PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

¿Propiedad o titularidad de los datos no personales en el uso de sistemas de Inteligencia Artificial de las Cosas (AIoT)?: Propuestas para una regulación especializada a partir de la experiencia de empresas B2B en el sector minero.

Tesis para obtener el Título Profesional de Abogada presentada por:

Villavicencio Kcomt Adriana Consuelo

Asesor

Cairampoma Arroyo Vicente Alberto

Lima, 2025

Informe de Similitud

Yo, **Vicente Alberto Cairampoma Arroyo,** docente de la **Facultad de Derecho** de la Pontificia Universidad Católica del Perú, asesor de la tesis titulada:

¿Propiedad o titularidad de los datos no personales en el uso de sistemas de Inteligencia Artificial de las Cosas (AIoT)?: Propuestas para una regulación especializada a partir de la experiencia de empresas B2B en el sector minero.

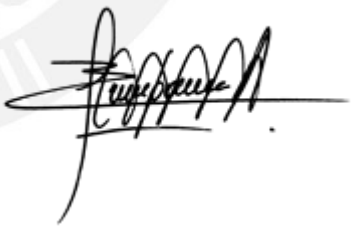
De la autora:

Adriana Consuelo Villavicencio Kcomt

Dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 12%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el **01/12/2025**.
- He revisado con detalle dicho reporte y confirmo que cada una de las coincidencias detectadas no constituyen plagio alguno.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima, 20 de octubre del 2025.

<table>
<tr><td colspan="2">Apellidos y nombres del asesor / de la asesora:
CAIRAMPOMA ARROYO, VICENTE ALBERTO</td></tr>
<tr><td>DNI:
40139896</td><td rowspan="2"> 
Firma:</td></tr>
<tr><td>ORCID:
https://orcid.org/0000-0002-9706-4910</td></tr>
</table>

"No cabe duda de que la llegada de la inteligencia artificial representa una verdadera revolución cognitivo-industrial, que contribuirá a la creación de un nuevo sistema social caracterizado por complejas transformaciones epocales […]. Sin embargo, podría acarrear mayores injusticias entre naciones avanzadas y en desarrollo, o entre clases sociales dominantes y oprimidas, planteando el peligroso riesgo de preferir una cultura del descarte en lugar de una cultura del encuentro."

Discurso sobre Inteligencia Artificial

— **Papa Francisco**

DEDICATORIA

Dedico este trabajo a mis tres grandes pilares en mi vida: *A mi abuela, Consuelo Li*, cuyo amor puro y entregado hizo de mi infancia un lugar seguro, lleno de curiosidad y grandes sueños. Su ternura me acompaña cada día y sigue sosteniéndome en cada paso que doy. *A mi madre, Betty*, ejemplo de fortaleza, disciplina y resiliencia. Su historia de vida y su infinito amor hacia mí, su única hija, me enseñó a no rendirme, a levantarme siempre, a luchar por mis sueños y a caminar con dignidad hacia mis metas. Este logro es una ofrenda de gratitud a ti que me has sostenido en cada parte de mi camino. *A mi tía Silvia*, mi inspiración intelectual y el faro de perseverancia que me guía. Su apoyo incondicional y su amistad han sido una fuente de fuerza inmensa en mi vida y en las decisiones del día a día. A ustedes tres, les debo lo que soy y lo que sigo construyendo. *A mi abuelo Felipe* por su carisma y su optimismo, su motivación y su presencia paternal a lo largo de mi vida, gracias por ser un padre y un refugio.

A mis grandes amigos y personas favoritas, Fiorella, Camila, Laura, Vanessa, Danna, Hernán, Kevin y Alonso. Gracias por su apoyo emocional constante, y por cada palabra de aliento que cruzó distancias y abrazó mi proceso. De ustedes aprendo y me nutro cada día. Llevo sus gestos de amor y compañía como una parte indeleble de este logro.

AGRADECIMIENTOS

Este trabajo no ha sido solamente un esfuerzo académico, sino profundamente personal y espiritual. Esta tesis es el reflejo de un recorrido que no podría haber transitado sola. Agradezco eternamente a mi asesor, Alberto Cairampoma, quien con paciencia y sabiduría, hizo del proceso un camino ameno, llevadero y sostenible. Su metodología, su mirada crítica, profunda y su apertura a los nuevos retos que plantea las nuevas tecnologías contribuyeron enormemente en el desarrollo de mi tesis. Agradezco por sus palabras de motivación, la transmisión constante de seguridad que fueron necesarias para mantener mi actitud positiva constante, mi espíritu innovador y plasmarlo en el trabajo. No habría podido elegir mejor persona para acompañarme en este proceso.

Expresar un especial agradecimiento a Óscar Montezuma, Lester Villar, Lorena Macedo, Abel Revoredo y Piero Malca, quienes generosamente me otorgaron tiempo para enriquecer y contribuir a esta tesis. Su tiempo, sus perspectivas y su experiencia fueron esenciales para profundizar mi análisis y dar mayor solidez a este trabajo.

RESUMEN

La presente tesis analiza el tratamiento jurídico de los datos no personales generados en entornos industriales, con especial énfasis en el sector minero peruano. A partir de la expansión de tecnologías como la Inteligencia Artificial de las Cosas (AIoT), los datos no personales han adquirido un valor estratégico para la innovación y la competitividad. Sin embargo, en Perú su regulación es incipiente, lo que limita su aprovechamiento como motor de desarrollo económico. El estudio plantea como cuestión central determinar si el marco legal vigente resulta suficiente para regular el acceso, uso y compartición de estos datos, o si se requiere construir un régimen jurídico especializado. Mediante una metodología cualitativa, de carácter descriptivo y analítico, se realiza un análisis de fuentes doctrinarias, normativas y de experiencias comparadas como el marco legal europeo, chino y estadounidense. La investigación concluye en la necesidad de diseñar un marco regulatorio especializado y sectorial que equilibre la promoción de mercados competitivos de datos y la innovación tecnológica, con atribución de titularidad de derecho bajo la lógica de los comunes digitales.

Palabras clave: datos no personales – propiedad de los datos no personales – inteligencia artificial – mercado de datos – datos industriales – datos comunes digitales.

ABSTRACT

This thesis examines the legal treatment of non-personal data generated in industrial environments, with a particular focus on the Peruvian mining sector. With the expansion of technologies such as the Artificial Intelligence of Things (AIoT), non-personal data has gained strategic value for innovation and competitiveness. However, in Peru its regulation remains incipient, limiting its potential as a driver of economic development. The central question of this study is whether the current legal framework is sufficient to regulate access, use, and sharing of such data, or whether it is necessary to construct a specialized legal regime. Through a qualitative, descriptive, and analytical methodology, the research analyzes doctrinal sources, national regulations, and comparative experiences from the European, Chinese, and U.S. legal frameworks. The study concludes that it is essential to design a specialized and sectorial regulatory framework that balances the promotion of competitive data markets and technological innovation by establishing a right holder's framework under the concept of digital commons.

Keywords: *non personal data – data property – artificial intelligence – data markets – non personal data Flow – industrial data*

ÍNDICE

INTRODUCCIÓN

En el contexto actual de digitalización e inteligencia artificial, los datos representan activos estratégicos y de gran valor comercial para diversos sectores económicos. Su aprovechamiento fomenta la transformación de negocios e industrias, impulsando el uso de nuevas tecnologías en su proceso productivo, más eficientes y productivas, que permitan maximizar beneficios y optimizar recursos a través de la automatización de procesos y la toma de decisiones basada en datos.

La expansión del uso de tecnologías emergentes como la inteligencia artificial de las Cosas (AIoT) y la apuesta por las industrias en su implementación, se consolida como un cambio de paradigma sobre los procesos industriales tradicionales, permitiendo procesar y analizar datos masivos, a tal velocidad y precisión, que hace eficiente la producción de información altamente relevante para los procesos de producción y en tiempo real.

Los datos generados en el uso de tecnologías como el AIoT aplicado a industrias hace posible el monitoreo de las operaciones, la predicción de riesgos y detección de patrones para la toma de decisiones casi inmediatas. Esto contribuye en los índices de productividad, utilizando menos recursos y empleando menos tiempo. En el AIoT, el uso de Big Data para la recopilación de datos es indispensable, por lo que el uso de los datos no personales representan un activo crucial para los procesos industriales en tanto son la fuente del diseño, innovación, entrenamiento y de funcionamiento de estos sistemas. Es simple: sin datos, no existen sistemas de AIoT.

Su valor estructural y operativo es significativo y, al ser reutilizables, preservan su calidad incluso ante su uso simultáneo. Dichas características crean condiciones necesarias para ser objetos de aprovechamiento, lo cual favorece el crecimiento de diversos sectores económicos y productivos como el minero. Sin embargo, la recopilación de datos y su tratamiento implica una serie de riesgos tales como: la monopolización de los datos, la diferencia difusa en el tratamiento de los datos personales y no personales, y las limitaciones técnicas y operacionales en su compartición.

A diferencia de los datos personales, su procesamiento no compromete directamente derechos fundamentales como la autodeterminación informativa o privacidad. Sin embargo, al no aplicarse un tratamiento diferenciado, surge la inquietud sobre si los datos no personales son pasibles de apropiación y puede ejercerse sobre estos atributos de la propiedad. En el ámbito privado, donde rigen las reglas del mercado y acuerdos contractuales perpetúan relaciones asimétricas, esta

cuestión suele abordarse de manera poco uniforme, dejando indisponible el acceso a los datos y creando barreras a la innovación.

Sin un tratamiento adecuado sobre la accesibilidad de los datos, se pone en riesgo la innovación tecnológica, disminuyendo la competitividad de los mercados tecnológicos y propiciando distorsiones a la libre competencia. Esto se deriva del uso concentrado de datos y un sistema que favorece a las grandes plataformas. El uso y acceso a los datos industriales generados en el uso de sistemas AIoT, desde una perspectiva jurídica, aún es incipiente en Perú, en donde no existe una regulación específica que permita su aprovechamiento desde la perspectiva del acceso para el fomento de la innovación y la competitividad del sector tecnológico.

Para ello, es pertinente identificar la naturaleza jurídica de los datos no personales a fin de establecer si es necesario asignar titularidad de derechos específicos o derechos de propiedad, a fin de promover su explotación en condiciones de igualdad y en pro de la innovación tecnológica. Lo mencionado establece un marco normativo que se desprenda de los regímenes de propiedad exclusiva y que garantice una adecuada gobernanza bajo la noción de comunes digitales.

La presente tesis aborda la problemática jurídica alrededor de la atribución de propiedad o titularidad sobre los datos no personales a partir de la experiencia en el sector minero peruano, el cual ha impulsado la modernización de sus procesos industriales y depende cada vez más de los datos generados por dispositivos conectados a internet (IoT).

En base a este cuestionamiento, el objetivo principal de la investigación es determinar si el marco legal peruano y la regulación sobre la propiedad, en el sentido público y privado vigente, resulta adecuada para regular el acceso, uso y compartición de los datos no personales en condiciones justas o si es necesaria la construcción de un régimen jurídico especializado que atienda a su naturaleza jurídica especial en el marco del concepto de los comunes digitales.

Asimismo, se analizan los regímenes jurídicos específicos de los derechos reales, la propiedad intelectual y protección de datos personales a fin de determinar la naturaleza jurídica del dato no personal y, finalmente, revisar regulación comparada sobre la materia a fin de rescatar los aspectos jurídicos más relevantes en la construcción de una regulación nacional que fomente el crecimiento en el mercado digital de los datos e innovación tecnológica en condiciones de igualdad.

La investigación sigue una metodología cualitativa, de carácter descriptivo y analítico, basada en el estudio de doctrina, normativa nacional e internacional, y en el análisis comparado de experiencias relevantes como el Reglamento de Datos (Data Act) de la Unión Europea y el sistema de derechos de propiedad sobre datos en China.

El presente trabajo se estructura en tres capítulos: el primero explora conceptos fundamentales alrededor de los datos no personales en el uso de tecnologías AIoT. El segundo analiza la importancia jurídica de los datos en entornos industriales, especialmente el minero, y los desafíos de su tratamiento como objetos de tutela en el contexto de la innovación tecnológica. El tercer capítulo desarrolla un análisis comparado de los modelos regulatorios actuales de la Unión Europea, China y Estados Unidos, identificando sus convergencias y divergencias, a fin de determinar lineamientos regulatorios aplicables al Perú, teniendo en cuenta las limitaciones y la necesidad de impulsar un ecosistema de datos que favorezca la competitividad, la innovación y la mejora en la calidad de vida de los ciudadanos.

CAPÍTULO I: LA APROPIACIÓN DE LOS DATOS NO PERSONALES EN EL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL DE LAS COSAS (AIoT)

En este primer capítulo, se presentarán los conceptos más importantes relacionados a los datos no personales, su rol en el uso en los sistemas de Inteligencia Artificial y el Internet de las Cosas (AIoT), y las cuestiones más relevantes alrededor de la atribución de propiedad sobre estos junto con los efectos que generan en el entorno económico digital. Además, se analiza la importancia que poseen estos sistemas al constituirse como fuentes principales de recolección de datos, los tipos de datos que se procesan, los actores que intervienen en estas nuevas interacciones del entorno industrial-digital, cuáles son los intereses que giran alrededor de los datos no personales aplicables a la industria minera y cómo se ha abordado la materia respecto a la atribución de propiedad a nivel nacional e internacional.

1. Definición del AIoT

Para definir la Inteligencia Artificial de las Cosas (por sus siglas en inglés, “AIoT”), es necesario entender, en primer lugar, que se trata de un concepto evolutivo y que surge de la incorporación de los sistemas de Inteligencia Artificial (IA) al Internet de las Cosas (IoT). En este sentido, resulta fundamental abordar los conceptos relacionados con estas tecnologías emergentes y analizar sus principales características y aplicaciones.

1.1. ¿Qué es el Internet de las Cosas (IoT)?

El internet de las cosas (IoT) es definido por Floris & Atzori (2015) como “*una red de objetos interconectados que son capaces de captar información del mundo físico y que hacen de esta información accesible o disponible en Internet*” (p.1747). De manera similar, el NIST (*National Institute of Standard and Technology* – USA), un referente mundial en tecnología, lo define como un conjunto sistemas y componentes que funcionan para proporcionar una funcionalidad específica. Estos se dividen en productos y dispositivos IoT. Los primeros suelen conectarse a equipos físicos, mientras que los segundos se distinguen por contar, al menos, con un sensor y una interfaz de red, que actúa como un punto de conexión entre dos o más partes del equipo (Boeckl et al., 2021).

Pallavi y Sarangi (2017, citado en Molaei et al., 2020) indican que el IoT es una combinación de tecnologías integradas que incluyen sensores conectados, receptores, dispositivos de accionamiento, también conocidos como controladores eléctricos, y otros artículos físicos conectados a internet, que se comunican a través de redes para lograr un objetivo común. Es decir, el IoT es un conjunto de dispositivos que, al estar conectados a internet, capturan datos del ambiente que procesan en la nube a partir de su conexión en la red y emiten algún tipo de acción.

El término “IoT” fue acuñado por primera vez en 1999 por Kevin Ashton, quien en ese entonces era director de *Auto-ID Labs* del MIT. Ashton presentó una propuesta a *Procter & Gamble* para utilizar máquinas capaces de capturar información del mundo real con mayor precisión, determinando el estado de las cosas en tiempo real, reduciendo tiempos de espera y utilizando menos recursos. No obstante, el uso práctico del término se remonta a los años 80, cuando estudiantes de la Carnegie Mellon University construyeron un dispositivo que monitorea las máquinas dispensadoras de botellas de Coca-Cola. Este aparato, conectado a internet, permitía controlar la disponibilidad de las bebidas y su temperatura antes de realizar el viaje para comprarlas (Foote, 2022).

El modelo de Ashton sobre el IoT se basaba principalmente en el uso de Identificación por Radiofrecuencia (RFID), un elemento indispensable para las soluciones de rastreo de inventarios, que permite identificar múltiples objetos simultáneamente, generando así una gestión y rastreo más eficiente. Estos dispositivos fueron adoptados, por ejemplo, por Walmart y el Departamento de Defensa de los Estados Unidos durante los años 2000 (Foote, 2022). Ese mismo año, LG aparece en el mercado con un refrigerador inteligente, en el 2007 se lanza el primer iPhone y para el 2009, se empezó con los pilotos de autos sin conductores (Marchant, 2021).

El uso del IoT en la actualidad forma parte de nuestra vida, aunque aún no lo hayamos interiorizado. Desde sus formas más básicas y simples, como sistemas de alertas o asistentes virtuales, hasta sus formas más complejas en aplicaciones industriales como drones que detectan calor o monitorean cultivos en grandes áreas, dispositivos médicos que miden el estado de salud de los pacientes, vehículos autónomos, redes eléctricas inteligentes que gestionan la generación y distribución de energía de manera eficiente, sistemas de gestión de flotas, y un sinfín de aplicaciones en diversas industrias.

Según Floris & Atzori (2015), la evolución del IoT no siempre fue como la conocemos hoy, sino que ha atravesado por diferentes cambios que caracterizan 3 generaciones. La primera se basó en el uso de Identificadores por Radiofrecuencia (*RFID*) para el rastreo de aplicaciones y logística. Luego, en la segunda generación, se incorporan sensores y activadores en redes inalámbricas (*Wireless Sensor Networks*) que captan estados o características del mundo real, como los sensores que miden los niveles de contaminación del aire.

Finalmente, la tercera generación introduce los Objetos Virtuales (*Virtual Objects*, VO) que vinculan el elemento físico del mundo real con la parte digital para dotarlos de inteligencia y permitiendo almacenar información y la comunicación a través de la nube (p.1747). Algunos ejemplos son Amazon Echo o Google Nest, que han evolucionado a través de estas generaciones, utilizando dispositivos que aprenden hábitos de los usuarios y optimizan el consumo a través de los datos, permitiendo reducir o usar de manera eficiente el consumo de electricidad.

Para los fines prácticos del presente trabajo, el IoT es un dispositivo tecnológico que está integrado por diferentes dispositivos que, al operar de manera conjunta, son capaces de desplegar diferentes funcionalidades a partir de las cuales se recopilan datos. Pensemos en un reloj inteligente como un dispositivo IoT, este suele tener sensores para poder medir el ritmo cardiaco y suelen conectarse a internet. El producto IoT es el reloj en sí mismo, más la aplicación en el teléfono que muestra una estadística sobre el pulso. El reloj envía datos a un teléfono, este envía los datos a un servidor en la nube y los analiza.

En ese sentido, al ser un concepto que engloba una red de componentes interconectados que intercambian datos e interactúan entre sí, se compone principalmente de 4 capas. Según el artículo "*Unpacking IoT Architecture: Layers and Components Explained*", estas capas son: 1) detección o percepción, 2) red o conectividad, 3) procesamiento de data y 4) interfaz del usuario o aplicativo. Esta estructura permite la interconexión, almacenar la información en servicios de la nube y protocolos que dan lugar a un ecosistema con sensores y/o activadores, permiten que lleve la información, viaje hacia la nube desde una fuente física, a través de redes, con el objetivo de gestionar, almacenarla, analizarla y/o procesarla, para ejecutar una tarea designada (*Device Authority*, s/f).

La primera capa, de detección o percepción, es la columna vertebral del ecosistema IoT. En ella, se genera la data de entrada o *input*, y utilizando sensores o actuadores, se capta información

de los equipos físicos o del ambiente. Imaginemos en una fábrica de autos, se colocan estos sensores o cámaras para poder verificar que se están ensamblando de manera correcta o si se cumplen con las condiciones de seguridad necesaria.

La segunda capa, de red o conectividad, permite la transmisión de datos de un dispositivo a otro dentro de toda la estructura del IoT. Comúnmente, se utilizan técnicas de comunicación que permiten solicitar información a los sensores, manejar grandes cantidades de datos y establecer comunicación directa entre dispositivos. Algunas de estas técnicas son HTTP, MQTT y AMQP, cada una con ventajas y aplicaciones diversas.

La tercera capa está compuesta por el procesamiento de los datos recopilados y su posterior análisis. Esta tiene como objetivo generar información de valor para el negocio y permita tomar decisiones informadas. En esta, los datos pueden encontrarse almacenados, ordenados o estructurados en su forma cruda o en bruto, lo que posibilita la creación de reportes y otros tipos de información relevante. Además, se pueden aplicar tecnologías de inteligencia artificial (IA) para procesar los datos utilizando modelos como *machine learning*, aportando valor agregado y automatización.

Finalmente, la cuarta capa, de la interfaz, es aquella que conecta el ecosistema IoT con el usuario final. Es decir, una persona que puede interactuar con el sistema y recibir la información en un formato accesible. Usualmente, se desarrollan dispositivos similares a una tableta que permiten al usuario controlar tareas específicas o visualizar información puntual sobre determinados aspectos.

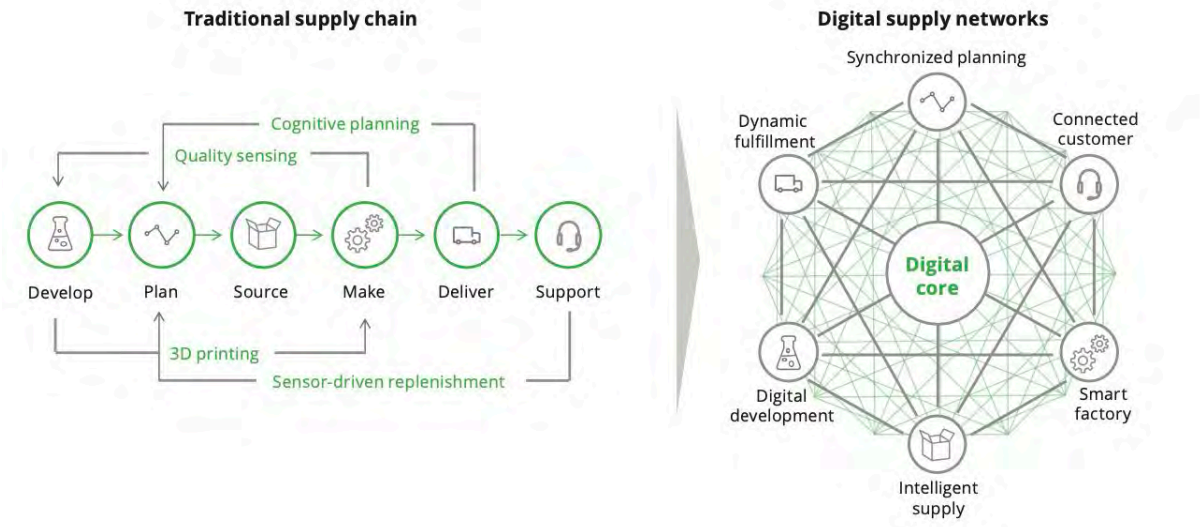
Existen, además, otras capas complementarias, como el *Edge Computing*, que descentraliza los datos y los almacena más cerca de su origen, con el objetivo de obtener tiempos de respuesta más cortos y rápidos. Finalmente, no podemos olvidar la capa de seguridad, que resulta indispensable para cuidar la privacidad de las operaciones y proteger los dispositivos, las conexiones y los datos.

En la aplicación práctica del IoT en el ámbito económico, se incluye el uso de inteligencia artificial para apoyar los procesos relacionado a las operaciones industriales en general. Esto permite maximizar el aprovechamiento de los activos de la empresa y la capacidad del personal, con el fin de optimizar procesos, maximizar beneficios, utilizar eficientemente los recursos y realizar las actividades con mayor seguridad y precisión.

Un artículo de *Deloitte Insights* sobre la industria 4.0 afirma que esta etapa es crucial, ya que no solo impacta la manera en que los fabricantes producen, sino también a la sociedad en general. Al constituirse como la columna vertebral de las industrias, contribuye a la transformación hacia una producción y logística autónomas, mejora la experiencia del usuario o consumidor, y, sobre todo, impulsa cambios en la fuerza laboral, ya que se requieren nuevas capacidades y roles para asumir esta transición (s/f).

En el contexto de esta nueva forma de operar comercialmente, producto de la automatización y digitalización, la industria 4.0 adopta tecnologías de IoT que funcionan en tiempo real, operan con total interconectividad entre dispositivos y rompen los esquemas tradicionales, como la cadena de suministro lineal con la que operan los negocios convencionales, tal como se puede observar a continuación (Figura 1).

Figura 1: Diferencia entre la cadena de suministro linear y una red de suministro digital



Nota*:* Adaptado de *"The Rise of Digital Supply Chain Network" (p.6), por Deloitte University Press, 2016*.

Ahora bien, esta interconectividad que caracteriza al IoT lo convierte en un sistema y/o producto totalmente adaptable, tanto en su estructura de hardware (aspecto físico del dispositivo) como en la estructura del software (aspecto de funcionamiento lógico). Por ello, la personalización de estos sistemas para un proceso específico dentro de una industria genera valor a partir de los datos recopilados por el aspecto físico, los cuales se transforman en información comercial o industrial relevante que permite tomar decisiones para optimizar o hacer más eficientes los procesos.

