos, para obtener su opinión sobre los riesgos identificados y las medidas propuestas.
- 6) **Revisión y actualización.** La evaluación de impacto de privacidad no es un proceso estático, sino que debe ser revisada y actualizada regularmente para reflejar cualquier cambio en el tratamiento de datos o en el entorno normativo.

En este contexto, la AEPD desempeña un papel crucial al proporcionar herramientas y directrices para la correcta implementación de estas evaluaciones. Una de las herramientas más destacadas de la AEPD es Evalúa-Riesgo V2, que permite a las organizaciones realizar una evaluación de riesgos sobre los tratamientos de datos personales y determinar si es necesario llevar a cabo una EIPD. Evalúa-Riesgo V2 facilita la identificación de riesgos en el tratamiento y ayuda a implementar medidas correctivas, alineándose con los principios de privacidad desde el diseño y por defecto, tal como establece el RGPD.

Sin embargo, a pesar de los avances, existen áreas en las que la regulación y las herramientas pueden mejorarse. Una de las principales problemáticas radica en la falta de claridad en algunos aspectos del proceso de EIPD, especialmente cuando se trata de tecnologías emergentes o de tratamientos que no encajan claramente en los ejemplos que ofrece el RGPD. Además, la regulación actual puede resultar poco flexible para adaptarse rápidamente a la velocidad con la que surgen nuevas tecnologías, lo que puede generar incertidumbre en las empresas y retrasos en la implementación de nuevos proyectos.

Para mejorar la regulación, sería recomendable una mayor actualización y flexibilización de las directrices de la AEPD, especialmente en lo que respecta a la interpretación de lo que constituye un riesgo alto. Además, se podría fomentar la creación de un marco normativo específico para sectores emergentes, como la IA o el análisis de “*Big Data*”, que incorpore directamente las peculiaridades de estos tratamientos.

Como solución, la AEPD podría fortalecer la educación y formación en torno a la EIPD, asegurando que las empresas comprendan no solo la obligación legal, sino también la importancia de implementar buenas prácticas de privacidad y seguridad de manera proactiva.

Por último, otro factor clave a tener en cuenta para realizar evaluaciones de impacto son las iniciativas legislativas, especialmente cuando se trata de tecnologías emergentes como las implementadas en las “*Smart Cities*.” Antes de implementar cualquier tipo de tratamiento o regulación, como por ejemplo en el ámbito de las telecomunicaciones, las Administraciones Públicas deben realizar un análisis exhaustivo de los riesgos asociados, evaluando tanto las consecuencias sociales, económicas y ambientales como los impactos sobre la privacidad y la seguridad de los ciudadanos.

Este proceso de evaluación se debe integrar en la elaboración de la Ley desde sus fases iniciales, asegurando que las regulaciones propuestas no solo fomenten la innovación tecnológica, sino que también garanticen la protección de los derechos fundamentales de las personas. La evaluación de impacto no solo identifica posibles riesgos, sino que también propone medidas mitigadoras, garantizando que las políticas públicas sean responsables, transparentes y alineadas con los intereses generales de la comunidad.

3.3 Gestión de Incidentes de Seguridad.

La gestión de incidentes de seguridad es un componente fundamental en la implementación de la protección de datos en telecomunicaciones. Un incidente de seguridad puede tener consecuencias graves, incluyendo la pérdida de datos, el acceso no autorizado a información sensible, y daños a la reputación de la organización. Por ello, es imprescindible contar con un plan robusto para la gestión de estos incidentes, que permita una respuesta rápida y efectiva.

3.3.1 Definición y tipología de incidentes.

Un incidente de seguridad se refiere a cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los datos personales. En el contexto de las telecomunicaciones, esto puede incluir:

- a) **Ciberataques.** Como “*Distributed Denial-of-Service*” (DDoS)⁷, inyección de “*malware*”, o “*hacking*”, que pueden afectar la disponibilidad y seguridad de las redes de telecomunicaciones.

⁷ DDoS: ataque de denegación de servicio distribuido, es un delito en el que el atacante inunda un servidor con tráfico de internet para evitar que los usuarios accedan a servicios y sitios en línea conectados.

- b) **Pérdida o robo de dispositivos.** Los dispositivos que contienen datos personales, como teléfonos móviles y ordenadores portátiles, pueden ser robados o perdidos, lo que compromete la seguridad de la información contenida en ellos.
- c) **Errores humanos:** Estos incluyen el envío de datos personales a destinatarios incorrectos, la eliminación accidental de datos, o la configuración incorrecta de sistemas que dejan vulnerables a los datos.

3.3.2 Proceso de gestión de incidentes.

La gestión de incidentes de seguridad debe seguir un proceso estructurado que incluye según se señala en la figura 3-1 del Esquema Nacional de Seguridad (ENS) de abril de 2020 las siguientes etapas dentro del ciclo de vida de respuesta a ciberincidentes:

- a) **Detección y notificación.** La detección rápida de un incidente es esencial para minimizar su impacto. Esto requiere la implementación de sistemas de monitorización que alerten a los responsables de la seguridad cuando ocurre un incidente. Una vez detectado, el incidente debe ser notificado inmediatamente a las partes pertinentes dentro de la organización.
- b) **Contención y mitigación.** Una vez identificado el incidente, el siguiente paso es contenerlo para evitar su propagación y mitigar sus efectos. Esto puede incluir aislar sistemas comprometidos, desactivar cuentas afectadas, o bloquear accesos no autorizados.
- c) **Investigación y análisis.** Es fundamental investigar el incidente para comprender cómo ocurrió, qué datos se vieron comprometidos, y quiénes fueron los responsables. Este análisis permite identificar vulnerabilidades en los sistemas y procesos que deben ser corregidas.
- d) **Recuperación.** Después de contener y mitigar el incidente, se deben tomar medidas para restaurar los sistemas y datos afectados. Esto incluye la recuperación de datos perdidos, la reparación de vulnerabilidades, y la implementación de medidas adicionales para prevenir futuros incidentes.
- e) **Revisión y mejora.** Una vez gestionado el incidente, es fundamental revisar el proceso de gestión para identificar lecciones aprendidas y mejorar las estrategias de protección de datos. Esta revisión debe conducir a la actualización de políticas, procedimientos y sistemas de seguridad. Tras el incidente, los responsables del organismo emitirán un informe del ciberincidente que detallará su causa originaria, su coste y las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.



Figura 3-1. Ciclo de vida de respuesta a Ciberincidentes. [26]

La implementación de la protección de datos en telecomunicaciones es un desafío complejo que requiere un enfoque integral. Las medidas técnicas y organizativas son esenciales para establecer una base sólida de seguridad, mientras que la evaluación de impacto de privacidad asegura que los riesgos sean identificados y mitigados antes de que se materialicen. Finalmente, la gestión de incidentes de seguridad es crucial para responder rápidamente a cualquier amenaza, minimizando su impacto y asegurando la continuidad de las operaciones. En conjunto, estas estrategias forman un marco robusto para la protección de datos en el dinámico y crítico sector de las telecomunicaciones.

3.4 Sanciones por incumplir el RGPD y la LOPDGDD.

El RGPD y la LOPDGDD contemplan sanciones similares por incumplimiento de la protección de datos, aunque con algunas diferencias. En España, la AEPD es la autoridad encargada de imponer las sanciones, y se clasifican por la gravedad de las infracciones según aparece indicado en la tabla 3-1[27].

Las sanciones por infracciones leves en la LOPDGDD pueden llegar hasta 40.000 euros, mientras que las graves oscilan entre 40.001 y 300.000 euros. Las infracciones muy graves pueden conllevar multas de hasta 20 millones de euros o el 4% del volumen de facturación anual de la empresa, según cuál sea mayor. Además, en algunos casos de infracciones leves, la Ley contempla el apercibimiento como medida inicial.

En el RGPD se incluyen infracciones de principios como la transparencia en el uso de los datos, la falta de medidas de seguridad adecuadas, o el tratamiento no autorizado de datos sensibles. Las más graves incluyen vulneraciones de los principios básicos del tratamiento de datos personales, las transferencias internacionales sin garantías adecuadas, y el incumplimiento de resoluciones impuestas por las autoridades de protección de datos.

El RGPD también clasifica las infracciones en graves y muy graves. Las infracciones graves pueden ser multadas con hasta 10 millones de euros o el 2% de la facturación anual, y las muy graves pueden alcanzar los 20 millones de euros o el 4% de la facturación, dependiendo de la mayor cantidad.

En la última memoria anual de 2023 de la AEPD se pueden consultar la información sobre la evolución de las multas impuestas en el año 2022 y 2023, quienes son los responsables de las multas superiores al millón de euros en resolución firme y ejecutiva y las seis áreas de actividad con mayor importe en sanciones durante el año 2023 [28].