En ese sentido, el IoT añade valor a las industrias porque les permite transformar sus procesos productivos, reducir riesgos y tomar decisiones más informadas con la disponibilidad de datos y su análisis en tiempo real. En el caso particular del sector minero, el IoT permite automatizar tareas peligrosas que podrían mejorar la seguridad de los trabajadores y optimizar el uso de los activos. En consecuencia, no solo favorece en la reducción de costos operativos en las industrias, sino que se producen modelos que cambian la forma en cómo opera la industria.

1.2. Definición de la Inteligencia Artificial (IA)

La inteligencia artificial (IA) está generando un gran impacto en la sociedad y en la forma en cómo vivimos e interactuamos. Sin embargo, dado que su uso conlleva a una serie de riesgos, deben asumidos con ética y responsabilidad. A fin de disfrutar de sus beneficios sin que ello constituya un riesgo para la industria tecnológica, es indispensable conocer sus características, beneficios y ventajas de aplicación.

El concepto de la IA no se ha uniformizado hasta la fecha y se mantiene como un desafío adoptar una sola definición. No obstante, a partir de los lineamientos establecidos por la Organización para la Cooperación y el Desarrollo Económico (OECD) se toma como referencia la siguiente definición:

> *"Un sistema de IA es un sistema basado en máquinas que, para lograr un objetivo sea implícito o explícito, infiere a partir de los datos de entrada que recibe, generando un dato de salida en forma de predicción, contenido, recomendación o decisión que puede influenciar ambientes físicos o virtuales. Son diferentes sistemas de IA que varían dependiendo del nivel de autonomía, adaptación y despliegue" (OECD, 2024).*

Los esfuerzos por definir la IA para incorporarla como definición normativa han sido liderados por la Unión Europea (UE) que, a través de la Ley de Inteligencia Artificial, introducen la siguiente definición:

> *"Un sistema de IA es un sistema basado en máquinas que es diseñado para operar con diferentes niveles de autonomía y que puede mostrar adaptabilidad después del despliegue y que, para objetivos implícitos o explícitos, puede inferir, a partir de la entrada que recibe, cómo generar resultados sea con predicciones, contenido, recomendaciones*

decisiones que puedan influir en los entornos físicos o virtuales". (Reglamento (UE) 2024/1689).

Como se puede apreciar, la Unión Europea ha tomado como referencia la definición desarrollada por la OECD, permitiendo una articulación normativa interinstitucional y generando uniformidad en la aplicación de conceptos. Esto se debe a que los sistemas de IA, en un contexto globalizado, trascienden el factor territorial y la nacionalidad del implementador, haciendo necesaria la estandarización de conceptos que permitan identificarlos independientemente de los avances tecnológicos y del país en el que se desarrolla. El objetivo es establecer reglas específicas que garanticen el ejercicio delos derechos y el establecimiento de obligaciones en su uso.

La inteligencia artificial es una tecnología, parte del campo de las ciencias informáticas y de datos, que permite que las computadoras simulen la inteligencia humana y sus capacidades para llevar a cabo una tarea o resuelvan problemas. (IBM, s/f). Estas tareas incluyen actividades humanascomo como el aprendizaje, el razonamiento, el reconocimiento de patrones y el procesamiento del lenguaje. Estos sistemas utilizan técnicas avanzadas como el aprendizaje automatizado (o *machine learning*), el aprendizaje profundo (o *deep learning*) y las redes neuronales para analizar datos, tomar decisiones y adaptarse a diferentes situaciones o tareas.

En la vida cotidiana, las personas han implementado asistentes virtuales como Siri o Alexa, que emplean IA para responder preguntas de forma natural, realizar tareas o ejecutar acciones y ofrecer recomendaciones. Otras plataformas muy conocidas como Netflix y Spotify usan IA dentro de sus procesos para ofrecer contenido basado en los gustos del usuario.

En las industrias, la IA se emplea para monitorear procesos, identificar defectos en los productos y optimizar las operaciones. En el sector minero, por ejemplo, la IA se combina con el IoT, permitiendo monitorear el rendimiento de las máquinas, optimizar el consumo de energía y mejorar la seguridad anticipando riesgos en entornos altamente peligrosos. Otras aplicaciones incluyen el diagnóstico en agricultura, mediante el análisis de datos climáticos, o en salud, a través de la interpretación de imágenes médicas.

En general, la IA ofrece múltiples beneficios, como automatizar tareas, reducen costos y tiempos para ejecutar una tarea, y mejoran el nivel de precisión de las actividades. También permite optimizar recursos, como el agua o la energía, en diversas industrias. La IA implementada en

entornos productivos facilita la toma de decisiones más inteligentes, al proporcionar información y datos procesados.

La integración de sistemas de IA en las industrias productivas ha crecido significativamente debido a sus capacidades únicas y los beneficios que se potencian al combinarla con el Internet de las Cosas (IoT). La IA emplea herramientas avanzadas que no solo recopilan y procesan grandes volúmenes de datos a alta velocidad, sino que también mejoran su rendimiento con el tiempo gracias a su capacidad de aprendizaje y predictibilidad.

Por su parte, el IoT aporta la capacidad de recopilar datos en tiempo real con gran precisión, sirviendo como una fuente esencial para que los sistemas de IA operen de manera efectiva. La combinación de ambas tecnologías transforma los datos obtenidos del entorno en información de gran valor y notable impacto, convirtiéndose en una herramienta clave para la transición digital de las industrias, optimizando la resolución de tareas y mejorando la eficiencia operativa.

La unión de estas tecnologías ha dado lugar al término Inteligencia Artificial de las Cosas o, por sus siglas en inglés, “AIoT” (*Artificial Intelligence of Things*). Este concepto combina las capacidades del IoT y la IA para mejorar las operaciones industriales como parte de la revolución de la Industria 4.0. La sinergia es especialmente relevante porque potencia la capacidad de recopilar grandes volúmenes de datos en tiempo real, que viajan a través de redes conectadas a internet y centralizan la información para analizar de forma avanzados para la toma de decisiones automatizadas, generando un impacto significativo en la eficiencia y la creación de valor a un sector en particular.

La inteligencia artificial ocupa un papel crucial en la economía y las industrias, ya que utilizan los resultados del procesamiento de datos para tomar decisiones complejas, ya sea de carácter preventivo o correctivo que aporta en la mejora de ciertos procesos. Tal como lo hemos mencionado, en el sector minero, el AIoT puede ajustar y adaptar sus aplicaciones a cubrir necesidades específicas de dicho sector, de tal forma que aprende de la particularidad de la dinámica minera, de sus procesos, de sus interacciones, sus principales riesgos y a partir de ahí, ofrecer un producto que se adapte mejor a responder requerimientos en base a datos.

Su maleabilidad y gran capacidad adaptativa en un sector y con otros dispositivos, es lo que lo hace un sistema de valor y de alta relevancia para las industrias extractivas. Lo importante es entender que, sin la recopilación de datos, no sería posible la puesta en marcha de estos

sistemas, por ende, es necesario la integración de ambas tecnologías para tener fuentes de obtención de datos y al mismo tiempo, procesamiento de datos automatizado.

1.3. La evolución hacia el AIoT y su importancia en el mundo económico actual

Una de las razones por las que es importante precisar la evolución del IoT hacia el AIoT es evitar la generalización de su aplicación al uso de robots y carros autónomos, dado que el término no se reduce a esos ejemplos. Por otro lado, su valor económico recae en la generación de datos y su procesamiento por parte de los sistemas de IA en el IoT. Esta vaguedad con la que se aborda el uso de la IA dificulta la aplicación de las leyes, debido a la escasa o nula delimitación del ámbito de aplicación respecto de las tecnologías que se usan en relación con la inteligencia artificial y la identificación del tratamiento del dato en un ciclo.

Como se ha advertido, el Internet de las cosas es una tecnología totalmente adaptable a las diferentes aplicaciones o industrias, puede ser en el sector minero, ambientes, médico, transporte, entre otros. Para Awaisi et al. (2024) señala que es un sistema que integra varios dispositivos que integran sensores y permite recopilar enormes cantidades de datos, la inteligencia artificial potencia el valor de estos mediante análisis y procesamiento de datos.

Esta sinergia tecnológica posee una serie de características particulares, flexibles y adaptables, que la legislación debe considerar con el objetivo de implementar una regulación que se ajuste a realidad técnica compleja y cambiante, más allá de los usos. En consecuencia, es importante conocer qué es el AIoT, cómo funciona, qué tipo de datos trata y cuáles son las implicancias en la aplicación de estas en las industrias.

Como se ha visto previamente, la IA es un sistema programable que simula la inteligencia humana, a un alto o bajo nivel, replicando alguna de las características de la inteligencia humana y el proceso de toma de decisiones. En ocasiones se ha hecho referencia a que la IA se asemeja al cerebro de un humano y el IoT al sistema nervioso, de tal forma que interactúan y funcionan de forma conjunta (Mar, citado en Stewart et. al., 2020) creando así una combinación perfecta para captar datos del ambiente y procesarlos de forma articulada.

En el mercado actual, la inteligencia artificial está transformando la economía mundial y la forma en que interactúan con las diferentes industrias. Según un artículo del Bank of America, los

mercados en Estados Unidos y China, catalogados como las economías más grandes de todo el mundo, están experimentando un crecimiento económico considerable debido al desarrollo de la IA. Ambos países representan el 70% del impacto económico global de la IA para el 2030 y generará el crecimiento del PBI en China superior al 26% y en Norteamérica un 14.5% (Israel, 2024).

El AIoT es un concepto emergente que integra diversas tecnologías en constante evolución, en las cuales las máquinas, junto con el Deep Learning (aprendizaje profundo), interactúan con nuevas aplicaciones que funcionan en tiempo real. Según IBM, el Deep Learning se define como un tipo de red neuronal, denominada 'redes neuronales profundas', que simula el complejo proceso de toma de decisiones que realizan los seres humanos. Esta capacidad permite a la inteligencia artificial aprender del comportamiento humano y aplicarlo a diversas tareas asignadas.

El *Machine Learning* (ML), como una herramienta clave del AIoT, es una subcategoría de la inteligencia artificial que ofrece grandes beneficios y mejora la eficiencia de los sistemas. Se centra principalmente en el análisis de datos y la aplicación de algoritmos, lo que le permite aprender de manera similar a los seres humanos, pero con la ventaja de detectar patrones con mayor velocidad y precisión. Además, tiene la capacidad de predecir situaciones y generar recomendaciones que mejoran a medida que el modelo se reentrena.

El Massachussets Institute of Technology (MIT) también define el ML como un subcampo de la inteligencia artificial que busca imitar la inteligencia y el comportamiento humano. Por su parte, Samuel Greengard lo define como "*el uso de modelos matemáticos avanzados, conocidos como algoritmos, para procesar grandes volúmenes de datos y obtener información sin participación humana directa*". Al ser un subtipo de IA, se compone de redes neuronales artificiales que interactúan entre sí, e incluyen Deep Learning (aprendizaje profundo), lo que permite imitar el modo de aprendizaje humano, pero con una diferencia en velocidad, precisión y predictibilidad (Greengard, 2022).

El AIoT incorpora técnicas de *machine learning* como parte esencial de su arquitectura, permitiendo que los dispositivos IoT recopilen datos, procesen, analicen y actúen de forma autónoma en función de patrones identificados. Esta técnica resulta fundamental para extraer valor de los datos, ya que posibilita el aprendizaje continuo de los sistemas y potencia la precisión

de sus resultados, generando predicciones en tiempo real, optimizando el rendimiento a partir de la toma de decisiones en entornos industriales complejos.

Para la Academia de Ciencia de Inglaterra, *The Royal Society*, los sistemas de *machine learning* son una de las creaciones técnicas más sobresalientes y económicamente relevantes de la IA (2017). Estos se aplican en la automatización de procesos de toma de decisiones en sectores claves y de múltiple aplicación como el económico, financiero, laboral, salud pública, función jurisdiccional, etc. Su utilidad se centra en la capacidad de analizar datos, detectar patrones y realizar predicciones, lo que optimiza la toma de decisiones basadas en la información disponible.

A pesar que la IA y sus técnicas, como el *machine learning*, mejoran el rendimiento técnico y funcional del IoT y lo potencian, aún existen diferencias importantes en ambas tecnologías. Este análisis diferenciador permite visualizar el impacto que genera la IA cuando se aplican a los datos y en la medida que se procesan a través de todo un ciclo, el valor de los datos se transforma, haciendo que cada fase de este representa un valor diferenciado para los diferentes agentes del mercado pero que, en general, el objetivo final es que permite tomar decisiones más inteligentes.

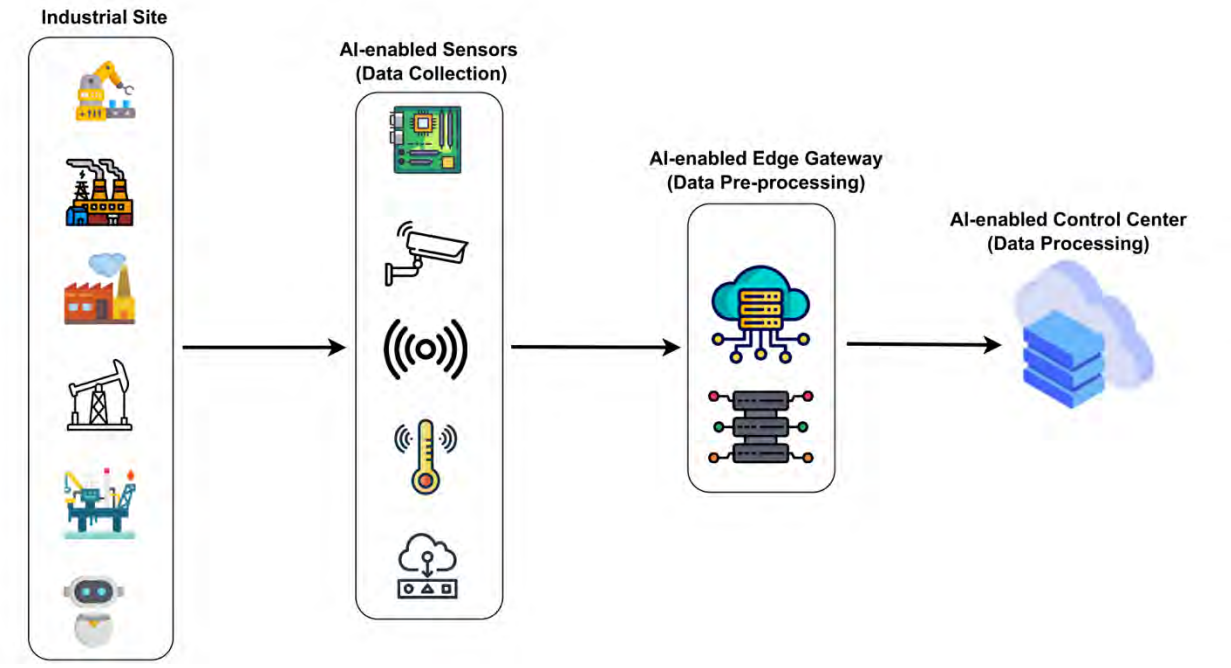
Es crucial abordar el tipo de datos recopilados cuando el AIoT se aplica a una industria específica, por ejemplo, en el sector minero. Identificar el tipo de datos es clave para analizar los posibles riesgos legales asociados con el uso del AIoT en la industria minera. Las interacciones con los datos y la aplicación de una arquitectura específica para cumplir una función determinada requieren conocer la finalidad del tratamiento y qué tipos de datos se van a utilizar.

En la industria minera, las oportunidades para optimizar los procesos con la aplicación de AIoT son diversas. En caso se tenga como objetivo garantizar condiciones de seguridad a los colaboradores y monitorear su actividad en áreas de alto riesgo debido a las condiciones hostiles de las minas, es probable que se recopilen tantos datos personales y/o sensibles y ligado a estos, datos no personales. Por el contrario, si el objetivo es obtener información sobre la salud de los equipos, tuberías o infraestructura, como sus estados y condiciones de temperatura, se recopilarán únicamente datos no personales.

Este avance representa un cambio importante en cómo se tratan los datos dentro de una arquitectura AIoT. Mientras que en un sistema IoT tradicional los datos solo se recopilan y se transmiten, en el AIoT, gracias a la integración de la inteligencia artificial, los datos pasan por

varias etapas de análisis que permiten tomar decisiones más rápidas y precisas. Cada una de estas fases aporta un valor distinto, y es ese cambio lo que permite que el sistema tome decisiones más inteligentes en tiempo real.

Para ser más específicos, a medida que los datos atraviesan las diferentes etapas del ciclo del AIoT (desde su recolección hasta su uso en el centro de control), van cambiando tanto en forma como en valor. Primero, son datos en bruto, tal como los captan los sensores. Luego, al ser organizados y limpiados, se convierten en datos preprocesados. Finalmente, cuando son analizados con IA, se transforman en datos procesados, de donde se extrae la información útil.

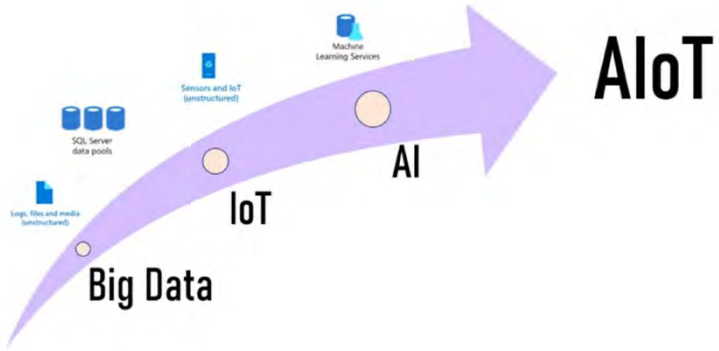


Nota. Adaptado de "*A survey of Industrial AIoT: Opportunities, Challenges, and Directions*" (p. 96948), por (Awaisi et al., 2024), IEEE Access, 12

Otra diferencia importante radica en la necesidad del uso de la nube (*Cloud Computing*) de los dispositivos de IoT para el tratamiento de los datos generados a partir de los sensores. Estos dispositivos dependen de este modelo para acceder a servicios de computación y almacenamiento mediante internet. En cambio, el AIoT permite procesar y analizar cerca de su origen, utilizando servidores o hardware instalado localmente, eliminando la necesidad de usar la nube, reduciendo costos, tiempo, mejora la calidad de la información, la precisión y la automatización de procesos de máquina a máquina (M2M – *Machine to Machine*).

Como se ha explicado, a nivel técnico, el IoT posee ciertas limitaciones como la capacidad de almacenaje, energía y capacidad de procesamiento, a diferencia de la IA, con su desarrollo, ha demostrado ser precisa, predictiva y altamente autónoma. En este contexto, para crear dispositivos más eficientes y mejorar la calidad de los servicios, surge el AIoT, que refuerza la calidad, precisión y el procesamiento de los datos recopilados por los sensores, así como el servicio de comunicación a un nivel superior (Qureshi y Newe, 2024).

En suma, en base a la opinión de Briso-Montiano en un artículo para Medium, el salto del IoT al AIoT se basa en la incorporación de la IA en la dinámica del Internet de las Cosas, donde la interpretación de los datos ya no es realizada por humanos, sino de forma autónoma, manejando la información con eficiencia y optimización. Este proceso se ilustra en la figura siguiente, que muestra la relación causal: el IoT facilita el Big Data, y al disponer de grandes cantidades de datos, permite que la IA se aplique con eficacia, auto-midiéndose, auto-evaluándose y auto-regulándose según las decisiones tomadas a partir de los datos analizados (2024).



Nota: Adaptado de "*IoT, IIoT, AIoT: qué son y en qué se diferencian*" [Gráfico] por Medium (2021). https://lean4-0.medium.com/iot-iiot-aiot-qué-son-y-en-qué-se-diferencian-c688915a33ef

La industria minera, al igual que otras industrias, está evolucionando y transformándose con la implementación de AIoT, por ejemplo, con sistemas que permiten la trituración de materiales de forma remota y en tiempo real o la gestión de flota de carguío a través de geolocalización o telemetría, que con su uso cada vez más frecuente, y el desarrollo de la industria automotriz, se prevé el uso de flota minera 100% autónoma.

Una encuesta realizada por *Global Data* revela que, en el 2023, el índice de adopción de tecnología en el sector minero a nivel mundial se estima en un 50% de minas encuestadas han implementado algún tipo de software para la planificación y gestión de la mina, un 19% ha implementado mantenimiento predictivo para sus equipos y el 23% ha implementado un mantenimiento predictivo para la planta (Zvarivadza et al., 2024).

Un informe de Deloitte señala que adoptar un enfoque proactivo en el mantenimiento, en lugar de reaccionar solo cuando los equipos mineros presentan fallas, generaría ahorros significativos. En la industria minera, el mantenimiento predictivo podría reducir el tiempo de planificación entre un 20% y 50%, y los costos generales, en un 5% a 10%. Tal es el caso de Votorantim Cimentos la fábrica de cementos más larga de Brasil logró evitar $5.5 millones en costos mantenimiento correctivo después de introducir mantenimiento predictivo, la cual no solo logró reducir los costos de reducción sino también a mejorar la fiabilidad operativa (NS Energy, 2022).

La información con valor agregado hace más productivo el sector, genera mercados más competitivos y una constante disputa por ofertar mejores servicios y productos por parte de los proveedores tecnológicos. No obstante, la implementación de estas tecnologías genera una serie de cuestionamientos sobre de quién es la propiedad de los datos recopilados y la información adquirida a partir de su procesamiento. La ausencia de regulación aplicable a estas nuevas relaciones, derivadas de la adopción de tecnologías como lo es el AIoT, puede generar incertidumbre respecto a esta situación.

En consecuencia, en el contexto del sector minero, dado que la implementación de las tecnologías de AIoT es una realidad inevitable, es importante que, en el proceso de transformación a la industria 5.0, se garantice bajo una correcta identificación riesgos, la interacción entre los agentes en el mercado, la adaptación a procesos mineros o de otras industrias y la relación con tecnologías emergentes, nuevos proveedores y competencia.

2. El AIoT en el sector minero

En la actualidad, el AIoT se ha consolidado como una herramienta clave en múltiples industrias debido a su capacidad de adaptación, flexibilidad operativa y los beneficios sustanciales que aporta en términos de eficiencia y competitividad. Su aplicación se ha extendido incluso a sectores altamente estratégicos para la economía nacional, lo que resalta la necesidad de

analizar su implementación en contextos específicos. En este contexto, resulta prioritario estudiar su incorporación en el ámbito minero, no solo por el impacto que puede generar en la transformación tecnológica del sector, sino también por las oportunidades y ventajas económicas que produce al optimizar procesos, mejorar la seguridad y fortalecer la sostenibilidad de las operaciones.

2.1. El modelo *Business to Business* (B2B) para la implementación de AIoT en minería

La implementación de sistemas AIoT en el ámbito minero se desarrolla, predominantemente, bajo el modelo de negocio conocido como B2B (*business to business*). Este modelo se caracteriza por proveer de soluciones o servicios tecnológicos diseñados específicamente para satisfacer las necesidades propias de la empresa en una industria. Es así como diversas compañías tecnológicas han orientado sus desarrollos hacia la creación de servicios personalizados para grandes corporaciones, tales como DHL, Volvo y otras, que integran estas tecnologías a fin de optimizar sus procesos de gestión de la cadena de suministro y de logística, aprovechando la transparencia y rentabilidad (Legchekov, 2022).

Los negocios B2B que desarrollan productos o servicios de tecnología para minería enfocan sus soluciones en diversas áreas del negocio minero, que incluyen diferentes etapas y procesos, tales como exploración, perforación, minado, extracción, procesamiento de minerales, entre otros. En el diseño de la mina, por ejemplo, se desarrollan explosivos que se posiciona mediante dispositivos automatizados y de forma remota a través de robots, esto busca evitar disponer de personal para el posicionamiento del material explosivo. Además, la optimización de las operaciones, se han implementado sistemas de gestión de flota y de materiales, monitoreo para la seguridad de los trabajadores, mantenimiento, entre otras (The Open Group, 2014).

Como ya se ha precisado, el AIoT cuenta con una estructura muy particular que permite la interconexión de diversos dispositivos a través de Internet siguiendo una arquitectura específica que marca el ciclo de sus funciones, las cuales son adaptables a la diversidad de procesos dentro de la mina. Esta estructura adaptable reduce los tiempos y emplear tareas innecesarias en los procesos operativos tradicionales y además contribuye significativamente mejorar el rendimiento con el uso de menos recursos, implicando menos costos y con mayor precisión.

El modelo B2B resulta interesante en el desarrollo e implementación de tecnologías que se adaptan a un sector específico, pues modelan tanto el producto como el servicio a las necesidades concretas de una industria. En este contexto, la empresa tecnológica aprende de las particularidades operativas del negocio demandante para diseñar soluciones que promuevan su digitalización y automatización. A su vez, el negocio demandante ajusta sus procesos para integrar eficazmente la tecnología ofrecida. En consecuencia, la gestión de las relaciones entre empresas de esta naturaleza implica que ambas partes generen valor en sus interacciones, tanto en el intercambio de información como en la planificación colaborativa y la estrategia (Berenguer-Contri et al., 2021, citado en AlHussan et al., 2021).

Esta situación adquiere especial relevancia al momento de regular la relación jurídica contractual debido a que no es posible crear reglas que protejan intereses contrapuestos dado que el valor que se crea a partir de los modelos B2B se genera en conjunto. Esto implica que, al existir una co-creación de valor en el intercambio de los datos, el proveedor tecnológico aporta capacidades técnicas y el negocio minero contribuye a modelar el conocimiento específico del negocio, de esta manera se crean condiciones para idealmente favorecer contractualmente a ambos a fin de maximizar los beneficios del nuevo conocimiento generado en conjunto.

Esta relación “co-creadora”, en particular bajo la aplicación en minería, implica la implementación de sensores en distintos procesos mineros (denominado también proceso de “sensorización” de la mina), lo cual hace posible la recolección de datos provenientes de diversas fuentes distribuidas en el espacio minero y a lo largo de la actividad de la mina y sus activos. Esta información es almacenada, organizada sistemáticamente y, posteriormente, procesada, dando lugar a información valiosa y útil que se usa como fuente para tomar decisiones de manera informada y gestionar integra y eficientemente las operaciones mineras.

Como señala Valero (2022), es necesario que este tipo de entorno colaborativo se defina desde el diseño, puesto que el rol que desempeña o la actividad que realiza cada parte en la creación o implementación de sistemas de AIoT en los activos mineros define los derechos y obligaciones respecto la contribución que cada parte realiza, la disposición de los datos y la accesibilidad a estos en términos de interoperabilidad (p.98).

La implementación de tecnologías AIoT en los procesos mineros, transforma la dinámica operativa tradicional del sector y también redefine la dinámica de interacción entre los diferentes actores involucrados, particularmente respecto de la recolección, procesamiento y uso de los datos industriales. Este proceso comprende una fase de diagnóstico y análisis por parte del proveedor tecnológico, dado que examina a detalle el funcionamiento de la mina, sus flujos operativos, las condiciones geográficas y cuáles son los objetivos estratégicos.

Este análisis permite al proveedor formular una propuesta técnica que contemple la personalización de una solución tecnológica, requieren un alto grado de adaptación para atender a las particularidades de cada operación minera y los objetivos a abordar. La relación por tanto es bidireccional: mientras que el proveedor adapta sus sistemas a los requerimientos concretos de la mina, la mina realiza ajustes internos, tanto desde un aspecto técnico como de capacidad operativa y organizacional, a fin de asegurar un correcto funcionamiento de los sistemas AIoT en su infraestructura.

Desde esta perspectiva, determinar quién y en qué medida participa en la generación de los datos y del conocimiento es una cuestión difusa ante la regulación jurídica actual. Para ello, es crucial delimitar jurídicamente el valor de los datos no personales y los intereses legítimos alrededor de estos, a través del establecimiento de derechos y deberes de los sujetos intervinientes, que eventualmente estarían asociados a la creación o producción de estos activos intangibles.

En tal sentido, las relaciones B2B constituyen un entorno propicio de interacciones que son objeto de relevancia para el derecho y su estudio debe atender la dinamicidad de las relaciones que se generan en la implementación de AIoT, a fin de establecer una estructura jurídica idónea y flexible que reconozca la naturaleza dinámica y evolutiva del proceso de innovación y que promueva un entorno de acceso para las partes.

2.2. Característica de los datos generados en el sector minero

Los datos recolectados durante las operaciones pueden implicar el tratamiento tanto de datos en bruto, es decir, datos que reflejan el estado real y actual de las cosas o procesos y se encuentran en un lenguaje legible por las máquinas; como de información procesada, que es información valiosa, estructurada, que tiene fines analíticos y estratégicos. Esta última podría incluir

información confidencial o sensible, como datos confidenciales o incluso secretos industriales, cuya protección requieren marcos contractuales claros entre las partes y conforme a la normativa vigente.

Hasta este punto, la instalación de dispositivos marca un punto crítico hacia un ecosistema operativo basado en la captura de datos en tiempo real que incluye el uso de información en bruto, que puede estar referida a temperatura, presión, vibraciones o composición del terreno, hasta datos procesados que pueden contener elementos sensibles como patrones de productividad, estrategias de producción, mantenimiento o rutas críticas, lo que usualmente lo convierte en información confidencial y de alto valor comercial.

Tal situación evidencia que es fundamental la adecuada gestión de estos datos, lo que implica contar o adaptar una infraestructura tecnológica robusta y también, como señala Jara (2021) implementar marcos contractuales que delimiten responsabilidad sobre la titularidad, aseguren la confidencialidad y regulen su uso, sobre todo ante la ausencia de regulación específica sobre los datos no personales (p.132).

Tal como han señalado algunos estudios sobre minería inteligente, el uso de los datos se convierte en un habilitador estratégico que permite optimizar decisiones en tiempo real, reduciendo costos, anticipando fallas y mejorando la sostenibilidad del proceso extractivo (Deloitte, 2021), Sin embargo, estas ventajas solo pueden alcanzarse si se implementan paralelamente medidas de protección técnicas y legales. Entre ellas destacan (celebrar o celebración acuerdos de confidencialidad) acuerdo de confidencialidad, clasificación de la información según su sensibilidad y adopción de mecanismos para pseudonominización o anonimización, de ser el caso (Corvalán et al., 2024).

Un ejemplo concreto de esta interacción tecnológica lo constituye el sistema de gestión de flota (SGF), el cual monitorea y controla las operaciones de la flota minera. Su propósito es reducir riesgos de accidentes, mejorar la eficiencia operativa de la flota y elevar la calidad del servicio logístico dentro del entorno extractivo (Billhardt, et al. 2014).

Este sistema recopila grandes volúmenes de datos en tiempo real sobre el comportamiento de los equipos móviles, los cuales son almacenados en bases de datos estructuradas y sometidos a procesos de filtrado y análisis. Mediante la aplicación de modelos predictivos y algoritmos de

aprendizaje automático, el SGF permite anticipar eventos críticos y tomar decisiones, su capacidad de rastrear individualmente cada equipo dentro del perímetro minero permite proteger tanto al personal como a los activos físicos, optimizar las rutas de operación y emitir alertas sobre necesidades de mantenimiento, ya sea en modalidad preventiva o reactiva. A continuación, se desarrolla el funcionamiento del sistema de gestión de flota a fin de entender la relación y la importancia de este sistema como fuente de recopilación de datos.

2.3. El sistema de gestión de flota (SGF) como referencia en la recopilación de datos

Cruz (2024), que escribe para la Revista Rumbo Minero, señala que el SGF es un sistema de control y monitoreo de equipos mineros que utiliza tecnología diversa para centralizar información que permite identificar y analizar la operación minera a fin de tomar decisiones basada en datos. Es un sistema que principalmente aporta en el incremento de la operatividad de la operación y, sobre todo, mejora la seguridad en la operación como tal.

Ahora bien, la arquitectura del SGF minera contiene: 1) sensores y dispositivos IoT tales como sensores, GPS o cámaras térmicas, controladores lógicos programables[1] (PLC), 2) IoT Gateways: es un dispositivo "traductor" que permite comunicar a los diferentes sensores o dispositivos inteligentes, como cámaras o sensores de calor, asegurándose que la data llegue sin problema y segura, 3) redes de comunicación inalámbrica (LTE, 4G o 5G): permiten llevar la información de un dispositivo a otro 6) servidores, aquí se almacena y procesa la información que se recopila de los sensores, 7) plataformas de gestión de flota (en el caso específico del SGF) por el software de gestión, que integra datos de diferentes fuentes y permite visualizar y analizar la operación de la flota y, 8) la interfaz del usuario que es con el que interactúa el operador minero.

Para ser más precisos con la arquitectura del sistema de AIoT, los componentes descritos anteriormente se reúnen en "capas" que cumplen un propósito específico dentro del sistema y son comunes a la mayoría de los sistemas AIoT, totalmente adaptables a diferentes industrias y tal como lo describe Smith & Moore (2018) a continuación:

[1] Los controladores lógicos programables (PLC, por sus siglas en ingles *Programmable Logic Controllers*) son dispositivos electrónicos diseñados para automatizar procesos o tareas repetitivas en entornos industriales como controlar maquinaria, sistemas de producción y otros equipos, reemplazando antiguos sistemas de control de funcionamiento de las máquinas basados en temporizadores. Por ejemplo, permite apagar un motor a partir de los datos que detecta un sensor sobre un sobrecalentamiento, protegiendo el sistema de daños mayores.

a) Capa de experiencia**:** Permite visualizar al usuario final las funcionalidades disponibles a través de interfaces gráficas de usuario. Es decir, aquí el operador minero se encuentra frente a pantallas similares a una computadora o *tablet*, donde puede dar uso al sistema, generar comandos y observar información importante.
b) Capa de servicios: Compuesta por bases de datos o archivos que representan el centro de datos de la mina, en donde se reciben reglas y procesos que gestionan las operaciones mineras como la planificación de rutas o mantenimiento de equipos. Por tal motivo, esta capa de divide en dos:
    i. Servicios: que implementan la lógica del negocio, reglas y procesos.
    ii. Integración y logística de datos: que se encarga de almacenar y gestionar los procesos de la información en el sistema.
c) Puertas de acceso (*Gateways*): aquí se manejan las comunicaciones entre interfaces de usuario, permite la comunicación de estos de manera segura y eficaz mediante la aplicación de políticas de seguridad, controles de acceso y de tráfico del sistema.
d) Capa de soporte o infraestructura: esta capa se encarga de las capacidades no funcionales del sistema como la gestión de claves y encriptación, registro, configuración, auditoría o registro de todas las actividades, entre cualquier otra medida necesaria que requiera la capa del servicio para ejecutarse de forma idónea.

De igual modo, Zvarivadza señala que, así como los dispositivos y las redes hacen factible la conectividad física entre sí, las aplicaciones que se desarrollan en el AIoT establecen interacciones confiables y robustas entre personas y máquinas (2024), por lo que son implementados en prospección minera, asistiendo eficientemente a la estimación de recursos, en planeamiento y optimización minera. Es también útil en otros aspectos o capacidades como abordar mecánica de rocas e ingeniería geotécnica, en ventilación minera, protección del medio ambiente y en la seguridad del personal en mina.

En suma, todo proceso en el que se incorpora una arquitectura AIoT genera una serie de oportunidades que permiten reconocer el valor crucial de la información dentro de un negocio específico. Esto plantea interrogantes sobre cuestiones técnicas y también sobre la propiedad de los datos recopilados y procesados, los cuales disponen de información altamente relevante. Este cuestionamiento surge tanto de los usuarios que adquieren o rentan un producto conectado, como en los diversos proveedores que intervienen en la implementación de la tecnología.

Ante este dilema, la definición de un posible concepto de “propiedad” o titularidad de los datos no personales es importante, especialmente para determinar qué actor o actores tienen legitimidad para utilizar, monetizar, procesar y atribuirse facultades de accionar sobre los datos.

Este cuestionamiento se torna complejo al considerar la incorporación de una regulación especializada en la materia. Debe prever límites en las negociaciones con los usuarios, incluir parámetros de interoperabilidad y seguridad, confidencialidad de la información, la protección de secretos industriales e incluso desde una perspectiva de protección de datos personales. Sin embargo, aunque es cuestionable la atribución de derechos sobre estos aspectos desde la perspectiva tradicional, es necesario considerar los tipos de datos que se recopilan y procesan, cuáles son las implicancias de tratar tales datos en un ecosistema del AIoT y establecer límites a la apropiación de la “información” en base a las características de los datos y el nivel de aporte de los actores.

Como veremos más adelante, desde un punto de vista tecnológico, el ciclo de los datos dentro de la arquitectura de sistemas AIoT es relevante en el análisis y determinación de una posible apropiación. Es decir, si los datos están en su fase original, como “datos en bruto”, o si han sido procesados y calidad de “datos derivados”, se debe aplicar o no la titularidad o propiedad a un actor en particular. El análisis debe contener disposiciones que no permitan una afectación a los esfuerzos de capital invertidos para obtener información relevante, evitando así desincentivos a la innovación tecnológica.

Para ello, es necesario prever y establecer reglas especializadas que permitan una implementación segura, equitativa y competitiva. Esto se debe hacer no solo bajo una perspectiva de protección exclusiva del usuario del dispositivo AIoT, sino también mediante la creación de una estructura legal dinámica que fomente la innovación tecnológica, asegurando un equilibrio justo en la protección de los derechos de ambas partes, principalmente respecto al acceso y a la información.

3. Tipos de datos que recopila el AIoT

La arquitectura descrita en el apartado anterior permite que las capacidades del AIoT y la naturaleza de sus componentes puedan capturar, recopilar, almacenar y procesar datos. Estas acciones son típicamente reguladas por la legislación en materia de protección de datos

personales como parte del “tratamiento” de datos. Como es evidente, los sistemas de AIoT a través de su capa de sensores, recopilan datos y posteriormente los transforman en información.

Según Jones y Tonetti, se debe distinguir entre “datos”, “información” e “ideas” importante de evidenciar. La información es un conjunto de bienes económicos no rivales que pueden representarse en cadenas de bits que son secuencias de unos y ceros, esta incluye tanto datos como ideas, que son un tipo de información (2018).

Siguiendo esa línea, el concepto de datos es un tipo de información que no son instrucciones en sí para crear cosas, sino que son útiles para el proceso productivo. Entonces, los “datos” son un concepto heterogéneo y diverso, pero, a efectos del presente trabajo, se hará referencia a “datos” como a toda representación fáctica de una característica, acción o hecho natural, pasible de ser calificada cuantitativa o cualitativamente y que puede ser almacenada en soportes digitales (Carriére-Swallow & Haskar, 2019).

A pesar de las diferencias conceptuales entre información, datos e ideas, en el lenguaje cotidiano se usan de forma indistinta. La discusión sobre este punto no ha tenido consenso, aunque existen algunos puntos en común. En un trabajo realizado por Duch-Brown et al., la “información” es un conjunto de señales interpretables y/o datos que necesitan transmitir un mensaje (Boisot & Canals, 2004, citado en Nestor Duch-Brown et al., 2017) y, por otro lado, define “datos” como un conjunto de códigos pasible de ser leído por máquinas a través de un proceso automatizado (2016, citado en Nestor Duch-Brown et al., 2017).

Respecto a la definición del “dato” como concepto clave para identificar si se debería atribuir derechos de propiedad o titularidad, Mylly (2024) sostiene que los datos son la materia prima de las industrias. Suelen presentarse como “datos en bruto” o “raw data”, los cuales se someten a un procesamiento posterior para generar información relevante, que luego se transforma en conocimiento o juicio. Este proceso de transformación es posible gracias a los datos en bruto, que sirven de base para dicha dinámica.

Este punto plantea un primer problema relacionado con el origen, la generación de los datos y de qué manera deben protegerse. Surge, entonces, la necesidad de una regulación que contemple la creación de una categoría jurídica específica que cumpla con la expectativa de promoción de la innovación en contextos industriales digitales y que faciliten la interoperabilidad

de datos en el mercado. Dicha regulación podría prever derechos de accesibilidad o la atribución de propiedad.

Por otro lado, Drexl destaca la distinción entre los niveles semánticos y sintácticos en la producción de datos. La "data semántica" se refiere a una forma de información que ya contiene un significado, mientras que los "datos sintácticos" hacen referencia a información codificada o datos en bruto, como un video en formato de bits y bytes antes de ser procesado (2018).

El *Data Act* de la Unión Europea, promulgada el 22 de diciembre de 2023, define a los datos como "*cualquier representación digital de actos, hechos o información y cualquier compilación de tales actos, hechos o información, incluso en forma de grabación sonora, visual o audiovisual*". Esta definición engloba tanto el nivel semántico y sintáctico de los datos, como el formato en el que pueden ser presentados, sin especificar quién es el generador de la información.

En ese sentido, es crucial determinar el tipo de datos que se recopilan en el uso de tecnologías emergentes, que podría estar relacionado a un sujeto u objeto (es decir, datos personales o no personales), o bien podrían referir a datos en bruto o procesados, dependiente de la etapa que se encuentren en su ciclo de vida del dato.

Este ciclo de vida tecnológico del dato es importante en los sistemas de AIoT, ya que están diseñados con arquitecturas específicas que cumplen con objetivos concretos en diversas industrias, lo que implica recopilar, filtrar, procesar y generar información de gran valor comercial. Dicha información se podría utilizar con fines alternos y en mercados alternos a la minería, contribuyendo así al crecimiento de múltiples sectores y de su eventual desarrollo.

En el sector minero, se busca implementar estas tecnologías con el propósito de mejorar la eficiencia y productividad, garantizar la seguridad reduciendo riesgos a nivel humano y de equipos que representan los activos más críticos en las operaciones mineras. En este escenario, es común que tecnologías como el AIoT se centran primordialmente en el tratamiento de datos no personales, sin excluir la posibilidad del tratamiento de datos personales, especialmente cuando la seguridad implica un seguimiento a la integridad de los trabajadores.

En consecuencia, en el contexto de las aplicaciones de AIoT para industrias, es necesario identificar el tipo de datos de tratamiento para determinar el tipo de regulación es aplicable. Este

análisis define las reglas que deben implementarse dentro del marco de interacción de diversos actores y, establecer si es necesario atribuir o desarrollar reglas sobre la “propiedad” de los datos. Además, es clave que se considere un enfoque de derechos fundamentales en la relación de la protección de datos, la propiedad intelectual y la competencia, para lo cual, a continuación, se abordarán las definiciones y características de los datos que lo diferencia en el alcance de la regulación.

3.1. Datos personales

En el Perú, la normativa de los datos personales está regulada por la Ley 29733, Ley de Protección de datos personales (LPDP) y su Reglamento aprobado por Decreto Supremo 016-2024-JUS (RLPDP). En el artículo 2.4 de la LPDP se establece que un dato personal “*es toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizados*”. En particular, el artículo 2.5 señala que los datos sensibles, “están constituidos por los datos biométricos, que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual”.

En el marco del uso de los sistemas de AIoT en el ámbito industrial minero, donde son necesarios los datos personales y datos sensibles, muchas aplicaciones de AIoT se desarrollan con fines de seguridad operacional, es decir para monitorear la salud de los operadores mineros durante el desempeño de sus labores en mina o para implementar soluciones que prevengan accidentes laborales asociados al personal, tales como accidentes por colisión, desastres naturales, distracción o somnolencia, entre otras situaciones de alto riesgo.

En el particular contexto de las operaciones en minería subterránea, los dispositivos tecnológicos pueden ser utilizados para rastrear la ubicación de los colaboradores, considerando los riesgos asociados a eventuales desastres, es decir, hay un especial interés por atender este ámbito, pues las operaciones son mucho más riesgosas por las condiciones de infraestructura. Es por ello que el monitoreo a partir de indicadores de salud son relevantes, como las horas de sueño, la presión arterial, la oxigenación y el ritmo cardíaco, entre otros, que constituyen datos de salud y, por ende, son una categoría especial de datos personales. Si bien el seguimiento de los colaboradores por motivos de seguridad ocupacional es una práctica vigente, el uso de esta

tecnología constituye un mecanismo habilitador que facilita la detección inmediata de anomalías y posibilita la adopción de decisiones preventivas efectivas.

Otros dispositivos también poseen capacidades para identificar y detectar la fatiga, distracciones y otras conductas a través de Visión por computadora (*Computer Vision*), un subtipo de IA que, a través de la captura de imágenes, capta elementos para identificar el rostro de la persona en tiempo real, y ante un evento de distracción o somnolencia, se envía una alerta hacia el centro del control principal, para que tome decisiones a fin de preservar la seguridad del operador. Ello implica como tal un tratamiento de imágenes en tiempo real y en otras, el uso de datos biométricos para identificar los eventos de fatiga y/o distracción asociados a un operador y a su rendimiento o condiciones de salud.

Ante la posibilidad latente del procesamiento de datos personales en tecnologías como el AIoT, es relevante hacer referencia a la definición de datos personales para identificar los criterios a considerar al momento de procesar tales datos. Tomaremos como primera referencia la definición realizada por la Comisión Europea (2023) que señala que es "*cualquier información que se refiera a una persona física identificada o identificable […] constituyen datos personales los distintos tipos de información que, en su conjunto, pueden permitir la identificación de una persona concreta*" (párr.1).

Por su parte, como ya hemos mencionado, en la regulación nacional los datos personales son toda información que *"identifica o la hace identificable"* a una persona, es decir que es posible que toda información que no esté directamente relacionada pero que, con el uso de medios razonablemente, pueda identificarlo, entonces constituye datos personales. Esto podría cuestionar la forma en cómo se está abordando el tratamiento de los datos personales en los dispositivos de AIoT, puesto que muchas veces la información puede ser residual pero es posible poder identificar a alguien y salir del ámbito que proponemos.

Asimismo, el Tribunal Constitucional Peruano señaló, en la Sentencia 02839-2021-PHD/TC, que la autodeterminación informativa es un derecho "*que toda persona posee para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentarlas posibles extralimitaciones de los mismos*" (Foja 4 de 04739-2007-PHD/TC) y que estaba sujeta al control de legalidad de la fuente de procedencia y que estos mantengan criterios de veracidad, integridad, utilidad y caducidad.

En esa misma línea, la Sentencia 292/2000 del Tribunal Constitucional Español es una resolución clave para el entendimiento del derecho de protección de datos personales porque reconoce que este derecho tiene un ámbito más amplio que el de la mera protección de la intimidad, sino refiere a "*cualquier clase de bienes y derechos constitucionalmente amparados*" (Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre). Aunque esta sentencia no aborda el valor económico de los datos, es el paso para concebir la protección de datos desde una perspectiva amplia, lo cual abre el debate sobre el control y acceso a los datos, incluso de carácter no personal, sustentado en que los datos tienen una dimensión económica evidente (Puyol, 2015).

Los datos personales son un concepto que ha tomado gran relevancia respecto a la protección que merecen. En ese sentido, para Piñar (2005), su tutela se desprende de un derecho que supone el reconocimiento de las personas de disponer de manera efectiva sobre sus datos personales que comúnmente se encuentran en disputa con otros derechos como la libertad de expresión, la transparencia y acceso a la información, pero, sobre todo, en este contexto, a los intereses y evolución del mercado (p. 13).

Para Nelson Remolina, los datos acerca de las personas y las bases de datos son insumos fundamentales para casi todas las actividades, en tanto permiten tomar e implementar decisiones de diversa naturaleza como económica, social, política y más. Son valiosas para las empresas en las que su principal activo son los datos porque pueden crear modelos de negocios en virtud de ellos, alquilarlos, cederlos, analizarlos, entre otros, pero además su valor no solo es económico sino también social y cultural (2012). Esta última idea es esencial porque los datos de las personas no son los únicos datos que poseen un valor económico, social y cultural, sino también que esas virtudes permiten ser explotadas por las industrias a fin de mejorar sus procesos, sus resultados e incluso hacer mejor el servicio para el público.

En contextos como el Big Data y otras tecnologías que se utilizan en el AIoT, el impacto cultural, tecnológico y académico nos obliga a reconsiderar la forma en cómo percibimos nuestro alrededor, pero también la forma en cómo las personas se relacionan. Dado que, interactuar con plataformas en calidad de consumidor-creador supone una pérdida del control del individuo sobre los datos que este produce (Zegarra, 2019, pp. 7-8), es crucial que desde el diseño se delimite el tipo de tratamiento de los diferentes tipos de datos, con la finalidad de adoptar las mejores

formas de protección de los datos, identificar qué normativa es aplicable y evitar una posible afectación de los derechos.

Además de las definiciones de datos personales antes planteadas, se han establecido criterios para determinar cuándo los datos son personales, los cuales se basan en estándares recogidos de múltiples definiciones y leyes aplicables. Por ejemplo, en la Unión Europea, el *WP Guideline* señala cuáles son las características que la autoridad debe tomar en cuenta para identificar cuándo estamos frente a un dato personal:

1) Por el contenido: cuando refiera a una persona en particular o el contenido se refiera a esta.
2) Por el elemento: cuando es posible que genere un impacto en una persona en específico incluyendo sus derechos o intereses.
3) Por el propósito: sea usado o tienda a ser usado para tratar de cierta forma o influenciar el estado o comportamiento de una persona.
4) Por el procesamiento: si a partir de dicha data resulta la identificación de una persona o de la posibilidad de identificar a una persona.

Estos criterios permiten la adecuada protección de los derechos del titular de los datos al permitir identificarlos dentro de los contextos de procesamiento masivos de datos, una técnica predominante en la actualidad para el desarrollo y despliegue de aplicaciones con inteligencia artificial. La afectación podría volverse invisible si no se adopta un criterio uniforme en diversos sectores a nivel nacional e internacional. Esto es especialmente importante considerando que los dispositivos de AIoT, al usar datos de manera masiva para su desarrollo y entrenamiento y al estar conectados a internet, el tráfico de los datos requiere de agudeza para identificar de dónde proviene, cuál es su naturaleza, qué medidas técnicas más rigurosas o particulares se debería implementar, entre otros.

Una vez que se expone la importancia de identificar los datos personales dentro de los contextos para desarrollar y entrenar dispositivos AIoT es pertinente conocer cómo es que se desarrollan en la aplicación del AIoT a minas. En la implementación de un sistema de detección de fatiga, por ejemplo, se pueden recopilar y tratar datos biométricos mediante reconocimiento facial que pueden estar asociados a un sistema de verificación o a través de sistemas de identificación que posee información sobre los turnos de operadores y permita identificarlos.