Infracciones LOPD	Multas LOPD	Infracciones RGPD	Multas RGPD
Leves: Art.74	Hasta 40.000 €	Graves: Arts. 8, 11, 25 a 39, 41.4, 42 y 43	10 millones de euros o el 2% de la facturación anual
Graves: Art. 73	De 40.001 € a 300.000 €	Muy Graves: Arts. 5, 6, 7, 9, 12 a 22, 44 a 49, 58.1 y 58.2	20 millones de euros o el 4% de la facturación anual
Muy graves: Art. 72	De 300.001 € a 20 millones de euros (o el 4% de la facturación anual)		

Tabla 3-1. Resumen de infracciones y multas de la LOPD y el RGPD. [27]

4 ESTUDIO COMPARATIVO

El estudio comparativo es crucial para entender cómo diferentes países y organizaciones abordan la protección de datos en las comunicaciones. A través de la comparativa internacional y la identificación de mejores prácticas, podemos extraer lecciones que permitan mejorar las estrategias de protección de datos en el ámbito local y global.

4.1 Comparativa Internacional (UE, EEUU y Canadá).

En esta apartado, se analizan las normativas de protección de datos en las comunicaciones de diferentes países, identificando similitudes y diferencias, así como los desafíos específicos que enfrenta cada región. El análisis se centra en cómo estas normativas impactan en la privacidad, la seguridad de los datos y el cumplimiento normativo en las comunicaciones electrónicas y digitales.

4.1.1 Normativas en Europa.

El Reglamento general de protección de datos de la Unión Europea es una de las normativas más rigurosas y completas en materia de protección de datos a nivel mundial. El Reglamento ha establecido un estándar alto para la protección de la privacidad en las comunicaciones electrónicas y el tratamiento de datos personales. Algunas de las características clave incluyen:

- **Consentimiento informado.** Las organizaciones deben obtener un consentimiento claro y explícito antes de procesar los datos personales de los usuarios.
- **Derecho al olvido.** Los individuos tienen el derecho de solicitar la eliminación de sus datos cuando ya no sean necesarios.
- **Transferencias internacionales de datos.** El Reglamento impone restricciones estrictas a la transferencia de datos fuera de la Unión Europea, garantizando que los países receptores ofrezcan un nivel adecuado de protección.
- **Multas severas.** El incumplimiento de la normativa puede resultar en sanciones financieras significativas hasta del 4% de los ingresos anuales globales de una empresa.

El impacto del RGPD ha sido profundo, no solo en Europa, sino a nivel mundial, ya que muchas empresas internacionales han tenido que adaptar sus políticas para cumplir con sus disposiciones.

4.1.2 Estados Unidos. La Ley de privacidad del consumidor de California [10].

En contraste con Europa, la regulación de la protección de datos en Estados Unidos es más fragmentada. No existe una Ley federal unificada como el RGPD, pero sí existen Leyes estatales, siendo la Ley de privacidad del consumidor de California, “*California Consumer Privacy Act*” (CCPA) la más destacada. Algunas de las características principales son:

- **Enfoque sectorial:** En EE. UU., la regulación de datos está segmentada por sectores, con Leyes específicas para áreas como la salud o las finanzas, lo que genera cierta complejidad en el cumplimiento normativo.
- **Derecho de exclusión (“opt-out”):** La CCPA otorga a los consumidores el derecho de optar por no permitir que sus datos sean vendidos a terceros.
- **Derechos de acceso y eliminación:** Al igual que el RGPD, la CCPA otorga a los consumidores derechos para acceder, rectificar y eliminar sus datos.

- **Enfoque en la transparencia:** La *CCPA* se enfoca en aumentar la transparencia, requiriendo que las empresas informen claramente a los consumidores sobre las categorías de datos recopilados y su propósito.

A pesar de las similitudes con el RGPD como los derechos de acceso y eliminación, el enfoque estadounidense es más laxo en términos de consentimiento y supervisión, lo que genera un entorno más favorable para las empresas, pero con mayores riesgos para los consumidores.

4.1.3 Canadá. Ley de protección de información personal y documentos electrónicos. [30]

En Canadá, la Ley de protección de información personal y documentos electrónicos establece las bases para la protección de datos en las comunicaciones electrónicas. Esta Ley se aplica a la mayoría de las organizaciones comerciales canadienses y comparte muchas similitudes con el RGPD en términos de los derechos de los usuarios y las responsabilidades de las empresas. Sin embargo, a diferencia del RGPD, esta Ley permite una mayor flexibilidad en la transferencia de datos entre organizaciones y tiene menos restricciones en cuanto al consentimiento, lo que ha sido objeto de críticas.

4.1.4 Comparativa general

A modo de resumen, las principales diferencias y similitudes entre las normativas de protección de datos a nivel internacional se pueden agrupar en las siguientes categorías:

- **Consentimiento.** Mientras que el RGPD es altamente riguroso en la necesidad de consentimiento explícito, las Leyes de Estados Unidos y Canadá permiten un enfoque más flexible, con la posibilidad de optar por no participar (opt-out).
- **Multas y sanciones.** Las sanciones del RGPD son considerablemente más elevadas que las de las de Estados Unidos y Canadá, lo que crea un incentivo más fuerte para el cumplimiento normativo.
- **Transferencias internacionales.** Europa, bajo el RGPD, es más estricta en las transferencias internacionales de datos, mientras que en EE. UU. y Canadá las normativas son más permisivas, especialmente con países que se consideran seguros desde el punto de vista de la protección de datos.

En el anexo II del trabajo se representan los últimos datos estadísticos relativos a las sanciones impuestas en países europeos por incumplimiento del RGPD desde 2018. Estos datos incluyen información detallada sobre el número de sanciones y las cantidades acumuladas por cada país, lo que permite analizar las tendencias y diferencias entre las naciones. [31]

Asimismo, el anexo detalla las sanciones más altas impuestas tanto a empresas como a sectores específicos, ofreciendo una visión clara de qué entidades y áreas han sido más afectadas por las infracciones de la normativa. También se incluye un desglose de las sanciones más altas según el tipo de violación, lo que proporciona una perspectiva sobre qué infracciones han generado mayores consecuencias financieras en términos de sanciones. Este conjunto de datos facilita la comparación entre países y sectores, brindando una comprensión más profunda de la implementación y efectos de las regulaciones de protección de datos en Europa.

Del análisis de todas las gráficas del anexo se puede identificar que sectores como tecnología y comercio han sido los más penalizados desde julio del 2018, destacando la vulnerabilidad en el manejo de datos personales. Las infracciones más costosas están relacionadas con la falta de consentimiento adecuado y una protección insuficiente de datos. Esto pone de manifiesto la necesidad de continuar mejorando la transparencia y la ciberseguridad en las empresas.

La solución que se propone para conseguir reducir este tipo de sanciones es continuar implementando políticas, procedimientos y acciones para cumplir con las normativas en vigor, capacitar al personal en protección de datos y realizar auditorías regulares. Todas estas medidas van a permitir fortalecer la protección de datos y minimizar riesgos financieros.

4.2 Mejores Prácticas.

Las mejores prácticas en la protección de datos en las comunicaciones no solo dependen de cumplir con las normativas vigentes, sino de adoptar medidas proactivas que vayan más allá de lo que exige la Ley. A continuación, se exponen algunas de las estrategias más efectivas adoptadas por organizaciones líderes en el mundo.

4.2.1 Cifrado de extremo a extremo.

Una de las mejores prácticas más extendidas es el cifrado de extremo a extremo. Esta clase de cifrado está pensada para proteger tanto la confidencialidad como la integridad de los datos y es una técnica que garantiza que solo el remitente y el receptor de una comunicación puedan acceder a su contenido. Esta práctica es especialmente importante en aplicaciones de mensajería como “WhatsApp”, “Telegram” y “Signal”, que han implementado este tipo de cifrado para asegurar que los mensajes sean ilegibles para terceros, incluidos los proveedores de servicios. “WhatsApp”, “Telegram” y “Signal” son aplicaciones con enfoques diferentes en seguridad, privacidad y funcionalidades tal y como se indican en el resumen de la tabla 4-1.

“Signal” destaca por ser la opción más segura y privada, ya que no almacena metadatos y todo su contenido está cifrado de extremo a extremo *E2EE*, lo que garantiza máxima confidencialidad.

“Telegram” por su parte ofrece funcionalidades avanzadas como grupos masivos y almacenamiento en la nube, aunque su cifrado *E2EE* solo se aplica en los chats secretos que no dejan rastro en los servidores de Telegram y solo existen en los dispositivos involucrados. Además, incluye características adicionales como la autodestrucción de mensajes después de un tiempo definido.