En este contexto de verificación, es posible monitorear información de salud, tales como ritmo cardiaco, calidad de sueño, niveles de oxígeno y/o presión, entre otra información concerniente a la salud. Estos datos son considerados como datos sensibles según la legislación en materia de protección de datos personales en el Perú a través de la LPDP y su Reglamento, normas que disponen que este tipo de datos deben ser recopilados y procesados bajo parámetros especiales y con especial cuidado por ser una categoría especial de datos personales.

Los datos personales requieren necesariamente la existencia de un sujeto o de una persona natural que sea identificable a partir de dichos datos, que los provea y autorice expresamente su tratamiento, ya sea por contener información directa como el nombre, DNI, imagen facial pero también ante la posibilidad de mediar cualquier inferencia que permitan identificarla de forma indirecta. En el contexto del Big Data aplicado al AIoT, incluso en entornos industriales como la minería, una forma adecuada de determinar si estamos ante datos personales consiste en evaluar si a partir de la información recopilada, es posible extraer atributos que permitan identificar las cualidades o aspectos subjetivos de individuo.

Por ejemplo, en el sistema de detección de fatiga en operadores mineros, se capturan datos personales de manera directa a través de sus imágenes biométricas, es incluso posible que, dependiendo de la tecnología no se utilizan imágenes, ni plantillas biométricas para detectar la fatiga y es posible que, al detectar en tiempo real, la imagen sin almacenarla ni transmitirla entonces no realiza tratamiento. Por otro lado, no se realiza tratamiento de datos personales si la imagen fácil se entrena solo para detectar un conjunto de puntos faciales vectorizados y este proceso es irreversible, de tal forma que no se puede identificar a la persona. Sin embargo, es probable que al utilizar tecnologías como las descritas, sean en el desarrollo como el despliegue, el tratamiento de imágenes de personas es indispensable.

Se advierte que, la detección de fatiga también se asocia a un tipo de tratamiento de datos “complementario” que puede estar asociada a patrones de comportamiento o actividad por día, y generar información personal de forma “indirecta”, lo cual puede utilizarse para evaluar el rendimiento del operador en una jornada o determinar el estado físico del operador a partir de patrones conductuales o fisiológicos. Dependerá del empleador determinar qué fines asignar a dicha información, cómo influye en las relaciones laborales, pero deberá someterse a las disposiciones en materia de protección de datos personales.

En este mismo entorno minero, se encuentran simultáneamente datos no personales, que están referidos a la temperatura del equipo, la vibración del motor, el consumo del combustible o el número de ciclos de carguío. Estos datos no identifican a una persona, ni directa ni indirecta y, en consecuencia, no le es aplicable la regulación en materia de datos personales. En la confluencia mixta de datos personales y no personales, cabe diferenciar los datos tratados a fin de evitar la aplicación de normativas que, en el caso de los datos personales, comprometería la afectación de derechos fundamentales pero que al mismo tiempo son útiles y de alto valor para la innovación industrial.

Sin embargo, en este tipo de entornos mixtos, donde coexisten datos personales y no personales, aplicar el mismo régimen jurídico a ambos tipos puede limitar injustificadamente el aprovechamiento de datos no personales con valor industrial. A través de las técnicas de anonimización y pseudonimización, se podría legitimar su uso. La legislación sobre protección de datos de la Unión Europea, el RGPD establece que, si para identificar a una persona se requiere de un uso desproporcionado de costos adicionales, tiempo y recursos tecnológicos para identificar a una persona, entonces no puede llevar a la categorización de datos personales, esta situación debe aplicarse solo cuando sea “fácilmente identificable”.

Aunque la protección de datos personales no reviste un carácter de derecho fundamental en todas las jurisdicciones, es posible afirmar que su protección está vinculada a la protección de otros derechos fundamentales. El dato personal persigue al titular, le es inherente y no es posible separarse de él, lo que lo convierte en un derecho relacionado con la identidad, intimidad, a su personalidad y dignidad de la persona.

Por tal motivo, la protección no debería depender únicamente del comportamiento del mercado y la innovación tecnológica, sino que debe centrarse en la protección de la persona humana y su dignidad. Sin embargo, en la era de transformación digital en donde las soluciones están pensadas para optimizar tareas e interactuar con las personas, estas tecnologías se deben adaptar para brindar soluciones en pro del bienestar colectivo y, para ello, es importante crear condiciones que promuevan un equilibrio entre la protección de estos derechos y los intereses económicos involucrados.

Aun cuando el uso masivo de los datos personales puede generar desarrollo y crecimiento en la economía digital basada en su uso indispensable, tanto si son personales como si no lo son, la sociedad en general puede y debe beneficiarse de su uso, pero sobre la base de la confianza y transparencia en su tratamiento, que permita brindar información suficiente al titular del dato para permitirle ejercer el poder de autocontrol y proporcionar herramientas para empoderarse frente a usos desproporcionados (Recio, 2017, p. 6).

En efecto, el contexto en el que los datos no personales adquieren una naturaleza personal, por ejemplo, mediante técnicas de reidentificación o correlación con otras fuentes, representa una preocupación en la perspectiva de la protección de los datos personales, por ejemplo, cuando cualquier dato se vincule, directa o indirectamente con una persona identificable dentro de un sistema, quedando sujeto al régimen de los datos personales. Este tipo de situaciones es especialmente relevante en contextos tecnológicos avanzados como el AIoT, donde el uso o tratamiento masivo y la interconexión de datos incrementan las posibilidades de que la información que inicialmente se recopiló o se determina como no personal adquiere el carácter de personal (Eckardt & Kerber, 2024).

No obstante, aunque ello produce un riesgo que debe ser reconocido y gestionado adecuadamente con medidas de seguridad, técnicas de anonimización irreversibles y otras organizativas, el presente estudio no busca abordar los criterios jurídicos de identificación o reidentificación de los datos personales. Tampoco pretende establecer lineamientos sobre el alcance del marco normativo en dicha materia, pero busca calificar a los datos no personales como una categoría autónoma especialmente tomando como referencia el contexto industrial minero para evidenciar un régimen jurídico especial para este tipo de datos.

Esta perspectiva la adopta el Data Act o Ley de Datos (en adelante, “Data Act”) de la Unión Europea que introduce derechos de acceso, uso y compartición de los datos no personales generados por los dispositivos IoT. Esta norma busca que se evite la excesiva concentración del control sobre los datos por parte de los fabricantes y busca crear espacios más abiertos, competitivos e innovadores. En particular, busca promover el acceso equitativo a los datos no personales generados por usuarios y dispositivos, contribuyendo así a dinamizar el ecosistema digital europeo (Eckardt & Kerber, 2024).

Desde un enfoque económico, también se ha advertido que una regulación centrada en la exclusividad sobre los datos personales puede derivar en fenómenos de fragmentación o limitando los beneficios sociales derivados de su circulación. Frente a ello, se ha propuesto que los marcos regulatorios favorezcan el acceso, la interoperabilidad y la compartición de datos, en lugar de reforzar esquemas de apropiación cerrada (Duch-Brown, Martens & Mueller-Langer, 2017).

Tales contextos difusos conllevan a que esta investigación proponga un análisis orientado a los datos no personales como activos estratégicos, cuya regulación debe enfocarse no en la protección individual, sino con la maximización del valor económico y social de los mismos. Para ello, se evaluará los modelos posibles de titularidad, acceso y gobernanza adecuados para contextos tecnológicos complejos como la industria minera, con el fin de proponer un marco normativo que favorezca tanto la innovación, el aprovechamiento de los recursos de un sector en específico y que el acceso sea más equitativo.

3.2. Datos no personales

Los datos no personales adoptan un papel clave en el ecosistema del AIoT en sectores como manufactura, minería, agricultura, etc. A diferencia de los datos personales, que se someten a regulaciones estrictas debido a su relación con la persona y su eventual riesgo de afectación de derechos fundamentales, los datos no personales no se vinculan a individuos específicos. En su lugar, estos datos refieren a información de valor económico - industrial que describe estados de los activos tales como maquinaria, condiciones ambientales, márgenes de producción, procesos operativos, indicadores, entre otros. Esta información es crucial para mejorar la eficiencia y optimizar la producción, reduciendo costos a partir de la toma de decisiones informadas y estratégicas basados en datos (lo que actualmente se conoce al modelo "*Data Driven*[2]").

Es así como, aunque los gobiernos han tomado predisposición para regular los datos personales, el concepto de los datos no personales ha sido definido de manera residual. Esto conlleva a categorizar a los datos no personales a todos los datos que no cumplen con las condiciones para calificarlos como datos personales. Por lo tanto, cualquier dato que no haga referencia a una

[2] El término *data-driven* (o "innovación basada en datos") hace referencia a un enfoque estratégico de innovación y toma de decisiones basado en el análisis masivo y sistemático de datos. Según la OECD (2015), el uso intensivo de datos provenientes de sensores, dispositivos conectados, interacciones en línea u operaciones comerciales, está transformando sectores tradicionales como el comercio minorista, la manufactura y la agricultura, permitiendo nuevas formas de creación de valor. En estos contextos, los datos no solo optimizan procesos, sino que generan productos y servicios completamente nuevos, impulsando la productividad, la eficiencia y el crecimiento económico.

persona o la haga identificable, entra en dicha categoría. Por ejemplo, la temperatura de la maquinaria o del ambiente, el consumo de combustible de equipos, niveles de presión atmosférica y oxígeno, estado de los gases de una maquinaria, entre otros relacionados con estados del entorno.

Según la Unión Europea, los datos no personales son información que generalmente no está relacionada con personas físicas, o que no se utiliza para identificar directa o indirectamente a una persona. Pueden ser datos que no pueden relacionarse con personas o se traten con la expectativa razonable de no utilizarse para identificar a alguien, por ejemplo, los datos meteorológicos o información sobre el tráfico vehicular. Es decir, es información que una vez anonimizada, difícilmente puede identificar a alguien (2014, citado en *International Chamber of Commerce*, 2023).

No obstante, es necesario precisar que, si bien los datos no personales están generalmente fuera del alcance de las regulaciones de protección de datos personales, estos datos pueden llegar a convertirse en datos personales a través de la correlación con nuevas variables, técnicas de reidentificación o análisis de patrones que puedan asociar a una persona. Sobre este punto no se harán mayores alcances en el presente trabajo, pero se resalta la necesidad de que la regulación pueda adaptarse a avances tecnológicos y ofrecer claridad en la frontera de ambos datos.

Una definición de datos no personales se encuentra en el recital 9 del marco regulatorio para la libre circulación de datos no personales de la Unión Europea, Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, señala que es todo aquel dato que no contenga información personal y que se genera a partir de infraestructura dentro de un proceso productivo industrial, operacional, comercial, tecnológico, técnico, ambiental (2018).

Otros autores como Supriyadi (2023), también define los datos no personales como:

> "*Datos que pueden referirse a cualquier información relativa a una persona no física cuando dicha información no lleva consigo ninguna identificación de una persona ya sea directa o indirectamente, como la información general confidencial de las empresas, datos estadísticos, activos de propiedad intelectual" (p.56).*

Esto incluye, además, los datos anonimizados, es decir, información que no se refiera a una persona identificada o identificable, o datos donde el interesado no sea o ya no se pueda identificar.

La importancia del concepto de los datos no personales radica, como afirma Mylly (2024), en su potencial para transformar las industrias y los negocios en la actualidad. Esto se debe a que la recopilación y procesamiento proporcionan información con un alto valor que se obtiene a partir del uso de nuevas tecnologías (p. 371). Los datos y la información se pueden reutilizar en diferentes sectores sin limitar o disminuir su valor o calidad, lo que facilita la innovación y desarrollo de nuevos productos o implementar mejoras. La Unión Europea ha equiparado el significativo valor de los datos con recursos como el oro o el petróleo.

Además, los datos no personales, además de ser trascendentales en la búsqueda de la optimización operativa de las industrias mediante el uso de sistemas de AIoT, juegan un rol clave en el desarrollo de nuevos productos y/o servicios que apuntan a un mayor rendimiento y precisión. Estos datos permiten a los productos adaptarse a la demanda en un mercado competitivo y personalizar los productos en respuesta a nuevas necesidades del mercado y de obligaciones legales, ambientales, condiciones de seguridad y/o privacidad.

Los datos no personales son cruciales para la innovación tecnológica, la comercialización de productos y la generación de competitividad en el mercado. Su recopilación y procesamiento constituye en una fuente de grandes volúmenes de información valiosa que sería aprovechada por la aplicación de nuevas tecnologías. Su libre disponibilidad y/o fácil acceso, permite la reducción de costos y mejora continua en la eficiencia, adaptabilidad escalabilidad y creación de impacto positivo en la sociedad.

Además, la innovación se fomenta sin comprometer la privacidad de las personas, lo que ofrece un mayor margen para su explotación y utilización en la creación de nuevos productos y generación de nuevos modelos de negocio. Esto es posible en la medida que se adopte un enfoque de derechos humanos en el diseño y despliegue de los productos, asegurando que no se conviertan en un riesgo inminente para los derechos fundamentales de las personas.

No obstante, existen al menos dos desafíos claves en el procesamiento de los datos no personales que requieren especial atención. El primero consiste en el refuerzo para identificar de

manera diferenciada los datos personales de los no personales en un contexto de recopilación masiva con técnicas de Big Data, en donde debido a la gran cantidad o volúmenes de recopilación de datos, resulta difícil distinguir si se están recopilando datos personales.

El segundo desafío radica en la necesidad de delimitar de manera clara y precisa el ámbito de aplicación de los datos no personales, que podría realizarse a través de la creación de una categoría específica que atienda a la naturaleza y sus características particulares. Abordar este desafío es importante para evitar una aplicación incorrecta e imprecisa de la normativa que puede llevar no solo a la violación de derechos de la privacidad o restringir los derechos de autodeterminación informativa, sino también a la restricción de capacidades comerciales de los agentes económicos tecnológicos y al freno de la innovación.

Es esencial determinar en qué medida los datos sometidos a técnicas de anonimización deben ser considerados como datos personales o no personales. Aunque los datos anonimizados adecuadamente y conforme a la legislación pueden utilizarse para diversos fines sin requerir el consentimiento del titular, persiste la inquietud sobre la posibilidad de reidentificar a una persona mediante el uso de datos no personales.

El dilema sobre qué tipo de datos son los datos anonimizados se esclarece cuando el Reglamento (UE) 2016/679, 2016), Reglamento General de Datos Personales (RGDP) señala que los datos anonimizados pueden mantener la calidad de datos personales si es posible reidentificar a la persona mediante un proceso de desanonimización. Sin embargo, el ámbito de aplicación del RGDP no abarca estos cuando las técnicas de anonimización son irreversibles, de tal forma que no se podría identificar a la persona directa o indirectamente (Klippa, 2023).

Es un hecho que las técnicas de Big Data permiten recopilar y procesar grandes volúmenes de datos de manera indiscriminada, lo que genera un riesgo de incumplimiento en la aplicación de regulación de datos personales en tanto estos no son técnicamente fáciles de identificar. Ello obligaría a los implementadores de AIoT a cumplir con una serie de prerrogativas legales y técnicas ante la eventualidad de recopilar datos personales aún si este no es el objetivo principal, dando a lugar costos innecesarios y barrera burocráticas para el sector industrial, en donde es posible la convergencia de datos personales como no personales, aun cuando la prioridad sean estos últimos. Por ende, los datos anonimizados podrían ser una alternativa viable en la medida

que mejore la calidad de procesamiento de información sin generar esfuerzos adicionales para detectar datos personales o no personales.

Este punto debe ser aclarado dentro un marco legislativo específico y concordante, que contemple criterios claros sobre la anonimización de los datos personales. Esto conlleva a determinar a los datos anonimizados como datos no personales o, en su defecto, establecer si deben adoptar una categoría distinta con un ámbito de protección específico, sin embargo, es un objeto de estudio que excede el alcance de la presente investigación.

3.2.1. El procesamiento de los datos no personales como proceso de valorización

En la implementación y uso de AIoT en la industria minera, como un sector que representa un porcentaje importante para las economías nacionales y mundiales, el valor económico se genera en el procesamiento de datos que se obtienen a partir de productos conectados a internet o a dispositivos AIoT. Estos datos son el núcleo central que crea un modelo de negocio de las empresas B2B enfocadas en el desarrollo de tecnologías y/o software como servicio, es decir, empresas de tecnología que desarrollan productos y/o servicios tecnológicos para otras industrias.

Pese a ello, el valor del dato no radica en cualquier tipo de dato, en su estado bruto o procesado, personal o industrial, sino que su valor predomina en el proceso de transformación del dato a información con un componente comercial o industrial. Este ciclo implica el procesamiento de los datos mediante la aplicación de métodos analíticos, relacionales y lógicos que permiten extraer información relevante a partir de los datos disponibles. Es esta transformación la que determina el valor de los datos y su utilidad depende de los resultados que se vean cuando se toma información en base a los datos.

Cabe resaltar que la fase de procesamiento de los datos en contextos de AIoT no es estática. Atraviesa una serie de etapas técnicas dentro de la arquitectura del sistema, en las cuales los datos se transforman progresivamente hasta adquirir un formato legible y funcional para distintos fines. Este recorrido no solo responde a las especificidades de cada componente desde la captación hasta el análisis avanzado, sino que también implica una variación en el valor que poseen en cada fase, lo que implica a su vez, un nivel de inversión tecnológica distinto que se requiere para procesarlos, almacenarlos o activarlos.

Por ello, para entender en qué momento los datos adquieren un valor significativo dentro de un proceso determinado, es necesario entender cómo son procesados dentro de la arquitectura y cómo se clasifican respecto al ciclo de vida del AIoT, es decir si estos se introducen al sistema en calidad de datos en brutos, luego son preprocesados para obtener que puedan ser posteriormente analizados.

3.2.2. Datos en bruto

Los datos en bruto o “raw data” representan un tipo de información que no se encuentra procesada o filtrada, se recopilan a partir de los sensores, detectores, cámaras o como ya hemos visto antes, a partir de la capa de sensores o actuadores del sistema AIoT. Estos datos se capturan en tiempo real y se encuentran en el estado más básico sin ningún tipo de transformación aplicada. Esto además puede incluir lecturas de temperatura, presión, humedad o parámetros físicos en general, suelen estar en su forma más cruda y voluminosa, por ejemplo, una serie de números que representan temperatura en diferentes momentos del día.

Otra forma de definirlo es como todo dato que refleja exactamente el estado en la realidad física, que pasan por una etapa de filtrado, clasificación y análisis. El estado en bruto significa que no se han filtrado ni organizado en “tablas relacionales”, es decir que no se sitúan dentro de un análisis de correlación entre las categorías, lo que significa que son difíciles de interpretar por personas o por máquinas, por ello es necesario que exista un análisis posterior, una vez que se haya determinado la categoría, otra información y relación con otro tipo de datos para encontrar correlaciones entre ellos y producir información relevante.

La arquitectura del AIoT está compuesta por diferentes capas que cumplen una función determinada dentro de un proceso minero. Empezando por la capa de sensores, estos dispositivos captan datos del ambiente u otros entornos físico s y son recopilados en tiempo real. Una vez recopilados, los datos deben atravesar una fase de “depuración” debido a la cantidad de datos que recopilan. Algunos de estos datos en su estado bruto podrían generar interferencias, duplicarse o creando inconsistencias por estar fuera del rango establecido y por ello, no son fácilmente procesables.

3.2.3. Datos preprocesados

Una vez recopilados en su estado natural y posteriormente “filtrados”, los datos se transfieren a la capa de la nube para una segunda transformación. Estos viajan a través de protocolos o *gateways* (dispositivos que permiten la transmisión de información), que suelen usar señales satelitales para enviar los datos. Después de ser enviados, los datos se almacenan en la nube o en servidores locales, donde las plataformas de AIoT los procesan.

El procesamiento puede ser tan sencillo como verificar si un dato cumple con un rango específico, como la temperatura o estados físicos de un equipo o, complejo, como cuando se utiliza visión por computadora para identificar objetos o medir distancias. Esta tecnología permite que las computadoras reconozcan objetos a partir de imágenes, lo que abre un mundo de posibilidades para el análisis de datos visuales.

Luego de ser enviados a servidores físicos o en la nube, estos son comprimidos y encriptados para asegurar la seguridad y compatibilidad entre diferentes protocolos utilizados en varios dispositivos de transmisión (*gateways*). Los datos suelen ser además almacenados en “*Data Lak*es”, que es simplemente un lugar donde se guardan los datos en su forma original o bruta.

Cuando se solicita información útil, se seleccionan los datos relevantes y se organizan en bloques o flujos, lo que permite transformarlos y filtrarlos para enviarla a un almacén de Big Data *(Big Data Warehouse)* (Lakhwani et al., 2020). Hasta este punto, los datos ya han sido transformados a través de un tipo de técnica y nos encontramos ante datos pre-procesados porque no generan una información de valor, pero se preparan para ser analizados y procesados con el fin de proporcionar información disgregada y relevante.

Por otro lado, los *Data Lakes* y el almacenamiento de *Big Data* tienen diferencias clave. En el almacén de *Big Data*, los datos no solo se almacenan de forma estructurada y procesada, sino también incluyen detalles adicionales, conocidos como metadatos, como la ubicación de los sensores y los comandos que pueden enviarse directamente a los dispositivos. Esta organización facilita las consultas y análisis de los datos, permitiendo que sean fácilmente accesibles y útiles (Lakhwani et al., 2020).

3.2.4. Datos preprocesados

Una vez recopilados en su estado natural y posteriormente “filtrados”, los datos se transfieren a la capa de la nube para una segunda transformación. Estos viajan a través de protocolos o *gateways* (dispositivos que permiten la transmisión de información, ver página 26) que suelen usar señales satelitales para enviar los datos. Después de ser enviados, los datos se almacenan en la nube o en servidores locales, donde las plataformas de AIoT los procesan.

El procesamiento puede ser tan sencillo como verificar si un dato cumple con un rango específico, como la temperatura o estados físicos de un equipo o, complejo, como cuando se utiliza visión por computadora para identificar objetos o medir distancias. Esta tecnología permite que las computadoras reconozcan objetos a partir de imágenes, lo que abre un mundo de posibilidades para el análisis de datos visuales.

Luego de ser enviados a servidores físicos o en la nube, estos son comprimidos y encriptados para asegurar la seguridad y compatibilidad entre diferentes protocolos utilizados en varios dispositivos de transmisión (*gateways*). Los datos suelen ser además almacenados en “*Data Lak*es”, que es simplemente un lugar donde se guardan los datos en su forma original o bruta.

Cuando se solicita información útil, se seleccionan los datos relevantes y se organizan en bloques o flujos, lo que permite transformarlos y filtrarlos para enviarla a un almacén de Big Data *(Big Data Warehouse)* (Lakhwani et al., 2020). Hasta este punto, los datos ya han sido transformados a través de un tipo de técnica y nos encontramos ante datos pre-procesados porque no generan una información de valor, pero se preparan para ser analizados y procesados con el fin de proporcionar información disgregada y relevante.

Por otro lado, los *Data Lakes* y el almacenamiento de *Big Data* tienen diferencias clave. En el almacén de *Big Data*, los datos no solo se almacenan de forma estructurada y procesada, sino también incluyen detalles adicionales, conocidos como metadatos, como la ubicación de los sensores y los comandos que pueden enviarse directamente a los dispositivos. Esta organización facilita las consultas y análisis de los datos, permitiendo que sean fácilmente accesibles y útiles (Lakhwani et al., 2020).

3.2.5. Datos procesados

Posteriormente, mediante la analítica de datos, se detectan correlaciones y patrones en los datos pre-organizados y almacenados en el *Big Data*. Además, se pueden asignar tareas específicas como presentar tal información en gráficos o diagramas, que están orientados a proveer información relevante de la operación a un usuario final. Esta forma ordenar y estructurar genera un valor adicional a las bases de datos, debido al tiempo y el capital invertido. Esto ha llevado a la UE a crear un marco de protección a través de la asignación de derechos de propiedad intelectual bajo categoría de los “derechos sui generis” establecidas en la Directiva de Bases de Datos.

En este sentido, se ha reconocido un valor especial en la estructura y originalidad que pueda generarse en el desarrollo o creación de bases de datos, lo que constituye un inicio para entender que los datos poseen valor no solo en su forma estructurada sino también en su estado en bruto. Si bien los datos por sí solos carecen de protección jurídica tradicional en tanto no incorporen elementos de creatividad, la organización, selección o disposición de estos puede ser protegida en ciertos regímenes a través de derechos sui generis, como ocurre en la Unión Europea (Duch-Brown, Martens y Mueller-Langer, 2017).

En el contexto del AIoT, los datos preprocesados resultan fundamentales para el desarrollo y despliegue de funcionalidades complejas. No obstante, los datos en bruto también poseen un valor económico, al permitir que otras empresas inviertan sus esfuerzos de tiempo y dinero para estructurarlos conforme a sus propias lógicas de clasificación, procesamiento y explotación. Esta capacidad de estructurar datos de forma independiente es precisamente lo que da lugar a distintas formas de agregación de valor, más allá de un enfoque de exclusividad sobre el dato como tal (Eckardt & Kerber, 2024).

Desde una perspectiva económica, este proceso se relaciona con la noción de "economías de alcance" en el análisis de datos, donde distintos actores pueden derivar valor de un mismo conjunto de datos brutos, pero a partir de distintas aplicaciones o modelos de negocio. De allí que restringir el acceso o apropiarse de los datos en sus etapas iniciales puede derivar en fallas de mercado y pérdida de eficiencia agregada (Duch-Brown et al., 2017). Por ende, los datos en bruto y los preprocesados poseen un valor económico dentro del ciclo de vida de los productos AIoT, lo que exige revisar su tratamiento respecto a la apropiación de estos y el impacto que su exclusividad generaría en el mercado digital.

En la última fase, una vez que se obtienen los análisis de los datos mediante la aplicación de Machine Learning a los datos pre-procesados, se puede mejorar la precisión de los dispositivos y asignar como realizar predicciones y/o recomendaciones basadas en un análisis sistemático y con una gran cantidad de datos. Los modelos de *machine learning* aprenden de los datos históricos registrados y generan información relevante a partir de ella. Por ejemplo, en el proceso productivo en una mina, se hace posible entender cómo se interrelacionan los datos de un proceso en específico, por ejemplo, combustible y tiempo recorrido de una maquinaria.

Los espacios en los que se genera información cada vez más valiosa atraviesan un proceso de transformación avanzado. En esta etapa, los datos pueden ser procesados mediante técnicas sofisticadas, como modelos de *machine learning*, analítica de datos avanzada, entre otras herramientas de inteligencia artificial. Estos modelos requieren una programación especializada que se adapta a procesos específicos, entrenamiento y mejora continua aplicados a un campo de expertise concreta. Este enfoque implica una inversión significativa de tiempo, recursos intelectuales y de capital, que persigue alcanzar niveles de precisión y efectividad a partir de los datos, de manera que genere información que permita tomar decisiones estratégicas.

En el caso del sistema de gestión de flota minera, el AIoT recopila datos a través de los sensores instalados en los equipos mineros como perforadoras, palas excavadoras o chancadoras o autos y, mediante un software que procese los datos, se monitorea estados de las máquinas como temperatura y ubicación que, con analítica avanzada permite detectar o predecir anomalías, eventos de riesgo, entre otros que son necesarios para usar los activos mineros eficientemente.

En consecuencia, los datos adquieren un valor agregado a medida que atraviesan por capas dentro de la arquitectura del AIoT, lo que les otorga un valor económico distinto. La información que se genera a partir de la aplicación de tecnología IA sobre los datos, que hace posible las predicciones y recomendaciones, no es lo mismo que visualizar el estado en tiempo real de los equipos, aún si ambas permiten de alguna forma, asegurar los niveles de eficiencia y optimización de las operaciones mineras.

Dicho esto, es importante considerar cómo debe proteger esta información, tanto desde el punto de vista de la propiedad intelectual como de la privacidad de los datos. Los datos generados pueden adquirir un valor económico pasible de ser distribuido, comercializado y mejorado para su posterior lanzamiento al mercado. Esto plantea cuestiones problemáticas respecto a quién

está autorizado a utilizar y explotar tales datos, y si algunas de estas acciones pueden ser excluidas entre los diferentes actores involucrados, y quien adquiere la calidad de titular del dato no personal.

En ese sentido, es crítico establecer diferencias entre los tipos de datos que se generan y el valor que tiene cada uno de ellos. Los datos en bruto y los datos procesados marcan un ciclo de vida dentro del procesamiento, y ello facilita las condiciones a tomar en cuenta para determinar quién y cómo serán obtenidos, utilizados y comercializados. También, es importante entender las interacciones entre los diferentes actores intervinientes en el proceso de tratamiento de los datos, de modo que se prevean derechos y deberes sobre el uso de dichos recursos.

4. Sujetos intervinientes en el uso de AIoT en el sector minero

La industria minera incorpora el AIoT dentro de sus procesos con la finalidad de adaptarse a la cuarta revolución industrial al constituir un habilitador clave para este proceso de transformación. En dicho entorno, la interacción entre máquinas se extiende a un ecosistema más amplio en donde intervienen múltiples actores en la generación, tratamiento y aprovechamiento de los datos.

Este vínculo interactivo entre actores no responde a relaciones de simple consumo o uso final, sino que se estructuran bajo esquemas de colaboración empresarial más complejos y, a efectos de la presente investigación, las relaciones se generan entre entidades privadas bajo el modelo *business to business* (B2B). Un reporte de McKinsey & Company evidencia que para el 2030 el valor potencial del IoT podría aportar de 5,5 billones a 12,6 billones de dólares en su valor a nivel mundial, incluido el valor que los consumidores y clientes de productos y servicios de IoT representan, sobre todo en la creación en aplicaciones B2B, de las cuales se estima un alrededor del 65% del potencial para este tipo de aplicaciones (Chui Michael et al., 2021).

Este modelo B2B se centra en el desarrollo de productos y servicios muy especializados, enfocados en procesos específicos y necesidades muy particulares de una industria en específico. En el caso minero, la aplicación del AIoT es adaptable a los procesos mineros como extracción, producción, exploración, entre otros. En ese sentido, se involucran múltiples actores, que cumplen una función especial en relación con el proceso y la arquitectura del AIoT. Identificar

de qué manera se relaciones los actores alrededor de las tecnologías es importante para discutir las cuestiones alrededor de la atribución de derechos sobre los datos.

Tal como lo definen Van Asbroeck y Debussche Jasmien, la cuestión de la propiedad de los datos se complica debido al ciclo del valor de los mismos, el cual es sumamente complejo y cuenta con la participación de una variedad de partes interesadas. Esta situación incrementa la dificultad de determinar quién tendría derechos legítimos a reclamar la propiedad de los datos. Muchas partes podrían reclamar la propiedad, ya sea por la creación o generación de los datos, o bien por su uso, compilación, selección, estructura, reformateo, enriquecimiento, análisis, adquisición de licencias o por cualquier otra forma que añada valor a los mismos (2017).

4.1. El usuario

El usuario es la persona que utiliza un producto o servicio en calidad de persona natural o jurídica. En el contexto de los sistemas AIoT, el usuario es quien accede a un producto conectado sea bajo la modalidad de venta o de alquiler.

Como lo ha señalado el Data Act, el usuario es quien arrienda un producto conectado, utiliza un servicio relacionado o recibe servicios vinculados al producto, convirtiéndose en los actores centrales para acceder a los datos (fundamento 12 y 13 del Data Act). Esta relación le permite interactuar con el dispositivo y producir datos, lo que a su vez le faculta acceder, usar y compartir con un tercero, todo tipo de dato que genera. Esta noción sitúa al usuario como el centro de la fuente de acceso y del efectivo ejercicio derechos de uso, compartición, acceso. Sin embargo, más adelante se estudiarán las teorías sobre atribuir derechos exclusivos a los usuarios y las consecuencias de la atribución exclusiva a diferentes actores.

4.2. El titular de los datos

En relación a las formas de agregar valor a los datos en el uso del AIoT, convergen diferentes agentes que representan titularidad sobre los datos que generan. Entre esta pluralidad de actores, se encuentra al titular de los datos que viene a ser el individuo o entidad sobre quien refieren los datos, a partir del cuál se recopilan y de qué se origina. Es decir su fuente de origen.

En forma sencilla, el titular del dato es aquel quien ostenta un poder sobre este, en el caso de los datos personales, es de quien el dato se refiere. Pero en el caso de los datos personales, en

tanto no refiere ni identifica a una persona natural, en la actualidad no existe una definición sobre quién tiene titularidad sobre estos. En el caso del AIoT en el sector minero, el titular del dato viene a ser la entidad que genera el dato a partir de una fuente que forma parte de una estructura que le pertenece al usuario o un tercero proveedor. No obstante, utilizar la "titularidad" en un contexto como el presente, resulta innecesario y poco eficiente en tanto debería identificarse los derechos o facultades que los titulares poseen respecto al dato en cuanto a acceso, uso y/o control de los datos, dependiendo del contexto de su generación y tratamiento.

El Data Act no define la figura del titular del dato no personal, pero por el contrario parte del principio de derecho funcionales de los datos, el cual consiste en que el usuario del producto o servicio conectado, es decir, quien opera el sistema, tiene un derecho de acceso sobre los datos. A su vez, permite que bajo ciertas condiciones, el acceso por terceros siempre exista un acuerdo previo con el usuario, dado que esto se da en condiciones de competencia, como por ejemplo los servicios complementarios.

Sin embargo, lo ideal es que a través de la atribución de derechos y obligaciones sobre nociones de exclusividad y restrictividad, busquen fomentar la innovación y evitar situaciones que generen un control exclusivo y que inciden negativamente en la noción de fomentar la compartición de los datos para mejorar el estado de la innovación en el sector.

4.2.1. El proveedor tecnológico

A su vez, el proveedor tecnológico del AIoT desempeña un rol crucial en la innovación dentro del ecosistema. Este agente es responsable de analizar las necesidades operativas específicas de las minas, conceptualizar, adaptar y desarrollar una solución tecnológica con algún dispositivo inteligente, y configurar una opción capaz de optimizar la recolección, procesamiento y análisis de datos a lo largo de la cadena de valor.

El proceso de generación de valor comienza con el diseño del modelo de negocio, el cual se define a partir del análisis de caso de uso y el entorno tecnológico del cliente. A continuación, se desarrollan y entrenan los dispositivos, los cuales pueden operar de forma autónoma o en red, recolectando datos en tiempo real. Una vez desplegados en campo, por ejemplo, instalados en las maquinarias o infraestructuras mineras, los dispositivos inician un ciclo continuo de recopilación, procesamiento y transmisión de datos.

Este ciclo técnico de vida del dato tiene diferentes instancias: recolección, estructuración, análisis y visualización. El proveedor puede asumir funciones como recolector, procesador y analista, lo que le otorga una participación en el flujo y un margen para la explotación del dato en cada etapa. En consecuencia, el valor no reside únicamente en el dato bruto, sino en su transformación con la aplicación de diferentes algoritmos, arquitecturas de red e interfaces que permiten convertir la información en conocimiento útil para la toma de decisiones estratégicas y con un enfoque preventivo.

Además, esta suma de valor se apoya no solo en la infraestructura tecnológica, sino también en el componente humano, el talento especializado, en análisis de datos, el diseño industrial y hasta la ciberseguridad. Este enfoque permite escalar soluciones de manera eficiente, sostenible y adaptable a diferentes entornos. Esto incluye el rol de las personas en la identificación de los inputs (o datos de entrada) y en la interpretación de los outputs (o datos de salida).

En suma, el proveedor tecnológico, al integrar capacidades técnicas y humanas, convierte a los datos, que son un recurso latente, en un activo estratégico. Así, contribuye al aumento de la productividad, la reducción de costos, mejora en la seguridad y toma de decisiones basadas en evidencias proporcionadas por los datos en el entorno minero.

En el sector minero, al igual que otras industrias, varios proveedores tecnológicos compiten ofreciendo diversas soluciones innovadoras basadas en tecnologías similares, dependiendo de la disponibilidad y del nivel de innovación. Aunque se ofrezcan servicios similares, la diferencia puede recaer en sus modelos de negocio o en el proceso minero en el que se enfocan.

A modo de ejemplo, estratégicamente la arquitectura del AIoT agrega valor al combinarse con la infraestructura de Tecnologías de la información (TI) con plataformas de datos que se integran entre sí y que permiten gestionar en tiempo real y de forma coordinada las operaciones mineras. Este modelo se conoce como “centro neurálgico”, en donde los datos que se encuentran dispersos a lo largo de la cadena de valor se puedan centralizar y tomar decisiones integradas con información basada en datos (Deloitte, 2021).

Otro modelo como parte del enfoque integral es el de “operaciones inteligentes” que junto con él permite que los datos sigan su flujo de forma estructurada, promoviendo la agilidad en la toma

de decisiones y que se tomen a partir de la evidencia. Es así como la arquitectura del AIoT habilita la conectividad técnica y, al integrarse con el talento humano, se genera una capacidad organizativa orientada al valor (Deloitte, 2021).

4.2.2. Los terceros proveedores

Además de los actores primarios, como el proveedor tecnológico que desarrolla, implementa y opera dispositivos AIoT, en el ecosistema B2B del sector minero, intervienen también terceros proveedores que desempeñan un rol cada vez más relevante en la creación de servicios tecnológicos complementarios. Dichos terceros no intervienen, por lo general, en la configuración estructural o en el diseño de la arquitectura del sistema, sino que operan sobre infraestructuras previamente instaladas o en tecnologías ya desplegadas por proveedores principales, a partir de las cuales ofrecen soluciones especializadas y/o complementarias, que son pasibles de integrar.

La participación de estos terceros, a menudo se articula a través de servicios híbridos, que combinan software de análisis, plataformas de visualización, servicios de interoperabilidad y otros. Por ejemplo, una empresa de procesamiento especializada para datos geoespaciales puede integrar su plataforma que permite visualizar otras variables operativas críticas como el rendimiento de equipos, estabilidad del terreno, entre otros.

Estos servicios requieren acceso temporal, estructurado e interoperable a los datos generados por dispositivos AIoT u otra infraestructura IoT industrial previamente establecida por los proveedores iniciales, lo que implica generar integraciones técnicas, a fin de compartir, transformar y utilizar los datos de manera compartida en sistemas heterogéneos.

Esta integración se hace posible cuando el proveedor principal acepta la conexión de tecnologías de terceros a su sistema, implicando a su vez asumir costos adicionales de la integración. Este escenario demuestra la etapa de las relaciones B2B en donde se generan condiciones de acceso, uso y reutilización de los datos, que son evaluadas a partir de un enfoque técnico, comercial y jurídico. Una falta de apertura del proveedor inicial o una negativa al uso de sus sistemas influye en las decisiones de la mina, los proveedores, pero, sobre todo, cómo se hace exigible la cooperación entre proveedores a fin de explotar el beneficio de ambas.

Además de lo expuesto anteriormente, está vigente un reto importante para los proveedores tecnológicos, referido a la infraestructura limitada, la cobertura de red y almacenamiento de datos insuficiente, lo cual puede dificultar la implementación de soluciones, especialmente en el contexto de las condiciones variables de la mina. Esto se debe a que los productos y/o servicios tecnológicos son desarrollados o adaptados por empresas especializadas en el rubro, que brindan soluciones de software y/o hardware bajo licencias. No obstante, en la realidad es inevitable no contar con múltiples proveedores de servicios similares pero especializados o complementarios que ayuden a cubrir ciertas demandas en el contexto de transformación digital de las minas.

Así, la figura de terceros proveedores plantea una serie de interrogantes: ¿Quién tiene derecho a acceder a los datos generados por los dispositivos? ¿En qué condiciones puede hacerlo un tercero y bajo qué límites? ¿Se debería considerar al proveedor inicial como un titular de derecho exclusivo de control? ¿Existen márgenes para reconocer una cogeneración de datos o una titularidad que permita compartir de manera funcional los datos?

Estas preguntas marcan un horizonte al planteamiento normativo que debe responder a cuál es la forma más viable para abordar jurídicamente la complejidad de las relaciones entorno a los datos generados por dispositivos AIoT en contextos industriales como el minero. La presencia de terceros ajenos a la relación B2B, como empresas subcontratistas, entidades no gubernamentales, investigadores, conlleva a repensar los límites del acceso y control de los datos más allá de una simple definición del proveedor inicial como único titular que ejerce control sobre los datos.

4.2.3. El fabricante de equipos originales (OEM)

En las relaciones B2B del sector minero, cuando hace uso del AIoT es indispensable considerar la figura de Fabricante de Equipos Originales (OEM por sus siglas en inglés "*Original Equipment Manufactur*er"), rol central en la arquitectura operativa de las maquinarias críticas y esenciales para llevar a cabo el proceso minero como camiones, excavadoras, chancadoras, perforadoras, palas. Estos activos no se limitan a suministrar bienes físicos, sino que poseen sistemas cerrados que limitan, contractual y técnicamente, la posibilidad de integrar dispositivos a terceros.

El término “OEM” hace referencia al fabricante del equipo original (“*original equipment manufacturer*” por sus siglas en inglés). El Diccionario Cambridge define este término como la empresa que fabrica piezas y productos para otras empresas que son vendidas bajo su propio nombre o los utilizan en sus propios productos. En la industria del sector automovilístico y tecnológico se usa para identificar a quienes fabrican productos y luego son vendidos o integrados para otras empresas bajo su propia marca.

No obstante, ha sido un término que puede contener algunas ambigüedades, ya que depende del sector en el que se utilice. Por ejemplo, en la industria de Tecnología de la información (TI), en sectores como microprocesadores o discos duros, adquieren algunas piezas de otros OEM y los utilizan para fabricar sus propios productos, convirtiéndose así en Clientes OEMs (Smith & Moore, 2018). En el caso de hardware, marcas como Dell, Lenovo, HP son conocidas a nivel internacional por vender productos bajo sus propias marcas, pero dependen de otros OEM de pequeñas piezas o componentes.

En el AIoT aplicado al sector minero, el concepto de OEM puede referir a diversos actores dentro de la cadena de producción. Por un lado, el OEM del equipo de equipo minero fabrica tanto hardware como software de las máquinas, como Hitachi, Volvo, Caterpillar, entre otros, que son conocidos por sus equipos de carguío para industrias y responsables de diseñar y fabricar la maquinaria que los mineros utilizan para operar.

Desde una perspectiva tecnológica, muchos OEM desarrollan sus propios sistemas de monitoreo, conectividad y diagnóstico, procurando preservar la integridad de su ecosistema digital. A diferencia de los proveedores tecnológicos, el OEM controla el punto de origen del dato a partir de sus equipos. El proveedor tecnológico solo habilita el flujo de procesamiento y de una estrategia sobre el dato (incluso con hardware y software). En consecuencia, al mantener un control dominante respecto al origen del dato, es posible establecer restricciones explícitas al uso de sensores, dispositivos AIoT o plataformas externas que pretendan instalarse o interactuar con sus equipos.

Esta posición podría responder, desde la seguridad operativa de la maquinaria, a la defensa de los modelos de negocios basados en servicios postventa o desde un punto de vista de la propiedad intelectual como licencias exclusivas. Cualquier intento de integración a otras

tecnologías desarrolladas por terceros, incluso por el mismo cliente, podría ocasionar alguna limitación contractual, técnica o jurídica impuesta por el OEM.

En este punto se plantea una coyuntura estructural, si bien la maquinaria opera en entornos del cliente, y ha sido adquirida por esta, los datos que generan pueden resultar estratégicos para su optimización. La arquitectura cerrada del OEM condiciona el acceso a los datos e impone barreras para reutilizarlos. Esto somete a debate si el titular de los derechos sobre los datos debería ser quien los capta o quien opera el equipo, o quien lo diseñó y controla su infraestructura.

Cada uno de los actores en este proceso tiene demandas específicas, usos concretos y un nivel de participación diferenciada en el tratamiento de los datos. Esto implica la necesidad un régimen de gestión de datos que permita organizar cómo se acceden, comparten y utilizan los datos, en función de la participación de cada actor dentro del ciclo de procesamiento de los datos como parte de un servicio integrado para la mina. Este régimen debe establecer qué facultades o atribuciones se les otorgan a los actores para acceder a los datos, de acuerdo con su nivel de intervención en el proceso.

Para fines didácticos, un OEM fabricante de camiones semi-autónomos posee sensores embebidos, sistemas de navegación y una plataforma cerrada que recopila y analiza datos operativos del camión mismo (velocidad, niveles de combustible, tiempos de actividad). Por su parte, un proveedor tecnológico independiente ofrece un sistema de gestión de flota con capacidad para integrar y visualizar los datos de múltiples fuentes, incluyendo los equipos del OEM, a fin de coordinar tiempos, predecir mantenimiento, pero la clave está en la centralización de los datos.

El sistema de gestión de flota necesita acceder a los datos generados por los sensores integrados en los camiones del OEM a fin de obtener información integral sobre la flota de la mina y tomar decisiones de manera eficiente. Sin embargo, el OEM argumenta que estos no pueden ser compartidos o limitar la calidad de los datos que comparte y hacer menos eficiente la operación, más aún porque podría existir competencia en el sistema de navegación interna de los camiones del OEM. Incluso podría argumentar control exclusivo en virtud de cláusulas contractuales de licencia de uso o confidencialidad, limitando el acceso a su API e imponer tarifas adicionales a la interoperabilidad.

Para el OEM, sigue siendo un riesgo el crear una puerta de acceso a los datos a otros proveedores que ofrecen tecnologías similares, por lo que restringir el acceso es un mecanismo de defensa de sus intereses respecto al control sobre su activo estratégico principal. Los riesgos sobre la propiedad intelectual y la competencia desleal se constituyen como amenaza si es que el sistema de navegación reemplaza sus funciones de análisis integradas a su equipo.

En este contexto, la mina se ve afectada por un conflicto de falta de integración del sistema de gestión de flota y los equipos OEM, lo cual produce un impedimento para la gestión eficiente, con información integral y centralizada, afectando su productividad operativa. Por su parte, para el proveedor tecnológico se limita su acceso libre a los datos industriales y su propuesta de valor tecnológica le impide brindar un servicio idóneo, preciso e incluso se ve impedido de cumplir con los acuerdos contractuales ofrecidos inicialmente.

A propósito de la intervención de diferentes actores en esta situación, en el *Data Act* de la Unión Europea (Reglamento (UE) 2023/285), se permite integrar normativamente las relaciones complejas que se dan en este contexto AIoT industrial. En ese enfoque, se entiende por "producto conectado" a todo equipo físico dotado de sensores o componentes que capturan, procesan y transmiten datos relativos a su funcionamiento o a su entorno operativo.

La definición es relevante para el análisis jurídico y la respuesta al debate sobre los derechos de los datos generados en la interacción de múltiples actores:

> "*Un bien que **obtiene, genera, o recoge datos** relativos a su uso o entorno y que puede comunicar datos del producto a través de un servicio de comunicaciones electrónicas, una conexión física o un acceso en el dispositivo y cuya función primaria no es el almacenamiento, el tratamiento ni la transmisión de datos en nombre de alguien que no sea el usuario*" (Data Act, 2023). (Énfasis añadido).

Esta definición se aplica al AIoT, es decir, el dispositivo que recopila los datos del entorno minero, los transporta a través de redes inalámbricas, almacena y realiza procesamiento. El "fabricante del producto conectado", que hace las veces de OEM, a menudo busca mantener el control exclusivo del flujo de datos que su maquinaria genera. Sin embargo, el Data Act también

establece que el usuario del producto conectado tiene derecho a acceder a estos, y si lo desea, podrá compartirlo con terceros proveedores, incluso si no son parte del ecosistema del OEM.

Establecer estas disposiciones refuerza la concepción que busca un manejo funcional de los datos donde su flujo y aprovechamiento no dependen exclusivamente de una voluntad, sino se centra en la utilidad que tiene el dato para generar valor en todo el contexto industrial. De este modo, considero que esta normativa permite interpretar los conceptos en los contextos complejos entre las relaciones de OEM, clientes, proveedores de tecnología y terceros a partir de un enfoque de acceso, innovación y gobernanza de los datos.

No obstante, aun cuando esta regulación establece reglas más claras sobre ciertas tensiones entre las relaciones, como aquellas derivadas del acceso y reutilización de datos, los retos normativos, contractuales y relaciones institucionales persisten. Subsiste la duda si este es el mejor modelo, o se debe replantear el otorgamiento de derechos y obligaciones sobre los datos, considerando el tipo de figura jurídica que se debe adoptar, a qué necesidad se debe atender y qué aspectos se deben proteger en esta relación en base a la naturaleza del bien.

El régimen vigente puede que no haya resuelto la asimetría entre los sujetos intervinientes, sea porque se encuentran en diferentes posiciones de poder para la negociación o porque no existe un marco normativo robusto que permita abordar riesgos derivados de las barreras técnicas al acceso. En consecuencia, si identificar a los sujetos intervinientes es un paso adicional para la gobernanza de los datos, aún está pendiente determinar qué modelo es el más adecuado para garantizar un equilibrio y justo acceso, compartición y reutilización de los datos no personales.

Este panorama podría requerir la creación de un nuevo marco regulatorio especializado que garantice derechos de quienes invierten en la innovación tecnológica y que prevea mecanismos de balance de derechos que den lugar a una protección adecuada de los datos generados y, a su vez, estableciendo cimientos para una cooperación hacia la gobernanza de los datos en espacios industriales.

5. El tratamiento de los datos no personales y la interoperabilidad en el sector minero

La transformación digital de la industria minera lleva un proceso sostenido impulsado por la incorporación de tecnologías emergentes como el AIoT. Estas tecnologías permiten capturar un

amplio volumen de datos no personales, que son esenciales para optimizar las operaciones mineras. El presente trabajo busca abordar cómo se gestionan estos datos en el contexto minero, enfocándose en los desafíos técnicos y normativos vinculados a la interoperabilidad tecnológica entre sistemas, la gobernanza de los datos y el equilibrio entre los intereses empresariales y el bien común en relaciones B2B.