Por último, “WhatsApp” es la aplicación más popular y utilizada globalmente, con cifrado *E2EE* activado por defecto en todas las comunicaciones, pero su gestión de metadatos genera preocupaciones debido a su integración con Meta.

Desde mi punto de vista, el cifrado de extremo a extremo en “WhatsApp” deja margen para ciertas dudas razonables. Aunque los mensajes estén cifrados, los metadatos (quién se comunica, cuándo, con qué frecuencia y desde dónde), no cuentan con la misma protección. Estos metadatos son extremadamente valiosos para la vigilancia masiva, ya que permiten reconstruir perfiles detallados de las personas sin necesidad de conocer el contenido específico de sus conversaciones. Además, una vez que la información que contiene el “WhatsApp” se almacena en los servidores externos de una compañía, aunque el canal de comunicación este protegido, se puede solicitar acceso a esa información siempre que se justifique por obligación legal como parte de una investigación.

Por ejemplo, en EE.UU. aunque no hay una obligación automática de ceder todos los datos personales a la “National Security Agency” (NSA), las Leyes estadounidenses permiten el acceso a datos bajo ciertas condiciones, especialmente en casos de seguridad nacional o actividades de inteligencia, y las empresas pueden ser requeridas a colaborar con las autoridades en estas situaciones.

	WhatsApp	Signal	Telegram
Propietario	Meta (Facebook)	Signal Foundation (Sin fines de lucro)	Pável Dúrov
Cifrado	Extremo a extremo	Extremo a extremo	Solo en "chats secretos"
Metadatos	Recopila y comparte con Meta	Mínimos, no guarda información	Almacena metadatos en la nube
Almacenamiento	Local y en la nube (no cifrado)	Solo local (cifrado)	En la nube (servidores propios)
Privacidad adicional	Copias de seguridad no cifradas	Copias de seguridad no cifradas	Chats secretos, autodestrucción
Ventaja principal	Popularidad y uso masivo	Máxima privacidad y seguridad	Funcionalidades avanzadas

Tabla 4-1. Características principales de las aplicaciones de mensajería.

El activista austriaco fundador de la ONG “*Europa versus Facebook*” Maximilian Schrems, cuestionó la transferencia de sus datos personales a EE. UU. por parte de “*Facebook*”. El Tribunal de Justicia de la Unión Europea (TJUE) argumentó que las prácticas de vigilancia en EE. UU. vulneraban los principios fundamentales de privacidad consagrados en la Carta de derechos fundamentales de la UE.

La sentencia *Schrems* [29], emitida por el TJUE en 2015, marcó un hito en la defensa del derecho a la privacidad en la era digital. La resolución de la sentencia invalidó el acuerdo de puerto seguro “*Safe Harbour*” entre la UE y EE. UU., al considerar que no garantizaba un nivel adecuado de protección de datos personales frente a la vigilancia masiva realizada por las autoridades estadounidenses. La sentencia ha impulsado la creación de marcos legales más estrictos y ha reforzado los estándares de protección de datos.

Desde mi punto de vista conseguir la privacidad digital de datos es un reto complejo en el contexto actual, pero existen medidas que pueden ayudarnos a conseguirlo. Entre ellas destaco el uso de aplicaciones de mensajería con cifrado y la creación de infraestructuras tecnológicas soberanas en cada país, reduciendo de esta manera la dependencia de empresas extranjeras en el que las Leyes de sus países permiten a las autoridades acceder a la información bajo condiciones específicas. También es fundamental fomentar la educación ciudadana sobre la importancia de proteger tanto los datos como los metadatos y promover normativas que limiten la vigilancia indiscriminada.

La clave es encontrar un equilibrio entre las necesidades de seguridad y la protección de los derechos fundamentales, una meta difícil de alcanzar en un contexto influenciado por intereses económicos y geopolíticos.

4.2.2 Minimización de datos.

La minimización de datos es una práctica que consiste en limitar la recopilación de datos personales al mínimo necesario para cumplir con el propósito específico para el cual se están procesando. Esta técnica es una de las recomendaciones clave del RGPD, pero va más allá de cumplir con la normativa.

La minimización de datos reduce los riesgos de una violación de datos, ya que, en caso de una brecha de seguridad, la cantidad de información comprometida será menor.

Empresas como “*Apple*” han hecho de esta práctica una piedra angular de su política de privacidad, limitando la cantidad de datos recopilados y almacenados en sus servidores.

Según mi opinión, esta medida adoptada por “*Apple*” es una respuesta ética y responsable a las crecientes preocupaciones sobre la privacidad. Sus beneficios en términos de seguridad y confianza del usuario son significativos y están alineados con las tendencias actuales hacia una mayor protección de los datos personales.

4.2.3 Transparencia y control para los usuarios.

Otro aspecto importante es la transparencia y el control para los usuarios. Las empresas líderes en protección de datos proporcionan a sus usuarios información clara y accesible sobre cómo se manejan sus datos y les ofrecen opciones de control sobre qué datos se recopilan, cómo se usan y si pueden ser eliminados.

Ejemplos de buenas prácticas en este ámbito incluyen la implementación de paneles de control de privacidad como el que ofrece Google [32], donde los usuarios pueden gestionar sus preferencias de privacidad de manera sencilla.

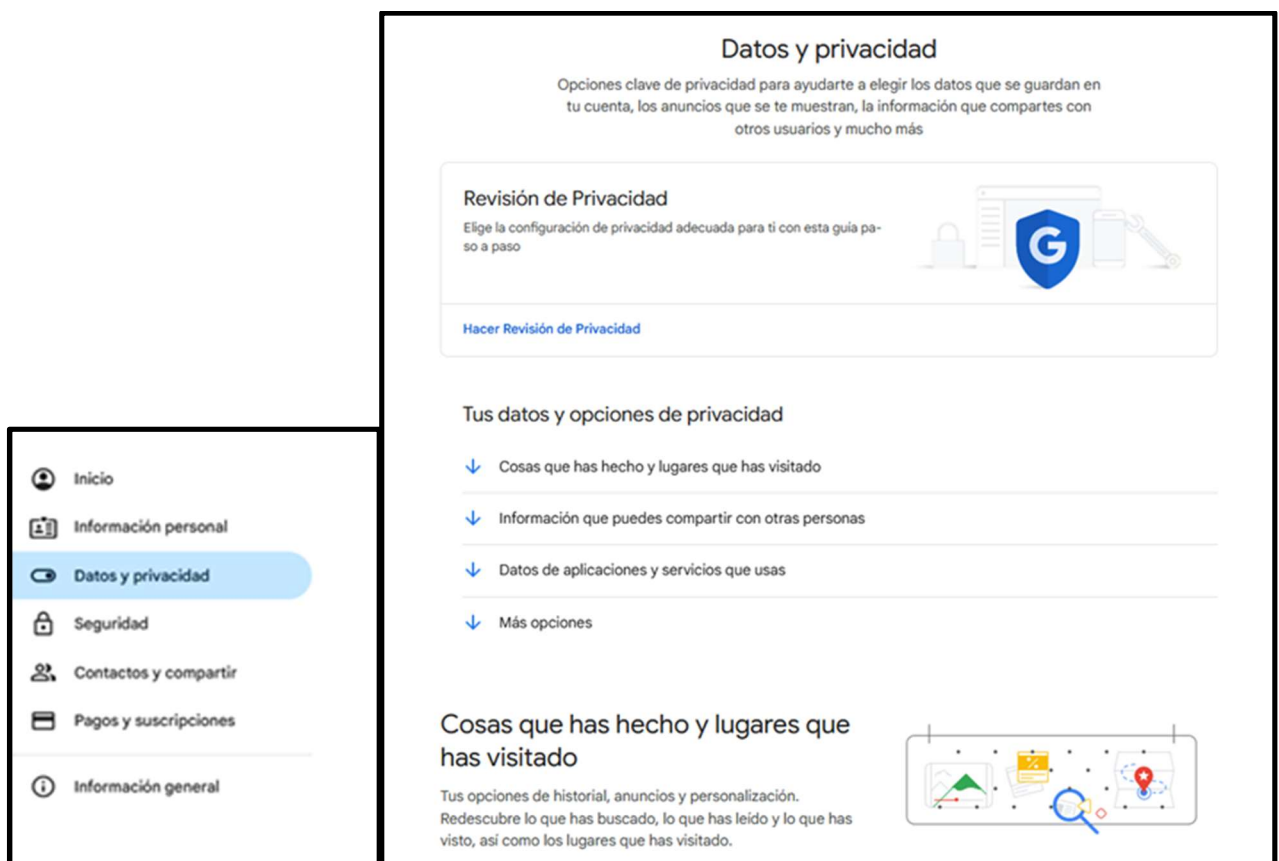


Figura 4-1. Panel de control de privacidad de Google. [32]

4.2.4 Auditorías regulares y cumplimiento proactivo.

Las auditorías regulares de los sistemas de protección de datos son otra práctica esencial. Estas auditorías permiten a las empresas identificar vulnerabilidades antes de que se conviertan en problemas graves y asegurar que se cumplan las normativas más recientes. Además, algunas empresas adoptan un enfoque de cumplimiento proactivo, que implica estar un paso por delante de los cambios legislativos y adoptar medidas preventivas para mejorar la seguridad y la privacidad.