El uso de los datos no personales en la industria minera se enfoca en la recolección de datos como parte de un proceso de sensorización generados a través de la infraestructura tecnológica aplicable a un proceso minero (como producción, extracción y transporte del mineral). Estos datos pueden estar relacionados al volumen de material que extrae una máquina, la ubicación en tiempo real de la maquinaria dentro de la mina, los niveles de carga de una pala, las dimensiones de los materiales que se dirigen al proceso de chancado, el número de ciclos de carga que registra una pala, el tipo y características generales del material, entre otros.

Los datos no personales permiten una representación objetiva y cuantificada de las operaciones mineras, lo que hace posible el análisis sistematizado de las condiciones de la operación, a fin de optimizar o hacer más eficiente el proceso en sí. Este análisis en tiempo real provee a los operadores y a los centros de operación de información suficiente, actualizada y real, necesaria para la toma de decisiones eficientes basadas en estadísticas o evidencia.

La gestión de los datos puede influir directamente en el volumen de la producción diaria y en la optimización de procesos, como el filtrado o procesamiento del mineral, lo cual se ve reflejado en los niveles de producción y distribución de los minerales a través de la eficiencia que el análisis de datos y de la disponibilidad de la información les provee. Además, en el ámbito del mantenimiento predictivo, es posible contribuir a la mejora del rendimiento de los activos mineros, a fin de prolongar su vida de uso y evitar posibles daños que suelen implicar grandes costos.

A su vez, al automatizar tareas que antes realizaban los operarios mineros, el uso de datos no personales en tiempo real elimina imprecisiones y aparece información que es difícil de percibir debido a las condiciones de la mina y, en consecuencia, busca evitar diferentes riesgos. Esto convierte al AIoT en una herramienta crucial para transformar los resultados de la mina, haciendo sus procesos más seguros y eficientes.

En ese sentido, Corrado et al. afirman que la acumulación de estos datos en una economía tiene el potencial de impulsar la producción, pero solo en la medida que se invierta en su transformación, junto con otra información económica, social o técnica disponible, para analizarla y generar conocimiento que pueda aplicarse efectivamente a un sector o negocio específico (2022). Esto sucede en la industria minera, se transforman los procesos manuales con la implementación de sistemas innovadores como el AIoT para brindar soporte en la toma de decisiones y la optimización de sus operaciones como planificación correctiva, mantenimiento predictivo y monitoreo y prevención de riesgos de seguridad.

Si bien es cierto que las diferentes soluciones que se encuentran en el mercado están diversificadas en uno o varios procesos mineros, considerando la amplitud de la cadena de valor de estos, existen soluciones a la medida para cada uno y ello no siempre resulta de la uniformidad de soluciones o la concentración de un solo producto tecnológico. La variedad de actores tanto como la variedad de procesos hace heterogénea la transformación digital de los procesos mineros y con ella, la intervención de múltiples actores.

Por ello, es indispensable contar con tecnologías adaptables e interoperables, capaces de integrarse con otros sistemas sin generar barreras técnicas. Esto permite un desarrollo más armónico del entorno industrial, evita fragmentaciones tecnológicas y promueve un ecosistema que favorece la innovación y acelera el proceso de transformación digital creando nuevas fuentes de datos que contribuyen al mercado de datos.

Como advierte Eckardt & Kerber (2024), garantizar derechos de acceso a los datos no personales en entornos industriales es una condición necesaria a fin de evitar la fragmentación de los ecosistemas tecnológicos y resuelven problemas de interoperabilidad entre dispositivos IoT (p. 136). En consecuencia, genera un flujo eficiente de los datos que habilita servicios de valor agregado por múltiples actores.

La interoperabilidad es un concepto clave dentro de todo sistema operativo, incluso para el AIoT. Se ha adoptado como una funcionalidad de algunas tecnologías, desde la “compatibilidad” entre aplicaciones hasta la interoperabilidad entre sistemas. Estos son los objetivos que hacen más competitivos y atractivos los sistemas de AIoT en el mercado, porque cuentan con la capacidad de comunicarse y entenderse con otros sistemas, modificando pequeñas estructuras que hacen que sistemas heterogéneos puedan funcionar interconectados e intercambiar datos, incluso en tiempo real.

Amazon, una de las empresas de tecnología más grande e importante en la actualidad, define la interoperabilidad como "la capacidad de las aplicaciones y sistemas para intercambiar *datos de forma segura y automática, independientemente de los límites geográficos, políticos u organizativos*" (Página web de Amazon, s/f). Esto permite que los usuarios finales se beneficien de las ventajas que varios sistemas ofrecen cuando están conectados entre sí, superando los efectos de red o de cualquier efecto que impida usar dos o más sistemas sin barreras técnicas o realizar ajustes desproporcionados y/o dilatorios para gozar de más de un servicio en un sistema integrado.

El NIST lo define como la "*capacidad de comunicar, ejecutar programas o transferir datos entre los diversos componentes funcionales sin interrupciones, que requiere que el usuario tenga poco o ningún conocimiento de las características únicas de esos componentes*" (Hanisch et al., 2024). Es decir, que no se requiere de una comprensión total del dispositivo con el que se desea integrar para poder operar conjuntamente.

Es por este motivo que la interoperabilidad es clave para evitar ecosistemas cerrados. Permitir la integración de múltiples proveedores y plataformas fomenta la innovación. Sin esta, se generaría efectos *"lock-in*" que limitan el desarrollo de servicios complementarios. Para la autora Begoña Gonzáles, la "interoperabilidad informática" es materia de interés público porque su ausencia produce en el mercado efectos negativos que inciden directamente en la competencia del mercado, en la esfera del consumidor y en la innovación. En ese sentido, señala que desde un punto de vista económico, mientras más grande es un negocio tecnológico, más usuarios posee, creando un efecto llamado "*network effect*s" o "efectos de red" y eso determina cuando una empresa pública o no información que permite la interoperabilidad (2019).

Un claro ejemplo de los "*network effects*" es Facebook, a medida que más usuarios se unían a la plataforma, más valiosa se volvía para otros usuarios, anunciantes y desarrolladores de aplicaciones. Ello dio lugar a la creación de barreras de entrada para nuevos competidores, puesto que hacía difícil atraer a otros usuarios a otras plataformas si la mayoría ya estaba en Facebook.

Para evitar la competencia, Meta adquirió plataformas emergentes como Instagram y WhatsApp, eliminando potenciales rivales antes de desplegar su crecimiento. En 2020, la Comisión Federal de Comercio de los Estados Unidos y otros estados demandaron a Meta por prácticas anticompetitivas, argumentando que sus adquisiciones redujeron la innovación y la diversidad de

opciones para los usuarios, mostrando como los "*network effects*" refuerzan los monopolios, establecen barreras de entradas en los mercados y frenan la innovación en el mercado digital.

Por su parte, en otros sectores como el de la banca, el concepto de interoperabilidad se adopta en las transacciones interbancarias, logrando que diferentes plataformas de pago de diferentes instituciones financieras puedan comunicarse entre sí de forma eficiente. Por ejemplo, en el Perú, el organismo autónomo del Banco Central de la Reserva del Perú ha adoptado la interoperabilidad como una estrategia para realizar pagos minoristas, con el objetivo de transformar el ecosistema de pagos digitales, convirtiéndolos en más disponibles y accesibles.

Esto beneficia a los usuarios en el uso de sus aplicativos móviles o servicios que permiten realizar diferentes transacciones independientemente de la entidad financiera a la que estén asociados. Lo que se genera en los procesamientos de pago interoperables es que el pago se realice en tiempo real. Así, dispone de una solución financiera accesible y sobre todo brindando un servicio financiero que sea inclusivo, es decir que más personas puedan integrarse al sistema bancario formal.

En consecuencia, la interoperabilidad, que permite la accesibilidad de datos, genera el crecimiento en el sector, mejora el servicio brindado y hace un sistema propicio para innovar. Tomando la experiencia del sector bancario, este sistema se promueve mediante ciertas entidades autónomas que regulan el sector en particular, siendo que el artículo 3 de la Circular No. 0024-2022-BCRP, Reglamento de Interoperabilidad de los Servicios de Pago provistos por los Proveedores, Acuerdos y Sistemas de Pagos (en adelante "Reglamento de Interoperabilidad"), establece los "Principios para la Interoperabilidad", tales como la competencia, la eficiencia y la seguridad; así́ como un alto nivel de servicio.

En dicho Reglamento, la interoperabilidad se define a través de fases como *"la capacidad de un servicio de pago de permitir que sus usuarios transfieran fondos a cualquier otro usuario, independientemente de la entidad que lo regula, provea servicios a cualquier beneficiario*" (Reglamento de Interoperabilidad, 2022, art. 2).

Asimismo, este instrumento normativo adopta otros principios interesantes que deben regir este marco para la implementación de interoperabilidad:

> *"3.1 Competencia, eficiencia y seguridad: Los Servicios de Pago interoperables deben ofrecerse de manera segura y eficiente, garantizando la privacidad y la seguridad de la información y bajo condiciones de libre competencia.*
> *3.2 No discriminación y acceso justo: Está prohibida cualquier práctica discriminatoria (limitaciones al acceso, pactos o acuerdos de exclusividad que puedan limitar la interoperabilidad, entre otras) hacia cualquier Usuario y entre Entidades Reguladas.*
> *3.3 Alto nivel de servicio: La Interoperabilidad debe asegurar la alta disponibilidad y continuidad del servicio, adecuados tiempos de respuesta y cumplimiento de los* acuerdos de niveles de servicio.
> *3.6 Neutralidad tecnológica: Las Entidades Reguladas eligen sus tecnologías y las adaptan, en caso de ser necesario, para lograr la Interoperabilidad."* (Circular N.º 0024-2022-BCRP, 2022).

La circular establece la interoperabilidad como un principio rector de los sistemas de pago, sustentado en la competencia, en la inclusión, la seguridad de las transacciones y la innovación tecnológica. Se considera que, más que un requisito técnico, es un marco normativo que busca equilibrar eficiencia y la protección de los usuarios en un ecosistema digital evolutivo.

En consecuencia, en el Perú, el concepto de interoperabilidad ya ha sido adoptado e implementado en otros sectores como banca o telecomunicaciones. Si bien su aplicación al presente sector industrial no es la misma, parten del mismo presupuesto: la capacidad de diferentes sistemas, aplicaciones y dispositivos de intercambiar información y usarla de manera efectiva, segura y eficiente, sin importar el estado de su tecnología, el proveedor o la plataforma que usa.

Ello constituye un reto principal en el uso de tecnologías que permitan que un servicio público pueda ser accesible, eficiente y de calidad. Por este motivo, la interoperabilidad debe ser un fin al que deben apuntar las políticas públicas o eventuales instrumentos normativos aplicables a las industrias y a los servicios públicos. Esto generaría una mejora en la prestación de servicios digitales de las entidades públicas y privadas, estableciendo ambientes seguros a nivel competitivo, centralizando y estandarizando los datos para un aprovechamiento conjunto de tecnologías.

En el sector minero, las minas cuentan con múltiples proveedores y la adopción de nuevas soluciones en el sector tecnológico se ha vuelto tendencia. Esta diversidad puede dificultar la

implementación de nuevas tecnologías, ya sea por los costos de adaptación de la infraestructura o por la imposibilidad de centralizar la información proveniente de distintos sistemas.

Para ello, las empresas proveedoras establecen condiciones para integrarse con otros proveedores y facilitar la implementación a nivel operativo, lo cual muchas veces implica un costo adicional que es, hasta cierto punto, legítimo de exigir. Ello no significa que sea la vía ideal dentro de un contexto de innovación.

Como bien señala Molaei et al. (2020), la comunicación es fundamental en la industria minera, ya que afecta tanto a la producción como a la seguridad en las operaciones. Así, la transferencia de datos entre el personal y la recopilación de datos de las máquinas, tanto en minas a cielo abierto como subterráneas, se debe adaptar a entornos digitales que hacen más precisa y segura la forma de comunicarse. Esto ha reemplazado el uso de radios tradicionales, con tecnologías más avanzadas como sensores, geolocalización, detección facial o el uso de indumentaria inteligente (cascos, clips, etc.).

En términos más concretos, las interrelaciones son comunes entre los proveedores de sistemas tecnológicos que usan diversos módulos y que no pueden ser visibles en una sola vía o plataforma. Una integración permitiría centralizar la información en un único dispositivo y mediante una interfaz única, se integren y se hacen visibles, adaptándose a la infraestructura existente, evitando cruces de información o desorganización y costos adicionales innecesarios.

Para contrarrestar dicha situación, las integraciones tecnológicas de los componentes son necesarias para asegurar una operación fluida y eficiente. Sin embargo, aún persisten desafíos de interoperabilidad técnica pero también comercial o contractual, que requieren acuerdos claros para garantizar la eficacia de este proceso. En este contexto, el principal interesado es el usuario final, es decir, la mina, quien se beneficiaría finalmente de los diferentes sistemas.

Esta situación adquiere una particular relevancia en el contexto del AIoT, ya que múltiples dispositivos fabricados por diferentes proveedores deben ser compatibles para funcionar conjuntamente. A nivel técnico, esto implica que los sistemas hablen “el mismo idioma”. A nivel legal, es necesario que existan acuerdos entre los fabricantes, proveedores y usuarios finales, que garanticen una colaboración eficiente, sin infringir derechos de propiedad intelectual ni

estipulan condiciones que creen barreras tecnológicas o posiciones dominantes que afecten la innovación.

Pensemos en el sistema de gestión de flota (SGF), un dispositivo que mide las condiciones ambientales y otro que mide los niveles de extracción de mineral, cada uno perteneciente a proveedores distintos. El proveedor del sistema ambiental tiene sensores de temperatura, el proveedor de la maquinaria, instala equipos para medir vibraciones y, el tercero, proporciona plataformas de almacenamiento en la nube. En este escenario, la interoperabilidad es esencial para que los sistemas compartan datos de manera centralizada. Si no se asegura esta compatibilidad, la operación se vería afectada y la gestión de la mina se complicaría.

Un artículo de Deloitte indica que a pesar de los avances en diferentes aspectos del IoT, el panorama general aún evidencia numerosos ecosistemas cerrados y patentados, lo que representa un desafío adicional cuando se trata de sistemas heredados o tecnologías antiguas, con distintas arquitecturas de datos y sensores que pueden usar diferentes formatos y protocolos de comunicación, lo que se traduce en que “hablan diferentes idiomas” (Chui Michael et al., 2021).

En la era de la Industria 4.0, donde el AIoT se ha convertido en uno de los instrumentos más disruptivos y de gran utilidad, estos se conectan a redes alámbricas o inalámbricas, lo que implica que los dispositivos no sean aislados, sino que dependen de su interconectividad y de la posibilidad de integrarse con otros dispositivos similares o que puedan relacionarse con servicios complementarios sobre los datos generados en la minería (Drexl, 2018), dando como resultado estructuras menos complejas y centralizada.

Sin embargo, aún existen desafíos para lograr la interconectividad efectiva de los dispositivos AIoT, debido a la fragmentación de los mercados tecnológicos y, consecuentemente, de los datos. La tendencia por crear efectos de bloqueos de los datos bajo un discurso de protección de datos no personales como derechos de propiedad genera problemas para establecer estándares de interoperabilidad. Aun así, la ausencia de regulación ha determinado que los mismos actores encuentren oportunidades de negocio en la disponibilidad de datos y monetizar la interoperabilidad como un servicio adicional.

En la industria minera, el AIoT puede estar dirigido a la flota minera, permitiendo un monitoreo en tiempo real y con alta precisión. En este contexto, quien tiene un acceso total a los datos generados es quien fabrica el AIoT, en otras palabras, mantiene la “posesión” de los datos por *default*. Los distintos modelos de negocio pueden influir en la negociación de la disponibilidad de datos, ya que los estándares y protocolos pueden variar entre dispositivos, lo que genera riesgos en brechas a nivel de integración técnica y a su vez, sobre la seguridad.

A pesar del avance de la digitalización como parte del proceso de transformación industrial, el sector minero enfrenta también esa fase de transición tecnológica. Gran parte de los activos mineros, particularmente, la maquinaria utilizada para las operaciones, no disponen de capacidades de conectividad ni de sistemas de gestión integrados. En razón a los altos costos que supondría la renovación por completo de la flota minera, las empresas orientan sus esfuerzos hacia la adopción progresiva de los equipos inteligentes y por lo pronto, adaptan sus equipos existentes, incorporando tecnologías que posibiliten la recolección, transmisión y análisis de datos operativos.

No obstante, la transformación digital de la maquinaria introduce una discusión jurídica y económica compleja que se relaciona al acceso a los datos generados durante su operación. Los fabricantes de equipos poseen, por lo general, un control directo sobre los datos que genera la maquinaria, aprovechando su posición en la cadena de valor para la imposición de condiciones restrictivas a los proveedore que buscan interoperar o desarrollar soluciones complementarias. Esta situación configura una asimetría típica de las relaciones B2B y que, en este contexto, se acentúa en los datos como eje estratégico en el entorno AIoT.

El procesamiento de datos en la digitalización minera no solo tiene implicancias económicas, sino también jurídicas y técnicas, pues su eficacia depende del tipo de datos que se generan, de la disponibilidad de estos y las condiciones de uso impuestas por los actores involucrados. Los sujetos intervinientes en esta relación establecen pautas de quién, cómo y cuándo puede darse tratamiento a los datos y de esta capacidad reside un derecho de uso (que se autodetermina sui generis). Ejercer este “auto derecho” conlleva tambien a restricciones que se basan en argumentos de protección de propiedad intelectual o la integridad y seguridad de los sistemas, pero en la práctica refuerzan esquemas cerrados, límites a la competencia en los servicios de valor añadido y por supuesto, representa un obstáculo a la innovación en minería.

En la actualidad, las grandes empresas se atribuyen “de facto” la propiedad de los datos que generan o utilizan a través de sus tecnologías, restringiendo deliberadamente el acceso a esos datos por parte de terceros. Esta práctica se adopta como una respuesta a una posible amenaza para su posición competitiva y su capital en el mercado. Por ello, es fundamental establecer límites claros y considerar marcos legales adecuados que promuevan el acceso responsable y equitativo a los datos no personales, mediante un análisis económico que equilibre los intereses empresariales con el avance del sector.

Adoptar los estándares de interoperabilidad implica la aprehensión de 3 enfoques que predominan la economía digital de hoy: El *Data Drive*n, *Data Trust* y el *Open Data*. El enfoque *Data-Driven* implica que las decisiones, estrategias y operaciones de una empresa estén basadas en datos generados, recopilados y analizados para maximizar el valor de sus actividades empresariales. Los dispositivos AIoT generan grandes volúmenes de datos no personales que impulsan procesos como el mantenimiento predictivo y mejora la eficiencia operativa. En relaciones B2B, estos datos permiten a empresas mineras y tecnológicas desarrollar modelos predictivos, soluciones personalizadas y análisis adaptados a necesidades específicas.

Por otro lado, el *Data Trust* se presenta como una entidad neutral que gestiona los datos en beneficio de un grupo de partes interesadas, garantizando el acceso equitativo, la seguridad y el cumplimiento de acuerdos legales y éticos. Estas entidades pueden actuar como intermediarias para gestionar los derechos de acceso y uso de datos generados por dispositivos AIoT, asegurando que todas las partes tengan acceso justo sin comprometer la confidencialidad ni la propiedad intelectual. En contextos B2B, estos *Data Trusts* pueden administrar datos generados por dispositivos en operaciones mineras, distribuyéndolos entre fabricantes y usuarios bajo términos claros y equilibrados.

Y por último, el *Open Data* implica disponibilidad de datos para cualquier persona, generalmente bajo licencias que permiten su acceso, uso y reutilización sin restricciones significativas. En sectores como la minería, los datos no personales relacionados con emisiones, eficiencia energética o rendimiento podrían publicarse como parte de este modelo a fin de fomentar la innovación y el desarrollo de soluciones colaborativas.

Aunque no todos los datos generados en relaciones B2B pueden ser abiertos, compartir conjuntos de datos no sensibles puede generar beneficios sociales y económicos más amplios.

Algunos principios regulan los datos no personales en AIoT basados en los lineamientos de la *Open Data Chart* (ODC) y algunas disposiciones desarrolladas de la OECD, las cuales se basan en los siguientes:

- Transparencia y Acceso Justo**:** Los *data trusts* deben asegurar que todas las partes involucradas tengan igualdad de acceso a los datos no personales, estableciendo mecanismos efectivos para resolver conflictos relacionados con su uso.
- Fomento de la Innovación: Es fundamental aplicar el concepto de *open data* a datos no sensibles, como aquellos vinculados a la sostenibilidad, para permitir que terceros desarrollen soluciones innovadoras que beneficien al sector y a la sociedad en general.
- Seguridad y Responsabilidad: Los *data trusts* deben operar bajo estrictos estándares de seguridad, protegiendo la confidencialidad de los datos y asegurando que su acceso y uso cumpla con los acuerdos establecidos y las regulaciones aplicables.
- Optimización del valor de los datos: Las empresas deben adoptar un enfoque basado en datos (*data-driven*) que impulse la colaboración, optimice procesos y maximice el valor generado a lo largo de toda la cadena B2B.
- Flexibilización normativa**:** Es necesario permitir que las partes negocien acuerdos contractuales personalizados dentro de un marco regulatorio que promueva la interoperabilidad, el acceso equitativo y un equilibrio de derechos entre usuarios y fabricantes. (OECD, 2015)

Contar con estos 3 enfoques nos permite no solo adoptar los mecanismos de seguridad que la interoperabilidad implica, sino que además nos permite ser conscientes de la importancia económica de los datos al momento de crear integraciones con otros sistemas sin que ello constituya un conflicto entre las relaciones del usuario-proveedor o proveedor-proveedor cuando los datos no personales les permiten ser más competitivos en el mercado.

También en los entornos industriales, la interoperabilidad es crucial para que los datos estén integrados y permita maximizar su valor a quien implementa tecnologías. Asimismo, disuade el efecto de bloqueo de datos que se mantienen centralizados en un solo proveedor, fomenta el acceso a otros agentes interesados y crea un ecosistema dinámico enfocado en la innovación.

En suma, los datos no personales generados por tecnologías AIoT en la minería constituyen un activo estratégico cuya interoperabilidad técnica y legal resulta esencial para garantizar eficiencia operativa, innovación y un ecosistema competitivo. Superar las actuales limitaciones de acceso

y control exige marcos normativos equilibrados, estándares abiertos y estructuras contractuales que reconozcan el valor compartido del dato en contextos B2B. El reto actual no es solo tecnológico, sino también jurídico y económico: diseñar mecanismos que distribuyan los beneficios de los datos no personales sin desincentivar la inversión ni consolidar posiciones dominantes

5.1. Regulación sobre los datos personales en el uso de AIoT

Díaz Vera sostiene que, para que la economía digital continúe expandiéndose en la región, es fundamental garantizar el acceso de las empresas a los datos en general, no solo a los datos personales, sino también, con especial énfasis, a los datos no personales, como una forma de fomentar el desarrollo de la industria digital (2023). Sin embargo, durante un largo período y en muchas legislaciones, la regulación de los datos se ha centrado predominantemente en los datos personales, es decir, en información que identifica o puede identificar a una persona física. Esto ha dejado de lado el potencial económico que los datos no personales representan para diversas industrias.

Es necesario analizar el aporte que la regulación de los datos personales puede ofrecer a la creación de un marco regulatorio sobre datos no personales. Aunque la regulación actual se limita a los datos personales, no excluye aquellos datos no personales que puedan asociarse indirectamente a una persona. En tal caso, que no es objeto de análisis en este trabajo, los datos no personales recopilados a través de sensores, cámaras u otros dispositivos podrían combinarse con otros datos para identificar a individuos. Cuando esto ocurre, las leyes de protección de datos personales resultan aplicables, delimitando con claridad su ámbito de aplicación para evitar un uso indebido de la regulación de los datos no personales.

En el Perú, la regulación se ha enfocado a desarrollar las formas de tratamiento de los datos personales previsto en la LPDP y su Reglamento. Esta normativa garantiza los derechos que protegen a los titulares de los datos y establece las condiciones del tratamiento de sus datos, un derecho de rango constitucional reconocido en el artículo 2, numeral 6, de la Constitución Política del Perú. Su objetivo es asegurar un tratamiento adecuado de los datos, en concordancia con otros derechos fundamentales, como la privacidad, la intimidad, el honor y la no discriminación, entre otros.

No obstante, esta ley en específico señala que el tratamiento refiere a:

> "*Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales*" (Ley N.º 29733, 2011, art. 2.19).

Aunque no se hace una referencia explícita al uso de tecnologías emergentes en concreto, la LPDP incluye especificaciones sobre la gestión de datos generados por dispositivos de AIoT, que implican procesos de automatización. Esto permite regular cómo las empresas acceden y utilizan los datos. Asimismo, se debe destacar la capacidad de adaptación de la ley frente a la evolución tecnológica, lo que incluye técnicas de tratamiento basadas en inteligencia artificial u otras herramientas emergentes. De este modo, se busca garantizar un tratamiento de datos seguro, transparente y conforme a los requisitos legales, tanto en bancos de datos privados como en la administración pública.

Un aspecto relevante es que, aunque algunas regulaciones pueden precisar de manera explícita el uso de tecnologías en específico y otras se derivan de su interpretación, el objetivo principal debe ser la protección y garantía de los derechos de las personas respecto de cómo sus datos son utilizados por terceros. Este principio debería extenderse también a los datos no personales

Por último, la LPDP no establece ninguna definición respecto de los datos no personales. Sin embargo, establece el concepto de los datos anonimizados a través de la definición del proceso de "anonimización" el cual refiere a "*el tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible".* Al respecto, este concepto es importante pues determina en qué medida los datos personales se desprende del elemento subjetivo y habilita su tratamiento sin consentimiento, pero a pesar de ello, la ley exige que la técnica que se utilice para este proceso, no sea reversible, de lo contrario, retoma el ámbito de aplicación de este.

Como se ha precisado, un dato personal que pasa por un proceso de anonimización excede el ámbito de aplicación de la normativa de datos personales. Sin perjuicio de ello, los datos no personales se generan sin el elemento subjetivo, por lo que es necesario determinar si los datos anonimizados son datos personales que se convierten en datos no personales mediante un

proceso de anonimización y si estos pueden se les aplica una eventual normativa de los datos no personales en la medida que su reidentificación sea técnicamente imposible.

En consecuencia, la ausencia de regulación sobre los datos no personales a pesar de su importancia en la economía digital, evidencia un vacío normativo que debe ser atendido a nivel nacional y regional. Es fundamental desarrollar un marco que fomente el uso de los datos no personales con fines de innovación, de manera que también proporcione seguridad jurídica a los agentes económicos que rentabilicen el tratamiento de los datos y que este no suponga infringir disposiciones normativas ni exponerse innecesariamente a multas.

5.2. Regulación sobre los datos no personales en el uso de AIoT

La ausencia de regulación sobre el uso, acceso y compartición de los datos no personales representa un desafío que ha sido postergado durante mucho tiempo, a pesar de los beneficios que estos datos representan en la economía digital actual. Esta carencia normativa no solo afecta el desarrollo económico - tecnológico, sino también a diversos sectores industriales, incluyendo al sector público, donde los datos tienen un gran potencial para generar bienestar común, especialmente reflejado en la disponibilidad de información de calidad para mejorar los servicios públicos, pero también privados.

La importancia de regular cómo se comparten los datos no personales radica no solo en su potencial valor económico, sino también en los efectos que su tratamiento puede tener en las personas, de forma directa o indirecta. Es pertinente cuestionarnos si el impacto es comparable con el que se genera sobre los datos personales y qué otros derechos podrían estar involucrados en el tratamiento de los datos no personales. Esto incluye considerar si existen afectaciones adicionales más allá de frenar la innovación tecnológica.

Si la definición de datos no personales queda fuera del ámbito de aplicación de la Ley de Protección de Datos Personales (LPDP), surge la interrogante sobre qué reglas deben aplicarse en casos donde, debido al alto valor económico de estos datos, se pretendan atribuir derechos sobre ellos, aún en ausencia de disposiciones normativas específicas. Este vacío puede derivar en conflictos entre empresas o usuarios, dependiendo de si el uso de tecnologías AIoT se desarrolla en el contexto de relaciones empresariales B2B o B2C.

Una regulación específica sobre datos no personales debería centrarse en cuatro ejes principales. En primer lugar, debe establecerse un marco que permita identificar los impactos directos e indirectos sobre los derechos fundamentales, para determinar si es posible aplicar las disposiciones de la LPDP o es necesario crear marco específico para datos no personales. En segundo lugar, dado que los datos son un recurso clave para la innovación (como el entrenamiento de sistemas de IA), deben delimitarse claramente aspectos como la titularidad de los derechos de uso, acceso y compartición, evitando así desincentivos que frenen la inversión tecnológica.

En tercer lugar, la regulación debe abordar escenarios complejos donde la ausencia de una regulación haya generado conflictos entre los actores involucrados, obstaculizando el avance en el desarrollo tecnológico. Finalmente, se debe procurar que la regulación de datos no personales se complemente con principios establecidos en la LPDP, sin comprometer derechos fundamentales pero equilibrándolos, permitiendo un desarrollo tecnológico sostenible.

No obstante los desafíos normativos, existen algunos marcos regulatorios que acompañan el proceso de transformación digital dentro de los órganos del Estado, que podrían tomarse como punto de partida para iniciativas frente a los datos no personales en el uso industrial. Por ejemplo, el Decreto Legislativo No. 1412, Ley de Gobierno Digital y su reglamento aprobado por Decreto Supremo No. 029-2021-PCM es una norma que promueve un marco de fobernanza para la adecuada gestión de la interoperabilidad, compartición de datos entre entidades públicas, y la gestión del dato como activo estratégico del Estado en la digitalización de procesos y prestación de servicios digitales.

Si bien esta norma no distingue expresamente entre datos personales y no personales y su ámbito de aplicación se limita a la Administración Pública, su impulso a plataformas interoperables, servicios digitales y arquitectura de datos abiertos sirve de base para establecer criterios funcionales en la gestión y reutilización de datos no personales de calidad, especialmente porque reconoce su valor económico y su impacto social en su reutilización.

De igual modo, el Decreto Supremo No. 085-2023-PCM, Política de Transformación Digital al 2030 aplicable a la administración pública, es otro instrumento que establece objetivos estratégicos para el desarrollo de un gobierno y una economía digital que prevea la digitalización de los servicios públicos y privados a través del de tecnología emergentes y de datos. Esta política reconoce como tal el valor de los datos y su importancia en la innovación y el desarrollo

económico. Para ello, busca el fomento de creación de normas e instituciones para la gestión segura (Confianza Digital) y ética de los datos, bajo entornos interoperables que puedan contribuir al desarrollo tecnológico.

Además, un panorama optimista se desarrolla en la publicación del Documento de Trabajo de la Estrategia Nacional de Gobernanza de Datos 2026-2030, el cual introduce de manera solo enunciativa el concepto de "datos no personales". Este documento establece en el punto 5.1. y 6, como parte del fortalecimiento del marco normativo de la gobernanza de datos, el "*desarrollar y/o actualizar el marco normativo nacional para acceso, uso, intercambio y protección de datos (personales, no personales, sensibles)*" y se contempla tanto como objetivo como un factor a implementar entre el año 2026 y 2027 (2025).

Una primera lectura de este objetivo evidencia la intención de establecer mecanismos de protección para los datos no personales en la gobernanza de datos, lo cual podría constituir una restricción de la innovación si es que no se definen bien los conceptos, el régimen sujeto a los datos no personales y la forma de compartir y acceder a estos.

La entrada en vigencia del Reglamento de la Ley que promueve el uso de la inteligencia artificial a favor del desarrollo económico y social del país mediante Decreto Supremo Nº 115-2025-PCM (en adelante, "Reglamento de la IA"), introduce cuestiones especiales respecto a la promoción de la IA. Cabe resaltar que para el desarrollo de estos sistemas "basados en IA" (como lo desarrolla este reglamento), es necesario el uso de datos, pero no cualquier dato, sino datos de calidad.

Para que una IA sea ética y responsable, es relevante que la fase de entrenamiento de los modelos prevea datos de calidad, que sean exactos, confiables y legítimos. La UNESCO, como parte de sus recomendaciones sobre la ética de la inteligencia artificial, hace un llamado a los Estados Miembros a elaborar e implementar estrategia de gobernanza de datos que garanticen la calidad de los datos que se usen en los sistemas de IA, como una medida de seguridad y de protección de los datos (2022, p.29).

La gobernanza de datos (incluye datos personales, no personales y sensibles) es crucial no solo en el ámbito público sino también privado. No obstante, el Reglamento de la IA ha declarado como una obligación de las entidades públicas, que estos puedan poner a disposición datos de "alto valor" a través del Centro Nacional de Datos a fin de establecer, transparencia y fomentar

entornos más abiertos en relación a los datos. Eso asegura la participación del Estado en la creación de un marco de gobernanza conjunta y abierta y en la disponibilidad de datos de calidad, ambas como parte de un proceso de innovación responsable y de aporte común.

Las industrias como la manufactura y la minería dependen de los datos no personales para el entrenamiento de los sistemas AIoT, pero no cuenten con reglas claras ni específicas sobre cómo deben interactuar los agentes que utilizan tecnologías emergentes y que necesitan integrarse y, eventualmente, acceder a los datos que recopilan los dispositivos. En este caso, los sistemas de gestión abierta no son obligatorios porque se manejan en entornos “cerrados” o “privados”, lo cual puede constituir riesgos en la innovación responsable. Otras industrias han regulado la materia de manera indirecta y tomando decisiones en base a ciertos fines como el de la interoperabilidad en el sector financiero o el de portabilidad en el sector telecomunicaciones.

De igual modo estas políticas, proporcionan elementos clave para la contribución de un desarrollo normativo en materia de datos no personales, pero incorporando componentes esenciales como la gobernanza de datos bajo un esquema de confianza, la interoperabilidad y los datos abiertos. Estos tres conceptos aportan en la disponibilidad de datos de calidad (idealmente en sectores públicos pero también privados), apertura técnica en la reutilización de los datos e incentivos a la innovación tecnológica. Establecer un marco de apertura y equilibrio impulsa la generación de datos de diversas fuentes, lo que enriquece el ecosistema de los datos y los pone a disposición común.

6. Regulación comparada europea sobre datos no personales

La Unión Europea es una de las instituciones que de manera proactiva y decisiva, ha regulado el tema de los datos no personales, especialmente para promover la interoperabilidad, facilitar su uso en la creación de nuevas tecnologías y regular los flujos transfronterizos entre los países miembros.

En los últimos años, la Unión Europea ha identificado la necesidad de debatir e implementar una serie de regulaciones relacionadas con el mercado de los datos y la economía digital que hoy en día rigen en los mercados nacionales e internacionales. Estas regulaciones también consideran nuevas formas de comercio, marketing y otras prácticas económicas basadas en el uso de tecnologías emergentes. Sin embargo, su uso porta consigo riesgos significativos que han requerido de regulación para mitigar los impactos negativos y proteger a los usuarios, desde perspectivas civiles, de derechos del consumidor, propiedad intelectual y derechos humanos.

6.1. Ley de Datos (Data Act)

Propuesta en el año 2020 y con entrada en vigor en enero del 2024, la UE ha creado un dispositivo legal que representa el pilar de la estrategia para la gobernanza de los datos en el sector de los “productos conectados” o Internet de las cosas. Hoy en día, solo los fabricantes de ciertos productos como los autos, robots o maquinaria en sí, pueden acceder a los datos y no existe otra alternativa más que acudir a ellos mismos para obtener un tipo de servicio respecto al producto conectado.

Por otro lado, se ha determinado que el *Data Act* aporta en 3 aspectos importantes: produce precios más bajos, nuevas oportunidades en el uso de servicios que recaen en el acceso a los datos y mejor acceso a recolección o producción de datos por dispositivos. Algunos sectores industriales suelen caracterizarse por contar con diversidad de proveedores y es común que los usuarios no puedan encargar el análisis de los datos generados de los dispositivos de sus múltiples proveedores a terceros (sobre maquinaria, por ejemplo), porque los datos están protegidos o bloqueados por los fabricantes de un producto.

Además, en el caso de una mina que utiliza maquinaria pesada con sensores para poder monitorear el rendimiento, estos equipos generan datos importantes para saber el estado de la máquina como tiempos de inactividad, consumo de combustible, estado del motor, entre otros, pero solo el fabricante de la maquinaria tiene acceso de manera exclusiva porque los almacena en sus servidores donde solo algunos tienen acceso, en ocasiones bajo un servicio pagado para el usuario.

Esto limita la forma en cómo la mina podría analizar tales datos de forma conjunta y centralizada para poder tomar decisiones de manera rápida respecto a los equipos. El *Data Act* permite que la mina pueda acceder de manera directa a los datos de su maquinaria y eventualmente compartirla con terceros, facilitando la competencia en mercados complementarios.

Asimismo, en un contexto donde la Unión Europea busca crear un entorno digital basado en datos abiertos, en el que tanto los ciudadanos como las empresas puedan beneficiarse de estos, persisten desafíos importantes. El marco jurídico actual no aborda de manera suficiente todas las cuestiones relacionadas con los datos, y los agentes involucrados en la cadena de valor de estos carecen de certeza sobre la propiedad de los datos que han recopilado. Por ello, en el caso

de productos analizados, enriquecidos o transformados de cualquier otra manera, se concluye que es necesaria una solución más sólida y jurídicamente segura (Van Asbroeck et al., 2017).

El Data Act de la Unión Europea es una propuesta regulatoria diseñada para establecer reglas claras en la utilización e intercambio de datos no personales. Su objetivo principal es garantizar que los datos generados en entornos empresariales y por dispositivos de IoT puedan aprovecharse de manera equitativa y eficiente, fomentando la interoperabilidad y el desarrollo tecnológico. Según Atik (2020), esta normativa introduce mecanismos que facilitan el acceso a datos entre empresas (B2B) y entre empresas y gobiernos (B2G), promoviendo un ecosistema de datos abierto que fomente la innovación sin comprometer la competencia.

Este instrumento regula además diversos aspectos claves. En primer lugar, otorga derechos a los usuarios para acceder y utilizar los datos generados por productos IoT en relaciones B2C y B2B, incluyendo la posibilidad de compartirlos con terceros. En segundo lugar, evalúa la equidad de las cláusulas contractuales en acuerdos B2B sobre el intercambio de datos, especialmente en contratos con PYMEs.

En tercer lugar, aborda situaciones excepcionales dentro del intercambio de datos B2G. En cuarto lugar, regula el intercambio de datos entre proveedores de servicios en la nube. Por último, establece garantías frente al acceso ilícito a datos no personales en un contexto internacional, protegiendo los intereses de la Unión Europea.

El Data Act no solo busca establecer reglas claras para el acceso y uso de los datos no personales, sino también abordar las desigualdades generadas por posiciones dominantes en el control de datos dentro de sectores clave. La regulación tiene como objetivo garantizar un acceso más equitativo a los datos, fomentando la innovación y la competencia en sectores donde los datos juegan un papel crucial para la eficacia operativa y la toma de decisiones.

Un ejemplo claro de esta problemática es la preocupación por los servicios de reparación y mantenimiento como servicios complementarios, por ejemplo, el de la maquinaria en las minas. Los fabricantes de maquinaria pesada de minas han diseñado sus coches de tal manera que los datos generados se transmiten directamente a servidores propios. Ni los propietarios de aquella maquinaria ni otras empresas pueden acceder a estos datos sin el permiso de los fabricantes. Esta situación ha desencadenado un debate político en la Unión Europea sobre la necesidad de

regular el acceso a los datos para proteger la competencia y la innovación en mercados clave como el de la maquinaria pesada.

Es decir, en el sector minero, esto se traduce en equipos que, con ayuda de sensores, monitorean parámetros como tiempos de inactividad, consumo de combustible, estado del motor, entre otros. Sin embargo, dado que los datos son almacenados exclusivamente por el fabricante de la maquinaria, las minas ven limitadas sus capacidades para usar o disponer de tales datos a través de la adquisición de servicios de terceros para monitorear o centralizar los datos de todas sus maquinarias que podría pertenecer a diferentes proveedores. Esto limita la forma en cómo la mina podría analizar tales datos de forma conjunta y centralizada para poder tomar decisiones de manera rápida respecto a los equipos.

En este último caso, los fabricantes de vehículos tienen un control exclusivo sobre los datos que se generan por los coches conectados, lo que dificulta el acceso sin autorización previa, incluso de los propietarios. Esta posición de dominio sobre los datos se ha hecho llamar como "gatekeeper" (guardián) en la legislación de la UE, la cual ha generado medidas para mitigar el impacto negativo en la competencia y la innovación en el sector automovilístico.

El Data Act aborda estos problemas especialmente regulando el sector del IoT, reconociendo que el acceso restringido puede limitar el acceso directo a los datos de su maquinaria, y lo empodera a compartir con terceros, para acceder a ellos y facilitar la competencia y la oferta de servicios complementarios innovadores.

Este dispositivo jurídico europeo también se preocupa por el impacto negativo sobre los usuarios, debido a la menor capacidad de elección entre servicios, menor innovación en el sector y precios más altos en los mercados secundarios. Además, surgen serios problemas con respecto a la distribución justa del valor de los datos generados por el IoT, desde un enfoque centrado en los usuarios, empodera a estos otorgando mayor control sobre sus datos y asegura una distribución más equitativa y equilibrada del valor potencial que los datos generan y, al mismo tiempo, mantiene los incentivos de inversión en tecnología. Fomenta también el enfoque de “datos abiertos”, que buscar dar acceso a los datos generados por dispositivos IoT para la innovación y promover el surgimiento de mercados secundarios como de mantenimiento y los nuevos servicios (Kerber, 2024).

Asimismo, entre los principales componentes del Data Act se encuentra la obligación de los proveedores de dispositivos IoT de compartir datos generados por sus dispositivos con usuarios y terceros autorizados bajo condiciones específicas. También incluye disposiciones para evitar el bloqueo de datos, conocido como "data lock-in", y garantizar la portabilidad de los datos entre servicios (Comisión Europea, 2023). Esta regulación promueve la transparencia y reduce las barreras de entrada para nuevos competidores, especialmente en sectores tecnológicos emergentes que necesitan de tales datos para hacer sus soluciones viables.

Otro punto adicional que aborda el Data Act es el fomento del intercambio de los datos con introducción de normas de interoperabilidad y otras especificaciones técnicas que permiten el acceso no solo a los datos en sí, sino que buscan formas de integración que ciertamente conforman barrera técnicas o límites para el acceso integral. En el caso de los datos personales, aún promueve el uso de normas técnicas y organizativas que sean confiables para que el nivel de anonimización sea suficiente para el tratamiento de los datos conforme la aplicación de esta norma y no la del RGPD.

A diferencia del RGPD, introduce una forma de identificar cuándo los datos que son tratados hacen referencia a datos personales y si refieren a una persona física identificable, en la medida que gran parte de los datos tratados en la economía basada en los datos se refieren (en algún momento) a una persona física identificable y, a menudo no siempre es posible distinguir los datos no personales cuando se trata de conjuntos de datos más amplios o combinados. Lo mismo se aplica a los datos generados por productos IoT, los datos de ubicación los datos de uso u otros datos pueden calificarse en muchos casos como datos personales en el sentido del RGPD y por ende, es necesario hacer una revisión del alcance y los límites para que se ajuste al objetivo del libre flujo de datos.

Por su parte, los autores Listener & Antoine señalan que el Data Act establece estructuras institucionales y descentralizadas que son comunes de los litigios de derecho privado y que consideran que también deben aplicarse para el acceso a los datos, su intercambio, su portabilidad y su utilización, superando el marco jurídico actual centrado principalmente en Gobernanza de los datos y servicios más centralizada (2022). Finalmente, es una forma de preveer un equilibrio sobre objetivos legítimos en el *Data Act* con el derecho fundamental de protección de datos personales e interpretando los respectivos puntos de legalidad del

tratamiento en el artículo 6 del RGPD de acuerdo con Obligaciones legales establecidas en el *Data Act.*

Por último, los autores Eckardt & Kerber (2024) señalan respecto al Data Act que el enfoque del proveedor de tecnología o “titular de datos” que adopta este como una extensión de derechos de propiedad intelectual, podría limitar algunos accesos legitimando el uso exclusivo de los mismos por este poseedor y terminarían siendo percibidos como los propietarios de los datos. Una posición exclusiva así es difícil de adoptar porque posee efectos negativos sobre el uso y la distribución de estos datos que, *per se*, no son rivales en su utilización. Para ello, proponen el concepto de gobernanza por un administrador de datos neutral, con el objetivo de conceder acceso a las empresas y otras entidades de acuerdo con determinados principios y condiciones de una manera no discriminatoria.

No obstante, aunque el *Data Act* busca incentivar el acceso a los datos, también plantea riesgos significativos. Uno de los principales desafíos es la posibilidad de que las disposiciones sobre el acceso obligatorio a los datos generen conflictos de propiedad intelectual entre los actores involucrados (Duch-Brown et al., 2017). Además, algunos expertos advierten sobre el riesgo de que el acceso indiscriminado a datos pueda comprometer la seguridad de la información, especialmente en sectores críticos como la salud, transporte, , donde los datos no personales también pueden ser sensibles por su contexto de uso.

El Data Act se presenta como un marco regulatorio integral que aborda la necesidad crítica de establecer reglas claras para el acceso, uso y distribución de los datos no personales en un contexto digital y económico altamente competitivo. Según el ICC Policy Primer on Non-Personal Data (2023), el Data Act contribuye a crear un mercado digital europeo más integrado, donde las empresas puedan colaborar de manera más efectiva mediante estándares comunes para el uso e intercambio de datos no personales.

La importancia de esta ley se encuentra en la capacidad para equilibrar los intereses de los usuarios, proveedores y terceros, garantizando una gobernanza de datos neutral y sostenible. Este enfoque busca prevenir la concentración de poder en ciertos actores que restringen el acceso a los datos generados, una práctica que limita la competencia y, en consecuencia, la innovación tecnológica.

En este sentido, el Data Act responde a una necesidad estratégica de fomentar un acceso equitativo a los datos, al mismo tiempo que mantiene incentivos para la inversión y el desarrollo tecnológico. Su modelo se posiciona como una referencia clave para otras jurisdicciones que deseen maximizar los beneficios de la economía digital, priorizando un justo equilibrio entre los actores implicados y promoviendo la gobernanza responsable de los datos.

No obstante, aún quedan algunos retos por superar. Por un lado el riesgo de la carga regulatoria para las pequeñas y medianas empresas, aún si se busca fomentar la inclusión y la equidad en el acceso a los datos, algunos expertos han señalado que las obligaciones impuestas por esta normativa podrían representar una carga excesiva, particularmente para este tipo de empresa.

Así también lo establece Atik (2020) argumenta que el cumplimiento de estándares de interoperabilidad y los requisitos de acceso obligatorio a datos pueden generar costos adicionales significativos para las PYMEs, quienes a menudo carecen de los recursos técnicos y financieros para ajustarse a estas exigencias. Este riesgo podría contradecir uno de los principales objetivos del Data Act: garantizar que todos los actores, independientemente de su tamaño, puedan beneficiarse equitativamente de la economía digital.

Otro reto es la excesiva protección exclusiva de los titulares de los datos. Si bien esta ley busca equilibrar el acceso a diferentes actores, podría enfocarse en los titulares de datos, es decir en las empresas que generan los datos a partir de los dispositivos AIoT. Según Duch-Brown et al. (2017), la normativa podría perpetuar desigualdades en el acceso a los datos al permitir que los data holders mantengan un control significativo sobre cómo y en qué condiciones se comparten los datos. Esto podría limitar la capacidad de nuevas empresas o competidores más pequeños para acceder a estos datos, afectando negativamente la innovación.

Por su parte, Eckardt & Kerber (2024) concuerdan con esta posición, en la medida que este instrumento normativo parece estar diseñado para proteger los incentivos económicos de los fabricantes de dispositivos IoT mediante el control exclusivo sobre los datos generados. Este enfoque ignora que los costos de producción de estos dispositivos pueden recuperarse a través de su precio de venta, sin necesidad de otorgar un control monopolístico sobre los datos. Esta situación, como ya hemos visto, podría restringir la competencia y la innovación en mercados secundarios, como los servicios de reparación y mantenimiento.

Asimismo, los autores aseveran que si bien se busca desbloquear datos para fomentar la innovación y la competencia, los mecanismos propuestos, como los derechos de acceso y compartición de datos por parte de los usuarios, son criticados por ser débiles y estar plagados de obstáculos. Estos incluyen altos costos de transacción y requisitos complejos que dificultan el uso efectivo de los datos. Como resultado, el impacto del Data Act en la liberación de datos para la innovación y la creación de nuevos servicios es limitado, lo que contradice sus objetivos declarados (Kerber, 2023).

En este sentido, el *Data Act* responde a una necesidad estratégica de fomentar un acceso equitativo a los datos, pero la protección de intereses e incentivos para la inversión y el desarrollo tecnológico deben abordarse desde una perspectiva económica y desde el bien social que podría generar. Su modelo se posiciona como una referencia clave para otras jurisdicciones que deseen maximizar los beneficios de la economía digital abordando también las debilidades y afrontando los retos que aún se desprenden al momento de regular el acceso a los datos no personales sin dejar de lado el justo equilibrio de los intereses entre los interesados.

6.2. Reglamento para el flujo libre de datos no personales de la UE

La Ley de Flujo Libre de Datos No Personales de la Unión Europea (Reglamento (UE) 2018/1807) propuesto en el año 2017 y con entrada en vigor en noviembre del año 2018, establece un marco normativo que tiene como objetivo principal eliminar las restricciones injustificadas al almacenamiento y procesamiento de datos no personales en los Estados miembros. Este reglamento busca facilitar el movimiento de datos entre fronteras dentro de la Unión Europea, permitiendo que las empresas y organizaciones puedan acceder a un mercado único digital más eficiente y competitivo.