El análisis comparativo internacional demuestra que, aunque las normativas de protección de datos varían de un país a otro, existe una tendencia clara hacia la adopción de normas más estrictas en torno a la privacidad y la seguridad de las comunicaciones. Estas medidas no solo ayudan a las empresas a protegerse frente a riesgos, sino que también fortalecen su reputación y cumplimiento con las expectativas crecientes de los consumidores y las autoridades.

4.2.5 Gestión de los datos personales.

El conflicto entre la seguridad y la privacidad en las comunicaciones representa uno de los mayores desafíos en la gestión de datos personales. Las medidas de seguridad implementadas por las empresas, como la monitorización de actividades sospechosas y la retención prolongada de datos para investigaciones, buscan prevenir delitos y garantizar la integridad de las redes. Sin embargo, estas prácticas pueden entrar en conflicto con los derechos de privacidad de los usuarios, ya que implican un acceso constante y potencialmente intrusivo a información sensible. Esta situación se intensifica cuando las entidades gubernamentales solicitan acceso a datos personales para fines de seguridad nacional o investigaciones penales.

Aunque estas medidas pueden justificarse para proteger a la sociedad, también generan importantes cuestiones éticas y legales sobre el equilibrio entre la seguridad colectiva y la privacidad individual. Este conflicto pone de manifiesto la necesidad de una regulación clara, estableciendo una política que limite la retención de datos a períodos estrictamente necesarios, garantice el anonimato en ciertos casos y defina protocolos transparentes para el acceso a la información, evitando abusos y garantizando la confianza de los usuarios.

Los datos personales recopilados en España por los operadores de telefonía, plataformas de contenidos en Internet, organismos públicos y dispositivos *IoT* se utilizan para diversos fines, pero su gestión en ocasiones plantea dudas sobre privacidad. La gestión de datos personales depende del sector en el que nos encontremos. Los operadores de telefonía recopilan información como ubicación, consumo de datos y llamadas, usándola para personalizar servicios, generar perfiles publicitarios y, en algunos casos, compartirla con terceros bajo términos de privacidad. En el caso de las plataformas de contenidos, como servicios de “*streaming*”⁸, recogen datos de navegación y preferencias con fines publicitarios para recomendar contenido.

Los organismos públicos administran datos sensibles, como información tributaria o sanitaria, con fines administrativos y de prestación de servicios, aunque su centralización y digitalización pueden exponerlos a brechas de seguridad.

En el ámbito médico, los datos se utilizan para diagnósticos y tratamientos, pero a menudo se almacenan en sistemas vulnerables. Los dispositivos domóticos y de *IoT* recopilan datos de hábitos, rutinas y consumo energético, que son enviados a servidores externos, muchas veces en otras jurisdicciones con estándares de protección menores.

⁸ El streaming es una tecnología que permite la transmisión continua de datos multimedia a través de internet, sin necesidad de descargar el contenido completo antes de reproducirlo. Esto permite que los usuarios accedan en tiempo real a películas, series, música, eventos en vivo o juegos, mientras los datos se descargan progresivamente.

En mi opinión, la regulación actual en España guiada por el RGPD, establece marcos sólidos, pero existen algunas lagunas. Estas lagunas incluyen la falta de transparencia en el uso de datos, la dificultad de los usuarios para ejercer control sobre su información, la exposición a ciberataques y una legislación específica dedicada exclusivamente a la protección de datos en dispositivos *IoT*.

Las soluciones que se podrían aplicar para resolver estas lagunas son exigir la localización y procesamiento de datos dentro del país, mayor cifrado de la información almacenada y sanciones más estrictas para el uso indebido de los datos. Además, se necesita una legislación que regule específicamente los dispositivos *IoT*, con estándares de seguridad obligatorios, que contribuyan a un ecosistema digital más seguro y respetuoso con la privacidad. Las características únicas del *IoT*, como la gran cantidad de dispositivos y la transferencia constante de datos a través de redes globales, exigen regulaciones que establezcan estándares mínimos de seguridad, cifrado obligatorio, interoperabilidad y mecanismos de control más accesibles para los usuarios.

Las mejores prácticas descritas proporcionan un marco sólido para que las organizaciones fortalezcan sus estrategias de protección de datos, contribuyendo no solo al cumplimiento normativo, sino también a la confianza del usuario en sus servicios.

5 RESULTADOS Y DISCUSIÓN

5.1 Análisis de los hallazgos

El análisis de los hallazgos se centra en evaluar cómo las regulaciones actuales de protección de datos influyen en las comunicaciones digitales y cuáles son los principales desafíos y vulnerabilidades identificadas en el manejo de datos personales en este ámbito. Además, se revisa las implicaciones prácticas de estas normativas en la privacidad y seguridad de los usuarios, tanto a nivel individual como empresarial.

5.1.1 Regulaciones existentes en protección de datos y su aplicación en las comunicaciones.

Un aspecto destacado del análisis es la identificación de las regulaciones vigentes, como el RGPD en la UE, la LOPDGDD en España, y otras legislaciones internacionales. Estas regulaciones han tenido un impacto significativo en la forma en que las empresas de telecomunicaciones y proveedores de servicios de internet gestionan los datos personales.

Un hallazgo clave es que, aunque las normativas han mejorado en la transparencia y el control de los usuarios sobre sus datos, todavía existen desafíos en la implementación efectiva, especialmente en entornos transfronterizos o en plataformas globales como redes sociales y servicios de mensajería instantánea.

5.1.2 Vulnerabilidades en el tratamiento de datos en comunicaciones digitales.

Otro aspecto importante encontrado en el análisis es la identificación de vulnerabilidades en el manejo de datos dentro del sector de las comunicaciones. A pesar de los esfuerzos regulatorios, persisten riesgos relacionados con la captura y el uso indebido de datos a través de ataques como el “*phishing*”, el “*malware*” y la monitorización no autorizado de la actividad en línea. La falta de control total sobre las herramientas de cifrado en servicios como correos electrónicos y mensajería instantánea es otro de los factores que pone en riesgo la seguridad de los datos.

Además, el análisis ha revelado que la mayoría de las plataformas de comunicación continúan utilizando sistemas de cifrado continuo (*end-to-end*), pero existen lagunas cuando estos datos se almacenan en servidores externos. Es decir, aunque las comunicaciones en tránsito pueden estar seguras, los datos almacenados pueden estar expuestos a posibles infracciones de seguridad.

5.1.3 Tensión entre seguridad y privacidad.

El equilibrio entre la seguridad y la privacidad es otro de los puntos resaltados en el análisis. Los sistemas de comunicación, como los correos electrónicos y las aplicaciones de mensajería, tienen que enfrentarse al desafío de proporcionar entornos seguros sin comprometer la privacidad de los usuarios.

El hallazgo más relevante es que las medidas de seguridad, como la monitorización de actividades sospechosas o la retención de datos para investigaciones, pueden entrar en conflicto con el derecho a la privacidad. Este conflicto es especialmente notable en las políticas de retención de datos y las solicitudes de acceso por parte de gobiernos y autoridades judiciales.

5.1.4 Adopción de buenas prácticas de protección de datos.

A partir de los datos encontrados, se ha podido observar que las organizaciones han comenzado a adoptar mejores prácticas en cuanto a la protección de datos. La implementación de políticas de privacidad más claras, la incorporación de oficiales de protección de datos “*Data Protection Officer*” (DPO) y la educación de los empleados sobre el manejo adecuado de la información son pasos importantes que muchas empresas han dado en los últimos años. Sin embargo, hay diferencias

significativas en la adopción de estas medidas entre pequeñas y grandes empresas, lo que pone de relieve la necesidad de apoyar a las pequeñas y medianas empresas en el cumplimiento normativo.

Los resultados obtenidos no solo confirman la importancia de las normativas en la protección de datos, sino que también resaltan las áreas donde se requieren mejoras significativas. La complejidad de los entornos digitales y la rápida evolución de las tecnologías de comunicación plantean un desafío continuo para la protección de los datos personales.

Los hallazgos muestran que, aunque la legislación existente es robusta, la implementación efectiva en diferentes escenarios y geografías es inconsistente debido a diferencias en las normativas de los países y a presiones políticas y comerciales. Esto afecta tanto a los derechos de los usuarios como a la confianza general en los servicios de comunicación.

5.2 Discusión crítica

5.2.1 Evaluación de las políticas actuales.

La normativa actual, como el RGPD, representa un marco fundamental para la protección de los datos personales. Sin embargo, la efectividad de estas normativas depende en gran medida de su correcta implementación y aplicación. Una crítica importante es que, a pesar de los esfuerzos de los legisladores, la aplicación de las leyes a menudo no es suficiente, especialmente en el contexto internacional.

Por ejemplo, las grandes plataformas globales, como “Google”, “Facebook” y “WhatsApp”, operan bajo diferentes normativas según las regiones, lo que plantea desafíos en el cumplimiento de la norma. Además, las jurisdicciones fuera de la UE no siempre están alineadas con los estándares de protección de datos establecidos en el RGPD, lo que deja a los usuarios vulnerables en ciertos contextos.

El análisis de los casos de infracciones de datos en los últimos años indica que, a pesar de las fuertes sanciones financieras que impone el RGPD, los incidentes de filtración y mal uso de datos siguen ocurriendo con frecuencia. Esto pone en duda si las sanciones son suficientes para disuadir a las empresas de prácticas inadecuadas, o si es necesario un mayor enfoque en la supervisión y la prevención proactiva.

5.2.2 Desafíos tecnológicos y su impacto

El rápido avance de las tecnologías en el ámbito de las comunicaciones ha generado nuevos retos para la protección de datos. Tecnologías como la IA, el “Big Data” y el “IoT” permiten la recolección masiva de información a través de comunicaciones digitales. Esta situación plantea preguntas sobre cómo las regulaciones existentes pueden adaptarse a estos avances.

Un aspecto clave, es que las normas como el RGPD están diseñadas para un entorno más estático, y no pueden abordar completamente los desafíos emergentes planteados por la vigilancia masiva o el análisis de grandes cantidades de datos. Por ejemplo, los dispositivos *IoT* transmiten datos de forma constante y, en muchos casos, los usuarios no son conscientes de la cantidad de información que están compartiendo. Este fenómeno expone una brecha entre las expectativas de privacidad y la realidad de los sistemas tecnológicos actuales.

Como solución para mitigar los riesgos asociados al uso del IoT se propone crear una normativa más detallada para *IoT*, que incluya y defina las siguientes características clave que garanticen la protección de los datos personales y la seguridad de los dispositivos:

- a) **Transparencia obligatoria.** Requerir que los fabricantes proporcionen información clara y detallada sobre qué datos recopilan los dispositivos, cómo se almacenan, con quién se comparten y durante cuánto tiempo.
- b) **Consentimiento activo del usuario.** Establecer que los dispositivos IoT solo puedan recopilar datos si los usuarios otorgan un consentimiento explícito e informado, con la posibilidad de modificar o retirar dicho consentimiento en cualquier momento.
- c) **Seguridad por diseño.** Exigir que todos los dispositivos IoT incluyan medidas de seguridad desde la etapa de desarrollo, como autenticación robusta, actualizaciones automáticas y cifrado de extremo a extremo para la transmisión y almacenamiento de datos.
- d) **Interoperabilidad y portabilidad de datos.** Promover estándares que permitan a los usuarios transferir sus datos de un dispositivo o plataforma a otra sin restricciones, asegurando que no queden atrapados en sistemas cerrados.
- e) **Auditorías regulares y certificación obligatoria.** Implementar un sistema de auditorías periódicas para verificar el cumplimiento de las normativas, así como un esquema de certificación que garantice que los dispositivos cumplen con los estándares mínimos de seguridad y privacidad.
- f) **Controles de usuario simples e intuitivos.** Asegurar que los usuarios puedan gestionar fácilmente sus configuraciones de privacidad y acceso, utilizando interfaces claras y accesibles que no requieran conocimientos técnicos avanzados.
- g) **Responsabilidad de los fabricantes y proveedores.** Asignar la responsabilidad a los fabricantes y proveedores de servicios en caso de violaciones de privacidad o fallos de seguridad, incentivando el cumplimiento riguroso de las normativas.

5.2.3 Conflicto entre intereses comerciales y derechos de los usuarios

Una de las cuestiones más importantes en este campo es el conflicto entre los intereses comerciales de las empresas de comunicación y los derechos de los usuarios en cuanto a la protección de sus datos. Las empresas de telecomunicaciones y las plataformas de mensajería basan gran parte de su modelo de negocio en la recopilación y análisis de datos personales. Este modelo pone a los usuarios en una posición vulnerable, ya que sus datos pueden ser utilizados para generar perfiles comerciales o ser vendidos a terceros sin su consentimiento explícito.

Existe una desigualdad de poder entre los usuarios y las empresas, ya que los primeros no siempre comprenden completamente las implicaciones del uso de sus datos. Además, los términos y condiciones suelen ser largos y complejos, lo que dificulta que los usuarios tomen decisiones informadas.

5.2.4 Recomendaciones para mejorar la protección de datos

De los resultados obtenidos en el trabajo surgen las siguientes recomendaciones indicadas a continuación para mejorar el marco de protección de datos en las telecomunicaciones. En primer lugar, es fundamental avanzar hacia una mayor armonización de las normativas a nivel global. La existencia de marcos regulatorios diferentes entre regiones y países crea inconsistencias y vacíos legales que pueden ser aprovechados por empresas multinacionales. Por tanto, se recomienda impulsar acuerdos internacionales que alineen los estándares de protección de datos, como una extensión del RGPD a otros países fuera de la UE, o la creación de normativas equivalentes que garanticen los mismos niveles de protección en todos los países.

Existen precedentes significativos de armonización de normativas de protección de datos, como el Convenio 108 del Consejo de Europa y su versión modernizada el Convenio 108+, que establece estándares internacionales. Sin embargo, armonizar normativas globales presenta retos importantes, como son las diferencias culturales y legales en la percepción de la privacidad, las tensiones sobre la soberanía nacional, los intereses económicos de empresas tecnológicas que podrían resistirse a mayores restricciones, y los conflictos con leyes orientadas a la seguridad nacional, como las de China o Rusia.

La Unión Europea como líder en protección de datos, podría impulsar una propuesta de acuerdo internacional basado en el RGPD, mientras que organismos internacionales como la organización de naciones unidas (ONU) o la organización para la cooperación y el desarrollo económico (OCDE), son plataformas ideales para liderar iniciativas globales. La clave será equilibrar los derechos de Organización para la Cooperación y el Desarrollo Económico privacidad con las necesidades económicas y políticas globales, promoviendo estándares universales que garanticen una protección efectiva de los datos.

En segundo lugar, se debe reforzar la aplicación de las normativas existentes mediante la implementación de medidas de supervisión más estrictas y la imposición de sanciones más disuasorias, especialmente en el caso de grandes empresas tecnológicas. Las multas deben ser proporcionales a los ingresos de las empresas para que realmente sirvan como un freno efectivo ante prácticas inadecuadas. Asimismo, sería recomendable implementar mecanismos de control que permitan verificar que las deficiencias detectadas durante las auditorías o inspecciones sean efectivamente subsanadas, asegurando así el cumplimiento de las normativas vigentes.

De igual manera, la educación y concienciación de los usuarios es esencial para mejorar la protección de datos en las comunicaciones. A pesar de los esfuerzos regulatorios, muchos usuarios siguen siendo poco conscientes de sus derechos y de cómo se utilizan sus datos. Según mi perspectiva, se necesita desarrollar campañas de concienciación a gran escala, dirigidas tanto a usuarios individuales como a empresas, sobre los riesgos asociados al mal uso de los datos y las formas de protegerlos de manera efectiva. Existen algunas campañas actuales que buscan este objetivo, como las promovidas por la AEPD, que ofrece guías y recursos educativos para usuarios y empresas, o iniciativas europeas centradas en el RGPD que explican los derechos de los ciudadanos y las obligaciones de las empresas. Sin embargo, estas campañas a menudo tienen un alcance limitado y no siempre utilizan canales o formatos que capten la atención del público general. Para mejorar su efectividad, podrían incluirse estrategias más innovadoras, como el uso de redes sociales o colaboraciones con “*influencers*”, además de centrarse en mensajes más prácticos y accesibles que expliquen cómo proteger los datos en el día a día.

Asimismo, se recomienda que las empresas inviertan en infraestructuras tecnológicas propias dentro del territorio nacional para guardar sus datos y disminuir la dependencia de compañías extranjeras, y en sistemas de detección temprana de infracciones de seguridad, basados en IA y ML, para identificar amenazas antes de que causen daños significativos. Estas tecnologías nos van a permitir adoptar una respuesta más rápida y eficaz frente a posibles incidentes. Algunas empresas como Amazon Web Services (AWS), Google y Microsoft ya han comenzado a implementar estas estrategias, desarrollando centros de datos regionales en diferentes países para cumplir con normativas locales de protección de datos. En el sector financiero, Santander y BBVA también han implementado infraestructuras tecnológicas propias, junto con sistemas de IA y ML para la detección de fraudes y ciberataques. Sin embargo, estas empresas se enfrentan a desafíos significativos, como las grandes inversiones iniciales necesarias para infraestructuras y tecnologías, la necesidad de atraer y retener talento especializado, y el constante avance de las ciberamenazas, que exige actualizaciones continuas. A pesar de todos estos

desafíos, las ventajas relacionadas con la independencia tecnológica, el cumplimiento de las normativas y la confianza del cliente superan considerablemente las dificultades.

Finalmente, es importante prestar apoyo a las pequeñas y medianas empresas para que puedan cumplir con las normativas de protección de datos de manera efectiva. Se recomienda que los gobiernos proporcionen recursos y herramientas específicas, como guías prácticas, formación especializada y financiación para la adopción de medidas de seguridad adecuadas. Esto garantizará que todas las empresas, independientemente de su tamaño, puedan proteger los datos de sus usuarios de manera efectiva. La colaboración entre gobiernos, organizaciones y la industria tecnológica será clave para poder afrontar todas estas situaciones. Actualmente existen en la Unión Europea diversas agencias y organismos que ofrecen programas de formación y asesoramiento para PYMES sobre el cumplimiento del RGPD. En España la AEPD ha desarrollado herramientas como el Facilita RGPD [16], que ayuda a las pequeñas empresas a implementar medidas básicas de protección de datos. A pesar de todo esto, muchas de estas iniciativas son limitadas en alcance y recursos, por lo que podrían mejorarse ampliando su cobertura, ofreciendo subvenciones más accesibles y diseñando soluciones tecnológicas más adaptadas a las necesidades específicas de las PYMES.

6 CONCLUSIONES Y LÍNEAS FUTURAS

6.1 Conclusiones

En la actualidad, la protección de datos en el ámbito de las telecomunicaciones se enfrenta a un panorama cada vez más complejo y desafiante debido a la evolución rápida de las tecnologías digitales y la creciente dependencia de estas en la vida cotidiana. El trabajo ha permitido alcanzar los objetivos planteados en el TFM de manera satisfactoria, aunque con matices en cuanto a la profundidad de los logros obtenidos.

El primer objetivo se ha cumplido mediante un estudio exhaustivo del RGPD como marco normativo central, además de otras regulaciones globales relevantes. Se ha demostrado cómo estas normativas han transformado significativamente la gestión de los datos personales en el sector, promoviendo un enfoque más transparente y centrado en el usuario. No obstante, también se identificaron lagunas en su implementación, especialmente en contextos transfronterizos y en plataformas globales, lo que evidencia que aún existen áreas críticas por abordar.

En el segundo objetivo, se ha constatado que las empresas de telecomunicaciones han implementado tecnologías clave como el cifrado, la anonimización y políticas avanzadas de acceso y control de datos. Sin embargo, la adopción de estas medidas sigue siendo desigual entre grandes y pequeñas organizaciones, con las primeras liderando en recursos y formación especializada, mientras que las PYMES se enfrentan a limitaciones significativas. Esto subraya la necesidad de fortalecer el apoyo a estas últimas para garantizar una protección uniforme.

El tercer objetivo se ha logrado al exponer los desafíos técnicos, organizativos y regulatorios a los que se enfrenta el sector. Entre los más destacados se encuentran el conflicto entre seguridad y privacidad, las dificultades para garantizar el cumplimiento normativo en un entorno digital global y los retos asociados a tecnologías emergentes como 5G, *IoT* e IA. Estas dificultades reflejan la complejidad de equilibrar la innovación tecnológica con la protección de los derechos fundamentales de los usuarios.

En cuanto al último objetivo, las conclusiones obtenidas en el TFM han permitido exponer una serie de recomendaciones que aparecen señaladas en el subsubapartado 5.2.4 para mejorar la protección de datos en el ámbito de las telecomunicaciones. Estas incluyen armonizar normativas globales, lideradas por la UE con apoyo de la ONU y la OCDE, y reforzar el cumplimiento con sanciones disuasorias y controles efectivos. Se destaca la necesidad de campañas educativas innovadoras y accesibles para usuarios. Además, se sugiere que las empresas inviertan en infraestructuras propias y tecnologías avanzadas, siguiendo el ejemplo de AWS, Google, Santander y BBVA, y que se brinde mayor apoyo a las PYMES mediante recursos, formación y financiación, mejorando iniciativas actuales para ampliar su alcance y eficacia.

En resumen, el análisis realizado ha permitido no solo evaluar el estado actual de la protección de datos en el sector de las telecomunicaciones, sino también destacar áreas críticas de mejora y proponer estrategias viables para abordar los desafíos identificados. Aunque los avances son significativos, queda un camino por recorrer para alcanzar una protección de datos más efectiva, uniforme y adaptada al rápido avance tecnológico.

6.2 Líneas futuras.

El trabajo presentado deja abiertas diversas áreas que pueden explorarse en futuros estudios para para mejorar y ampliar la protección de datos en el sector de las telecomunicaciones. Una línea interesante es el análisis de las implicaciones de las tecnologías emergentes, como la IA, el *ML* y el “*blockchain*”, en la protección de datos personales. Estas tecnologías tienen el potencial de mejorar la seguridad de los sistemas, pero también plantean desafíos éticos y regulatorios que deben ser evaluados en profundidad. Por ejemplo, investigar cómo el “*blockchain*” puede mejorar la trazabilidad y el control de acceso a datos sensibles sería una contribución valiosa.

Otro aspecto significativo es la evaluación del impacto de las nuevas normativas internacionales que podrían surgir en los próximos años. El trabajo podría incluir estudios comparativos sobre cómo distintos países adoptan y adaptan el RGPD u otros marcos similares, y cómo estas adaptaciones afectan la competitividad de las empresas del sector. Asimismo, podría ser interesante explorar cómo las empresas internacionales ajustan sus estrategias de cumplimiento normativo en contextos con regulaciones divergentes.

Desde una perspectiva práctica, un enfoque en la implementación de estrategias efectivas para PYMES sería particularmente valioso. Esto incluye desarrollar herramientas específicas de bajo costo y fácil acceso que les permitan cumplir con las normativas sin comprometer su viabilidad económica.

Finalmente, una línea de trabajo que combine aspectos técnicos, legales y sociales sería investigar cómo se pueden diseñar campañas educativas más efectivas para usuarios y empresas, utilizando canales modernos como redes sociales o colaboraciones con instituciones educativas. Estas campañas podrían incluir simulaciones prácticas sobre ciberseguridad y protección de datos para mejorar la concienciación y la preparación ante posibles incidentes.

Estas propuestas no solo complementan los hallazgos del presente trabajo, sino que también abren nuevas oportunidades para continuar mejorando la protección de datos en un sector en constante evolución.

BIBLIOGRAFÍA

- [1] «Diario oficial de la Unión Europea» [En línea]. Available: [REGLAMENTO\(UE\) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE \(Reglamentogeneral de protección de datos\)](#) *Versión consolidada NO oficial: incluye las correcciones de errores publicadas en DOUE L 127 de 23.5.2018 y DOUE L 74 de 4.3.2021. [Último acceso: 10 enero 2025].
- [2] «Diario oficial de la Unión Europea» [En línea]. Available: [Corrección de errores del Reglamento\(UE\) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE \(Reglamentogeneral de protección de datos\)](#) [23 mayo 2018]. [Último acceso: 10 enero 2025].
- [3] «Diario oficial de la Unión Europea» [En línea]. Available: [Corrección de errores del Reglamento\(UE\) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE \(Reglamentogeneral de protección de datos\)](#) [4 marzo 2021]. [Último acceso: 10 enero 2025].
- [4] «Boletín Oficial del Estado» [En línea]. Available: Sentencia del Tribunal Constitucional (STC) 254/1993, de 20 de julio de 1993. https://www.boe.es/diario_boe/txt.php?id=BOE-T-1993-21425 [Último acceso: 10 enero 2025].
- [5] «Boletín Oficial del Estado» [En línea]. Available: Sentencia del Tribunal Constitucional (STC) 290/2000, de 30 de noviembre de 2000. <https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332> [Último acceso: 10 enero 2025].
- [6] Bygrave, L. A. (2014). Data Privacy Law: An International Perspective. Oxford University Press.
- [7] «Diario oficial de las Comunidades Europeas». Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. [En línea]. Available: [L00031-00050.pdf \(boe.es\)](#) [Último acceso: 10 enero 2025].
- [8] «Diario oficial de la Unión Europea» [En línea]. Available: [DIRECTIVA \(UE\) 2016/ 680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016 - relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/ 977/ JAI del Consejo \(boe.es\)](#) [Último acceso: 10 enero 2025].
- [9] «Diario oficial de las Comunidades Europeas». DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas. [En línea]. Available: [L00037-00047.pdf \(boe.es\)](#) [Último acceso: 10 enero 2025].
- [10] «California Legislative Legislation Web» Ley de privacidad del consumidor de California (CCPA). [En línea]. Available:

- https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 [Último acceso: 10 enero 2025].
- [11] «Presidência da República Secretaria-Geral Subchefia para Assuntos Jurídicos Web». Ley de protección de datos personales de Brasil (LGPD). [En línea]. Available: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. [Último acceso: 10 enero 2025].
- [12] «Japanese Law Translation Web». Ley de protección de la información personal de Japón. [En línea]. Available: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en#je_ch2 [Último acceso: 10 enero 2025].
- [13] Jessica Losada, (enero 2021). 40 años de protección de datos en Europa (2): el caso español. [En línea]. Available: <https://protecciondatos.conversia.es/proteccion-de-datos-europa-espana>. [Último acceso: 10 enero 2025]
- [14] [En línea]. Available: https://www.researchgate.net/figure/Data-Protection-Impact-Assessment-DPIA-Data-Wheel_fig2_341608950 [Último acceso: 10 enero 2025]
- [15] [En línea]. Available: <https://www.telefonica.com/es/sala-comunicacion/blog/proteger-redes-5g-retos-oportunidades-sector-telecomunicaciones/> [Último acceso: 10 enero 2025]
- [16] [En línea]. Available: <https://www.aepd.es/guias-y-herramientas/herramientas/> [Último acceso: 10 enero 2025]
- [17] [En línea]. Available: <https://www.realinstitutoelcano.org/analisis/descubriendo-los-desafios-tecnicos-para-la-seguridad-en-las-redes-5g/> [Último acceso: 10 enero 2025]
- [18] Akashah Arshad, Zurina Mohd Hanapi, Shamala Subramaniam, Rohaya Latip, September 22, 2021 [En línea]. Available: [A survey of Sybil attack countermeasures in IoT-based wireless sensor networks \[PeerJ\]](#). [Último acceso: 10 enero 2025]
- [19] Donpiti (Mick) Chulerttiyawong, Abbas Jamalipour, (julio 2023). [En línea]. Available: [\(PDF\) Sybil Attack Detection in Internet of Flying Things-IoFT: A Machine Learning Approach \(researchgate.net\)](#) [Último acceso: 10 enero 2025]
- [20] Guia de privacidad desde el diseño de la AEPD (octubre 2019) [En línea]. Available: <https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf> [Último acceso: 10 enero 2025]
- [21] [En línea]. Available: <https://www.normaiso27001.es/> [Último acceso: 10 enero 2025]
- [22] Resolución de procedimiento sancionador de la AEPD. Procedimiento N°: PS/00059/2020. [En línea]. Available: <https://www.aepd.es/documento/ps-00059-2020.pdf> [Último acceso: 10 enero 2025]
- [23] [En línea]. Available: www.incibe.es/incibe/sala-de-prensa/los-incidentes-de-ciberseguridad-de-2023-gestionados-por-incibe-aumentan-en [Último acceso: 10 enero 2025]
- [24] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). [En línea]. Available: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079> [Último acceso: 10 enero 2025]

- [25] Gestión del riesgo y evaluación de impacto en tratamientos de datos personales de la AEPD (junio 2021) [En línea]. Available: <https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf> [Último acceso: 10 enero 2025]
- [26] Esquema Nacional de Seguridad. Gestión de ciberincidentes. Guía de Seguridad de las TIC CCN-STIC 817, (junio 2021) [En línea]. Available: <https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html> [Último acceso: 10 enero 2025]
- [27] [En línea]. Available: [Infracciones y Sanciones LOPDGDD y RGPD | Grupo Atico34](#) [Último acceso: 10 enero 2025]
- [28] Memoria anual de la AEPD. [En línea]. Available: <https://www.aepd.es/memorias/memoria-aepd-2023.pdf> [Último acceso: 10 enero 2025]
- [29] Puerto, M.I. y Sferrazza Taibi, P. 2017. La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. *Revista derecho del Estado*. 40 (dic. 2017). [En línea]. Available: <https://doi.org/10.18601/01229893.n40.09>. [Último acceso: 10 enero 2025]
- [30] «Office of the Privacy Commissioner of Canada Web» [En línea]. Available: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/> [Último acceso: 10 enero 2025]
- [31] «GDPR Enforcement Tracker Web» [En línea]. Available: [En línea]. Available: <https://www.enforcementtracker.com/> [Último acceso: 10 enero 2025]
- [32] [En línea]. Available: [Data privacy settings & controls – Google Safety Centre \(safety-google.translate.goog\)](#) [Último acceso: 10 enero 2025]

ANEXO I: EVOLUCIÓN DE MULTAS EN ESPAÑA.

Evolución de las multas impuestas	2022	2023	Δ% anual
Número de multas	378	367	-3%
Importe total	20.775.361	29.817.410 €	44%

Figura A1-1. Evolución de multas impuestas en España. [28]

Responsable	Infracción	Multa
BANCO BILBAO VIZCAYA ARGENTARIA, S.A.	Art. 6.1 RGPD, art. 25 RGPD, art 32 RGPD	1.184.000€
CAIXABANK, S.A.	Art. 5.1.f) RGPD, art. 25 RGPD, art. 32 RGPD	5.000.000€
OPEN BANK, SA.	Art. 25 RGPD, art. 32 RGPD	2.500.000€

Figura A1-2. Multas superiores al millón de euros en resolución firme y ejecutiva. [28]

Importe de multas en euros según el tema	2022	2023	% relativo	Δ% anual
Seis temas con mayor importe total en 2023	14.241.901€	26.433.600 €	89%	86%
Quiebras de seguridad	821.800 €	12.907.000 €	43%	1471%
Entidades financieras / acreedoras	596.200 €	5.321.000 €	18%	792%
Derechos protección datos	5.900 €	2.633.400 €	9%	44534%
Contratación fraudulenta	706.800 €	2.571.500 €	9%	264%
Telecomunicaciones	632.000 €	1.942.000 €	7%	207%
Servicios de Internet	11.479.201 €	1.058.700 €	4%	-91%
Otros	6.533.460 €	3.383.810 €	11%	-48%
TOTAL	20.775.361 €	29.817.410 €	100%	44%

Figura A1-3. Áreas con mayor importe global de multas. [28]

ANEXO II: SANCIONES POR INCUMPLIMIENTO DEL RGPD.

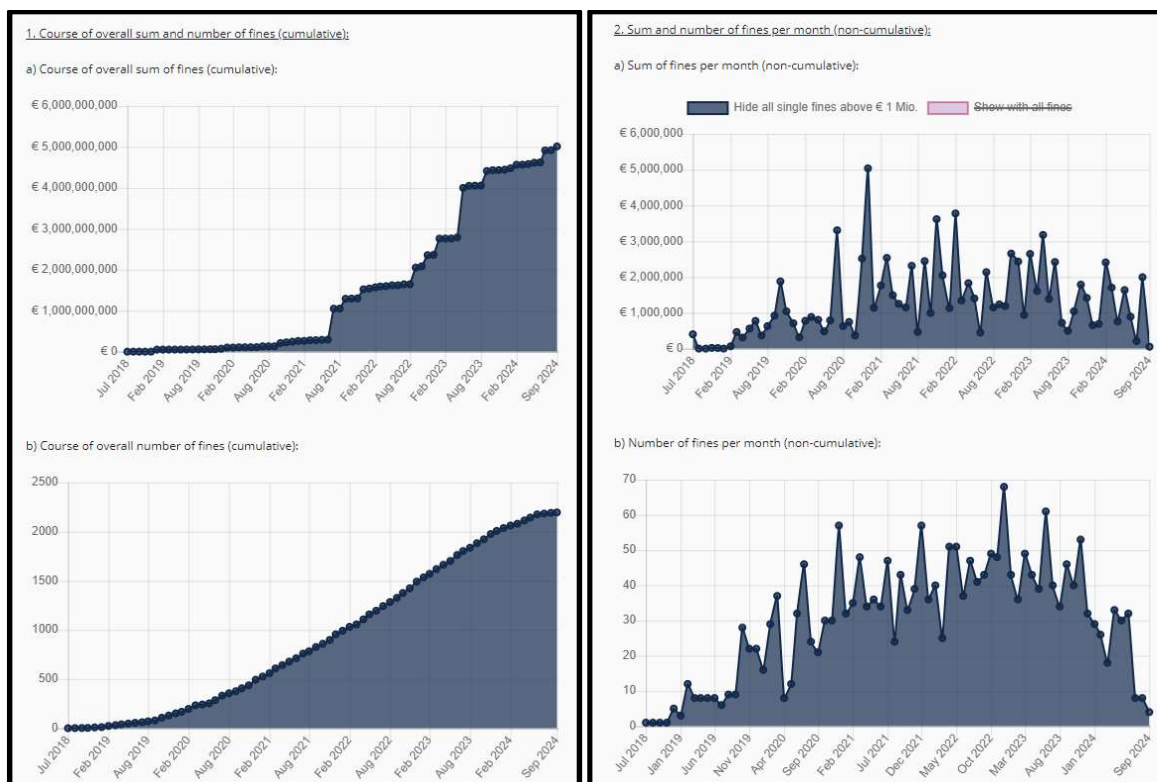


Figura A2-1. Número de sanciones y cantidades acumuladas desde 2018. [31]

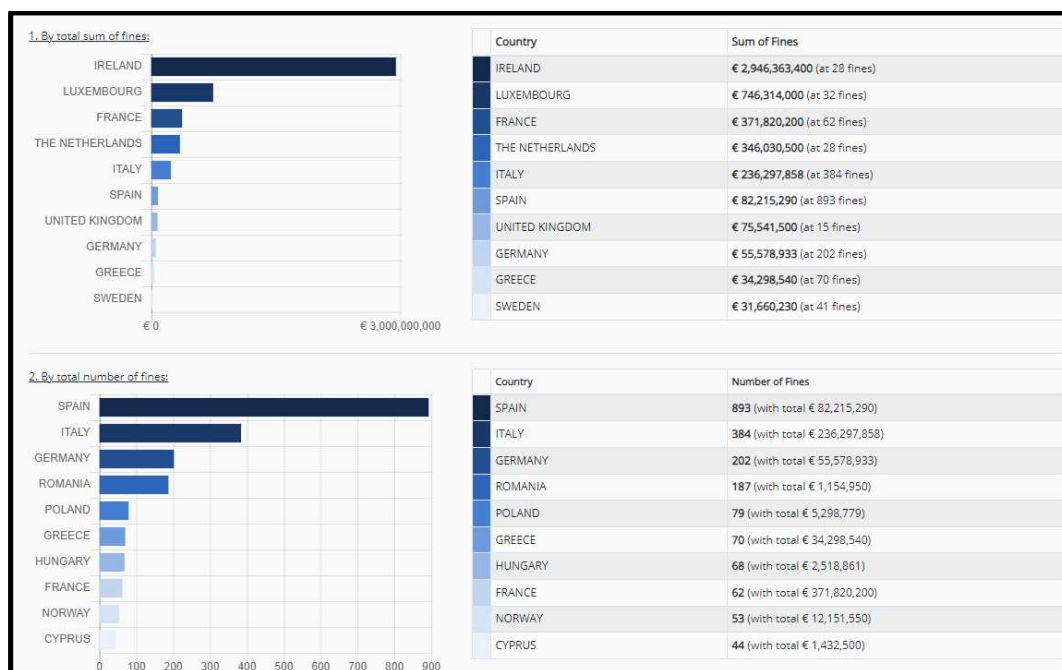


Figura A2-2. Sanciones más altas por países. [31]

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	1200000000	Insufficient legal basis for data processing	2023-05-12
2	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746000000	Non-compliance with general data processing principles	2021-07-16
3	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405000000	Non-compliance with general data processing principles	2022-09-05
4	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	390000000	Non-compliance with general data processing principles	2023-01-04
5	TikTok Limited	Media, Telecoms and Broadcasting	IRELAND	345000000	Non-compliance with general data processing principles	2023-09-01
6	Uber Technologies Inc., Uber B.V.	Employment	THE NETHERLANDS	290000000	Non-compliance with general data processing principles	2024-07-22
7	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	265000000	Insufficient technical and organisational measures to ensure information security	2022-11-25
8	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225000000	Insufficient fulfilment of information obligations	2021-09-02
9	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	91000000	Insufficient technical and organisational measures to ensure information security	2024-09-27
10	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90000000	Insufficient legal basis for data processing	2021-12-31

Figura A2-3. Sanciones más altas por empresas. [31]

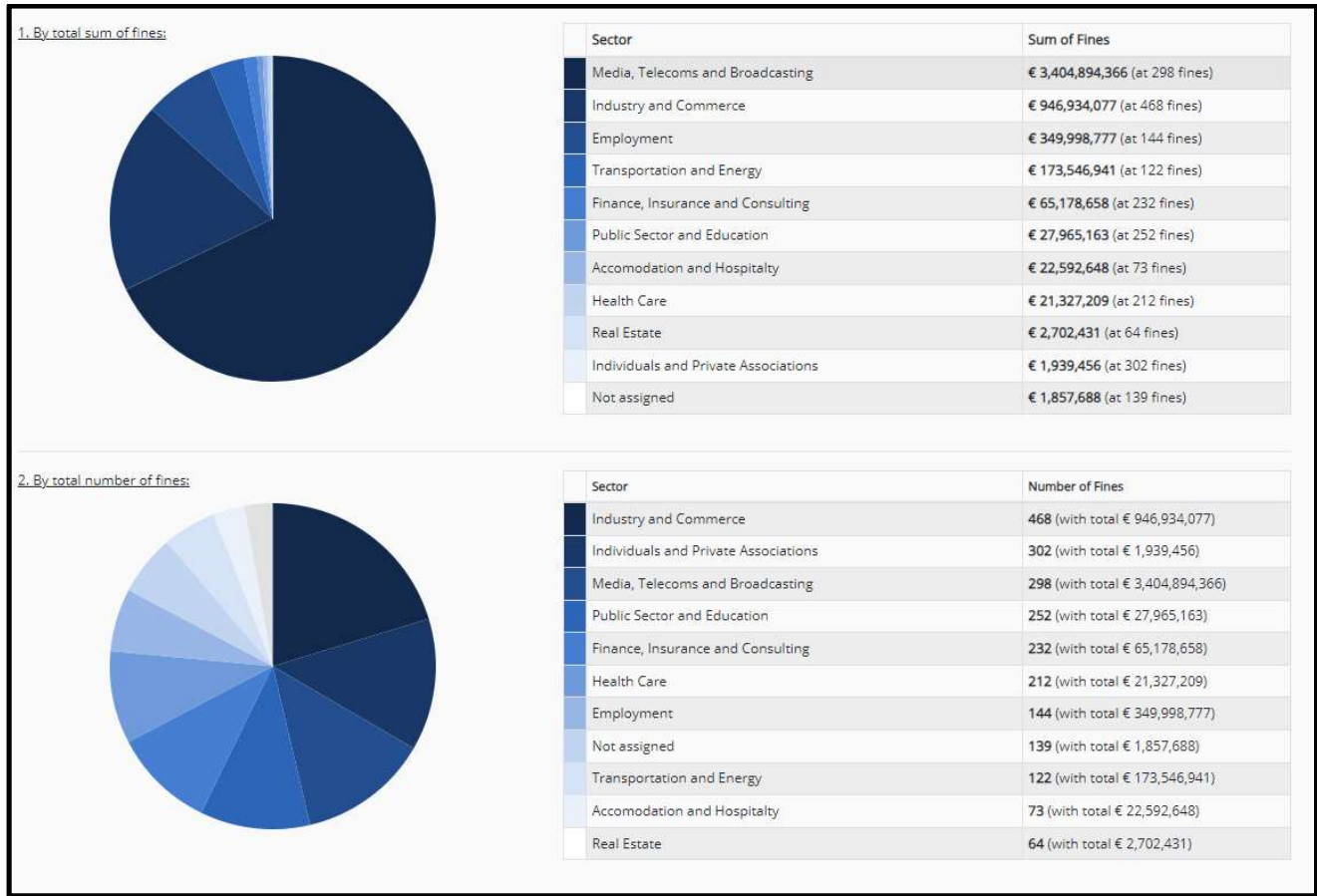


Figura A2-4. Sanciones más altas por sectores. [31]



Figura A2-5. Sanciones más altas por tipo de violación. [31]