Según la Comisión Europea (2018), el propósito central de esta ley es promover la innovación, fomentar la competencia y apoyar el desarrollo de la economía digital mediante el acceso fluido a los datos no personales. Responde a la necesidad de garantizar un entorno donde empresas puedan almacenar y procesar datos

La ley responde a la necesidad de garantizar un entorno donde las empresas puedan almacenar y procesar datos no personales sin restricciones geográficas dentro de la UE. Esto incluye datos generados por dispositivos IoT, análisis de grandes volúmenes de datos y aplicaciones en la

inteligencia artificial. Un aspecto clave de esta regulación es que prohíbe a los Estados miembros imponer requisitos de localización de datos, excepto cuando sea estrictamente necesario por razones de seguridad pública (Reglamento (UE) 2018/1807, Art. 4). De este modo, la ley busca eliminar barreras que fragmentan el mercado único digital y promueve la interoperabilidad y la portabilidad de datos entre diferentes plataformas y servicios.

Además, el reglamento establece que los proveedores de servicios en la nube deben desarrollar códigos de conducta para facilitar la portabilidad de datos entre diferentes servicios. Este enfoque tiene como finalidad reducir la dependencia de los usuarios a un solo proveedor (conocido como "*vendor lock-in*") y fomentar un entorno más competitivo (Eckardt y Kerber, 2024). A pesar de sus objetivos ambiciosos, esta ley no está exenta de críticas por 3 motivos: falta de claridad de la definición de datos no personales, insuficiencia en la protección del derecho de acceso y el impacto limitado en la interoperabilidad.

En primer lugar, no se ha definido qué constituye datos no personales. Esto genera incertidumbre en casos donde los datos pueden mezclarse con datos personales, lo que podría llevar a conflictos en la aplicación de esta ley frente a otras normativas como el Reglamento General de Protección de Datos (RGDP). Según Wiebe (2023), la falta de un marco claro para los datos "mixtos" es uno de los mayores desafíos para garantizar una implementación efectiva.
Aunque la ley elimina las restricciones a la localización de datos, no aborda adecuadamente los derechos de acceso y uso de los datos. Esto es particularmente relevante en mercados donde ciertos actores, como los fabricantes de dispositivos IoT, mantienen un control exclusivo sobre los datos generados, lo que puede limitar la competencia y la innovación (Eckardt y Kerber, 2024).

Si bien el reglamento promueve la interoperabilidad, su implementación ha sido criticada por depender en gran medida de códigos de conducta voluntarios por parte de la industria. Esto ha llevado a una adopción desigual, limitando el impacto potencial de la ley en la creación de un mercado más accesible y competitivo para los datos no personales Martens (2023, citado por Eckardt y Kerber, 2024).

La Ley de Flujo Libre de Datos No Personales de la UE representa un avance importante hacia la construcción de un mercado único digital más eficiente, eliminando barreras geográficas y promoviendo la portabilidad de datos para facilitar la innovación y la competitividad en sectores

clave como la minería, la agricultura y los servicios de agua. Sin embargo, su impacto no puede analizarse de manera aislada, ya que está integrada en un marco normativo más amplio que incluye leyes como el *Data Act* y el RGPD.

Este enfoque armonizado permite abordar cuestiones complejas relacionadas con la clasificación de datos no personales y datos personales, particularmente en casos donde los datos anonimizados pueden revertirse y, por tanto, requerir la aplicación de disposiciones más estrictas de protección de datos. Para maximizar su efectividad, será esencial abordar desafíos como la claridad en la definición de los datos no personales, la regulación de los derechos de acceso y el fomento de la interoperabilidad. Al contemplar estos aspectos se podrá garantizar un equilibrio entre la protección de derechos, la promoción de la innovación y el desarrollo de un mercado digital competitivo, aprovechando al máximo el potencial de los datos en sectores industriales y económicos.

6.3. Reglamento de Inteligencia Artificial (AI Act)

El recién publicado Reglamento de Inteligencia Artificial en la UE (en adelante, “Ley de IA”), Reglamento (UE) 2024/1689, es una de las normas más esperadas en la expectativa de regular por primera vez tecnologías como la inteligencia artificial en la implementación de sistemas que circundan la vida de los humanos y que pueden constituir diferentes riesgos. Está centrada específicamente en regular el uso y el desarrollo de sistemas de inteligencia artificial en general, pero a efectos del presente trabajo, analizamos algunos artículos que contribuyen de forma indirecta a la creación de una regulación específica sobre los datos no personales, sin dejar de lado que contar con principios como la transparencia y otras obligaciones en su uso, limita a los interesados en el uso de AIoT de manera positiva,

El Reglamento de IA de la Unión Europea, específicamente en su artículo 10, dispone los requisitos estrictos de calidad para los conjuntos de datos utilizados en el entrenamiento de sistemas de IA. Este enfoque asegura que los datos, tanto personales como no personales, sean de alta calidad, confiables y representativos del mundo real, evitando la generación de sesgos o resultados inexactos. Esto es particularmente relevante para datos recopilados por dispositivos IoT, que son críticos en sectores como la industria minera y agricultura. Al garantizar que estos datos reflejan estándares elevados, se busca prevenir afectaciones en las relaciones B2B y proteger los intereses de los usuarios al tiempo que se promueve la eficacia de los modelos de IA.

Por otro lado, es importante destacar que el artículo 60 dispone las pruebas en entornos reales antes de la puesta en marcha o comercialización de los sistemas de IA de alto riesgo en el mercado. En este contexto, los datos no personales son fundamentales para el correcto funcionamiento de los sistemas. Por ello, se establece que estos datos deben garantizar calidad, integridad y trazabilidad, dado que permiten entrenar los modelos de IA durante las pruebas y realizar mejoras o ajustes necesarios.

Asimismo, la trazabilidad es clave en la supervisión exigida por la Ley de IA, especialmente en los procesos realizados por las autoridades competentes. Es esencial garantizar que los datos generados durante las pruebas sean utilizados de manera ética, evitando que su acceso por parte de actores que interactúan con el AIoT sea indebido. Además, la trazabilidad durante las pruebas debe asegurar que el producto final sea confiable y verificable, cumpliendo con los estándares preestablecidos.

En el Capítulo VIII, artículo 71 de la Ley de IA "bases de datos de la UE para los sistemas de IA de alto riesgo enumerados en el Anexo III", el cual entrará en vigor en el 2026 señala que:

> *"Con excepción de la sección contemplada en el artículo 49, apartado 4, y en el artículo 60, apartado 4, letra c),* ***la información contenida en la base de datos de la UE registrada de conformidad con el artículo 49 deberá ser accesible y estar a disposición del público de forma fácil de utilizar. La información deberá ser fácilmente navegable y legible por máquina.*** *La información registrada de conformidad con el artículo 60 solo será accesible a las autoridades de vigilancia del mercado y a la Comisión, a menos que el proveedor o prestador potencial haya dado su consentimiento para que la información sea también accesible al público."* (Reglamento (UE) 2024/1689) (Énfasis añadido).

En este sentido, la normativa refuerza el uso de los sistemas de IA y de los datos no personales en términos de interoperabilidad y accesibilidad. Por un lado, se enfatiza que los datos deben estar abiertos al público, lo que facilita la creación de repositorios que puedan ser utilizados con fines particulares o comunes por proveedores tecnológicos. Por otro lado, el requisito de que la información sea navegable y legible por máquinas implica un nivel de interoperabilidad necesario para garantizar el cumplimiento de la misión principal: el acceso eficiente y seguro a los datos.

No obstante, las oportunidades, la Ley de IA no proporciona claridad sobre el manejo de los datos no personales, no existen lineamientos específicos de cómo tratar los datos no personales o cómo deben manejarse en el contexto de entrenamiento de sistema de IA, lo que podría generar incertidumbre para sectores que dependen de este tipo de datos. Pero tampoco se ha uniformizado con las normas complementarias, pues no hace referencia a estas normas especializadas, generando complejidades a nivel legal y operativo.

En conclusión, aunque el AI Act de la Unión Europea no regula específicamente la gestión o titularidad de los datos no personales, reconoce su importancia en el desarrollo de sistemas de inteligencia artificial y establece disposiciones clave para garantizar su calidad y trazabilidad. Este enfoque, aunque limitado, contribuye a ampliar las fuentes de intercambio de datos entre sectores públicos y privados, promoviendo el desarrollo tecnológico en la economía digital.

Sin embargo, la falta de especificidad sobre el papel de los datos no personales y su interrelación con otros marcos legislativos, como el Data Act, plantea desafíos para la claridad y la implementación efectiva de estas disposiciones. Para garantizar un impacto integral, sería necesario un marco regulatorio que detalle explícitamente la gestión de datos no personales, incorporando estándares de calidad, trazabilidad y accesibilidad en un entorno de datos abiertos (Open Data), fomentando así la innovación y la competitividad en el ecosistema digital europeo.

6.4. Reglamento General de Datos Personales (RGPD)

El Reglamento General de Protección de Datos Personales (RGPD) es la normativa que regula la protección de los datos personales en el contexto europeo. Este reglamento garantiza derechos para los usuarios y establece obligaciones específicas para quienes gestionan estos datos. En el ámbito industrial, especialmente en el uso de tecnologías AIoT, su impacto radica en la adopción de principios de transparencia y ética, con el objetivo de proteger la privacidad de los usuarios, incluso en relaciones B2B, donde prevalece la necesidad de establecer condiciones que promuevan el desarrollo científico.

Aunque esta normativa se centra únicamente en los datos personales, su alcance puede extenderse para abarcar situaciones en las que los datos recopilados por dispositivos AIoT en entornos B2B no cumplen con los estándares suficientes de anonimización o pueden ser identificados de manera indirecta. En tales casos, el RGPD será aplicable, ya que estos datos pueden afectar la privacidad de los usuarios si no se gestionan de forma adecuada.

Para Herbert Zech (2016) aborda cómo el RGPD establece un marco normativo robusto para la protección de datos personales en un contexto donde tecnologías como el IoT generan volúmenes masivos de datos. Según Zech, aunque el reglamento se enfoca en datos personales, la capacidad de las tecnologías IoT para recopilar datos aparentemente no personales, pueden combinarse y reidentificarse, y en consecuencia se deben aplicar las disposiciones del RGPD. Esto es especialmente relevante en entornos industriales como el AIoT, donde los datos de sensores y dispositivos pueden transformarse en datos identificables mediante métodos indirectos. Esto implica que incluso en relaciones B2B, si los datos no cumplen con los estándares de anonimización, están sujetos al RGPD y deben tratarse bajo sus disposiciones.

Además, el RGPD introduce la exigencia de implementar métodos o sistemas que cumplan con una estructura técnica de privacidad por diseño ("*privacy by design"*) y por defecto (*privacy by default*). Esto implica que los datos procesados a través de dispositivos AIoT deben ser gestionados con mecanismos diseñados para respetar la privacidad de todos los actores involucrados, incluso si no constituyen estrictamente datos personales. Esto se debe a que ciertos intereses económicos vinculados al desarrollo tecnológico podrían verse afectados si no se aplican dichas medidas. En este contexto, lo fundamental es que estas disposiciones puedan adaptarse para proteger los derechos afectados por las soluciones tecnológicas de AIoT, fomentando un equilibrio entre privacidad y desarrollo tecnológico.

En esa misma línea, Drexl (2017) enfatiza que la insuficiencia en los procesos de anonimización en datos recogidos por dispositivos IoT puede generar problemas legales significativos. En su análisis, menciona que si los datos anonimizados pueden reidentificarse mediante correlaciones indirectas, el RGPD se aplica automáticamente. Esto es crucial en entornos de AIoT, donde los datos generados por sensores y dispositivos pueden combinarse con otros conjuntos de datos para identificar a personas, lo que plantea riesgos para la privacidad. Drexl también sugiere que, para evitar vulneraciones, las empresas deben implementar procesos de anonimización más rigurosos y garantizar que estos cumplan con los estándares técnicos exigidos por el RGPD.

Finalmente, para que el RPDP genere un impacto positivo en la economía digital y las industrias que dependen de tecnologías AIoT, es fundamental armonizar su aplicación con otros marcos regulatorios, como el Data Act y la Ley de Flujo Libre de Datos No Personales, asegurando que la innovación y la protección de derechos puedan coexistir, adoptando un enfoque dinámico que equilibre el desarrollo tecnológico con la ética y la privacidad.

6.5. Ley de Gobernanza de Datos (Data Governance Act, DGA)

La Ley de Gobernanza de Datos es una normativa pilar dentro del marco regulatorio de los datos y las nuevas tecnologías en la Unión Europea. Su objetivo principal es generar confianza y facilitar el intercambio voluntario de datos, armonizando las condiciones de uso en ciertos sectores sin alterar los derechos materiales asociados a estos. Asimismo, busca fortalecer los mecanismos de disponibilidad de datos, proponiendo formas de superar las barreras técnicas en su intercambio mediante la reutilización, la intermediación y el altruismo.

Para la UE, los datos son el motor de la economía de hoy, una regulación en este aspecto beneficiará a las compañías y a los usuarios a través de la eficiencia. Se estima que el impacto se refleja en una mejora significativa en los servicios de salud, transporte, medio ambiente, agricultura y la administración pública, entre otras industrias. Si bien muchos datos no pueden categorizarse como abiertos debido a su carácter confidencial u otras restricciones, esta ley facilita su acceso y reutilización para fines altruistas específicos.

A pesar de que algunas empresas, especialmente aquellas que invierten significativamente en la recopilación y análisis de datos, perciben como una amenaza la posibilidad de compartir sus datos, la UE busca crear un entorno confiable y seguro para el intercambio voluntario.

Este proceso permite que empresas y particulares compartan datos bajo condiciones previamente establecidas. En el caso de la reutilización, la ley promueve el uso de datos generados por organismos públicos en sectores no gubernamentales, como empresas u otras entidades. Aunque no impone la obligación de reutilizar datos, sí establece condiciones técnicas, temporales y contractuales para llevar a cabo este proceso.

Respecto a la intermediación de servicios, se busca contrarrestar el dominio exclusivo y restrictivo que tienen empresas grandes de tecnología sobre los datos y permite que a través de los servicios de intermediación se pueda acceder a estos, dotándolos de una posición “neutral” y permite conectar pequeñas empresas y *startups* con los usuarios de los datos. Para garantizar esta neutralidad, los intermediarios deben cumplir requisitos estrictos, como la separación estructural, condiciones no discriminatorias y el uso exclusivo de los datos para mejorar los servicios que ofrecen.

Finalmente, sobre el altruismo de datos, este debería ser el fin último de la ley: el fomento del bien común. Se promueve la voluntariedad de las organizaciones para compartir datos, siempre que cumplan con requisitos específicos como la transparencia, la legibilidad y otros estándares establecidos. Este enfoque permite la creación de una nueva fuente de datos destinada a fines de investigación u otros intereses comunes, beneficiando a la sociedad en general.

En resumen, la Unión Europea lidera actualmente este campo regulatorio, apostando por facilitar el intercambio voluntario de datos. Dado que los conjuntos de datos poseen un gran valor económico, esta ley aboga por compartirlos, en la medida de lo posible, libres de cargos monetarios, reforzando así las prerrogativas establecidas en el Data Act y los derechos relacionados con los datos no personales. En este camino, los países fuera de la UE enfrentan el reto de implementar disposiciones similares que persigan estos objetivos, permitiendo una estandarización normativa que facilite la interoperabilidad extraterritorial en beneficio de la comunidad global y del desarrollo tecnológico.

Ahora bien, en síntesis, el análisis del marco normativo peruano y las tendencias a nivel europeo permiten observar que, si bien existen avances hacia la gobernanza de los datos no personales aplicados a los sectores industriales, aún persisten vacíos normativos significativos y dudas de la aplicación de las normas ya establecidas. Es aún más difícil cuando, en sectores estratégicos como la minería, existe un uso intensivo de AIoT que permite el incremento de la generación de los datos que poseen un alto valor económico.

Una revisión de la normativa existente evidencia la necesidad de un enfoque regulatorio que supere las lógicas tradicionales de la propiedad, replanteándose el tipo de situación jurídica que los datos no personales deberían adoptar en el contexto planteado, priorizando esquemas de garantías al acceso, compartición y reutilización de los datos en condiciones equilibradas, seguras y competitivas.

A partir de este marco, en el siguiente capítulo se abordará con mayor precisión el debate jurídico que existe sobre la atribución de derechos “de propiedad” en torno a los datos no personales y cuál es la mejor opción o modelo para abordar la gestión de estos en un entorno altamente dinámico.

CAPÍTULO II: LA RELEVANCIA JURÍDICA DE LA ATRIBUCIÓN DE TITULARIDAD DE LOS DATOS NO PERSONALES EN EL USO DE AIoT EN EL SECTOR MINERO

1. El mercado de los datos en la economía digital

Según la Organización de las Naciones Unidas (ONU**)**, Latinoamérica y el Caribe son regiones que experimentan un crecimiento en la economía digital, pero con características y ritmos distintos. Las estrategias necesarias para maximizar el impacto en la economía digital, el desarrollo, la innovación y la inclusión social deben enfocarse en establecer las condiciones necesarias para incentivar las inversiones en tecnologías y en información (Bercovich et al., 2013). Esto permite una articulación del conocimiento y la información de valor que contribuye al desarrollo de las industrias, la economía y el sector tecnológico.

La economía digital reconoce un valor estratégico a los datos como un recurso de innovación fundamental, equivalente al valor del petróleo en el mundo actual, sobre todo por su fácil disponibilidad y capacidad de procesamiento (Puyol, 2015, p. 350). Las economías del mundo se transforman rápidamente debido a la digitalización y automatización, impulsada por el uso de nuevas invenciones tecnológicas como el Internet de las cosas (IoT), asistentes virtuales con inteligencia generativa, sensores inteligentes y automóviles autónomos, entre otros. A esto se suma la rápida implementación de la inteligencia artificial, que mejora y acelera diferentes tareas y otros procesos que constituyen cargas innecesarias en la vida de los individuos.

Este proceso de transformación de la economía hacia espacios digitales depende de un modelo de negocio centrado en un activo fundamental: los datos. Recolectar, almacenar, procesar y transferir grandes volúmenes de datos implica cada vez menos inversión conforme avanza la tecnología. No es un secreto que la generación de información relevante a partir de los datos proporciona un valor significativo a los agentes económicos, promoviendo mayor eficiencia, productividad y rentabilidad. Por esta razón, muchas empresas han comenzado a considerar la implementación de tecnología como una inversión estratégica más que como un gasto operativo.

La evidencia de los grandes beneficios derivados del uso de los datos ha impulsado a diferentes industrias productivas a invertir en la transformación digital. Esto les permite adaptarse a las demandas de competitividad y eficiencia, además de acceder a información valiosa para optimizar sus operaciones y tomar decisiones que reduzcan costos**.** Verma & Gurtoo destacan que, debido al gran potencial de los datos para generar valor, los gobiernos de todo el mundo

buscan regular aspectos relacionados con su acceso e intercambio en diversas esferas, tanto públicas como privadas (2023).

Por ejemplo, la Unión Europea ha implementado una herramienta de Seguimiento de Mercado de Datos que proporciona información sobre el tamaño de las empresas, tendencias y sujetos clave. Su objetivo es apoyar a los reguladores con evidencias para el desarrollo de políticas públicas y concluyó que el sector minero alcanzó un 22.5% de monetización de datos en 2020, así se posiciona como sector estratégico y crucial en relación con el uso de datos no personales. Este sector es el primero y más relevante en la economía de los datos y en el porcentaje de monetización de datos.

Asimismo, si nos enfocamos en el sector minero, un artículo de Seequent (2023) concluye a partir de un reporte, que 8 de cada 10 profesionales de la minería consideran el manejo de datos como un aspecto altamente importante o crítico en sus organizaciones. Además, el 27% de ellos señala que dedica gran parte de su tiempo al manejo de datos, mientras que un tercio afirma no contar con suficiente información para tomar decisiones cruciales basadas en estos. Ante este panorama, es evidente que la implementación de tecnologías relacionadas con datos ofrece más beneficios que complicaciones; no obstante, su uso no está exento de incidentes de seguridad ni de riesgos asociados a un manejo inadecuado.

Particularmente en el proceso de explotación minera, los sensores aportan un valor significativo porque permiten identificar actividades, automatizar procesos y estimar el impacto de las decisiones, como por ejemplo mantener mapeada la ubicación de los depósitos minerales desde el proceso de extracción, así como monitorear el impacto ambiental de perforaciones y excavaciones, monitorear los ciclos de carguío y de procesamiento del mineral, entre otros.

Esto constituye un paso importante hacia economías y procesos de extracción más sostenibles y escalables, además de contar con la posibilidad de que dicha data sea reutilizable y aplicable a otros sectores. Obtener información sobre las operaciones permite reducir márgenes de contaminación o reducir la huella de carbono, evitar incidentes de seguridad, operacionales y ambientales, así como verificar avances, efectividad de las decisiones, probar alternativas a partir de datos, y más.

En base a lo expuesto, a medida que los sistemas tecnológicos se adaptan cada vez más a las diversas necesidades industriales, es crucial que los procesos de transformación tecnológica

integren distintas tecnologías y para ello, exista disponibilidad de los datos. En contextos industriales de especial relevancia como la minería, la multiplicidad de actores intervinientes en el proceso de digitalización hace compleja la interacción en la obtención, uso y explotación del procesamiento de los datos. Disponer de acceso general a los datos y aprovecharlo depende de la promoción de compatibilidad de sistemas. De lo contrario, la incompatibilidad técnica es una barrera que genera bloqueos en la disponibilidad de los datos y sin incentivos para hacerlos, frena la inversión en innovación.

Dicho ello, es crucial que se garantice un intercambio de datos en condiciones equilibradas, de interoperabilidad, fluidas y no burocráticas, con la finalidad de promover un uso y aprovechamiento compartido de los datos. De este modo se propicia un ambiente y condiciones para la innovación que exprese legibilidad de los datos, escalabilidad de los proyectos y adaptabilidad a los contextos cambiantes de la tecnología en un entorno con reglas claras pero flexibles.

Hasta la fecha, no hay un marco jurídico que establezca mecanismos para disponer los datos no personales con el fin de promover el aprovechamiento por las industrias, y por ello, para conocer la necesidad de contar con un marco regulatorio que permita gobernar los datos en condiciones de acceso equitativo, es necesario analizar los elementos de los datos no personales que los convierten en activos de especial condición y son de relevancia económica que merecen tutela en pro del beneficio común. Posterior a ello, se determinará si es posible aplicar lógicas de los derechos reales, de la propiedad intelectual u otro marco preexistente o si es necesario un marco normativo nuevo que responda a la naturaleza innovadora de los datos.

2. La naturaleza jurídica de los datos no personales

El tratamiento jurídico de los datos no personales plantea debates complejos y actuales en el derecho de las tecnologías. A diferencia de los datos personales, que su protección se enmarca en la tutela de la autodeterminación informativa como derecho fundamental de la persona humana, los datos no personales responden a un interés económico y colectivo, que crece más en la economía digital y que apoya a las industrias, que cada vez más dependen de la tecnología para su crecimiento.

El sector minero, siendo un pilar de la economía en nuestro país, experimenta una acelerada transformación digital y tecnológica mediante la adopción de sistemas de AIoT a fin de implementar el concepto de “minas inteligentes”. Este proceso implica la generación de grandes volúmenes de datos no personales, lo que permite optimizar las operaciones mineras, reducir costos y mejorar la seguridad (Cajahuaringa, 2025), lo que adquiere especial relevancia por su contenido de carácter industrial que impulsan la productividad del sector.

La explotación de los datos no personales otorga ventajas competitivas a diferentes agentes económicos tanto dentro como fuera del negocio. Su uso genera beneficios colectivos porque constituyen un insumo esencial para la planificación de políticas públicas, la sostenibilidad y el desarrollo de soluciones colectivas que trascienden el interés individual. En decir, el valor económico de los datos resulta incuestionable porque constituyen un recurso cuya circulación y aprovechamiento contribuyen al bienestar general y al progreso económico.

Sin embargo, ante contextos complejos aún se presentan dudas sobre si existen propietarios sobre los datos en el marco de la explotación y uso de los datos no personales. Para ello es necesario que se analice la relevancia jurídica de atribuir titularidad de derechos sobre los datos personales, a partir de la delimitación de su verdadera naturaleza jurídica. Entonces, cabe preguntar, a partir de las características particulares de los datos no personales en contextos digitales ¿cuál es la naturaleza jurídica de los datos no personales que los hace pasibles de tutela y qué garantías los protegen de manera más adecuada sin frenar la innovación?

En el contexto peruano, los datos no personales carecen de regulación específica que pueda determinar por sí su naturaleza jurídica. Tampoco han sido definidos en los marcos sobre la protección de datos personales, sin embargo, su creciente valor representa una necesidad de establecer marco normativo que logre identificar su naturaleza jurídica y que demarquen el establecimiento de una regulación promoviendo la competencia y la innovación en entornos industriales.

Con este propósito, conviene examinar el papel de los datos en la economía digital, el modo en que se han convertido en un insumo estratégico para el desarrollo de las industrias, sobre todo con la finalidad de atribuirles importancia real e identificar las características que los dotan de valor y pasibles de tutela jurídica.

2.1. La dicotomía de los datos no personales como “bienes”

En el debate sobre la naturaleza jurídica de los datos no personales, resulta pertinente analizar si estos pueden ser comprendido bajo la categoría de “bienes” en sentido del derecho civil. Al igual que los bienes tradicionales, los datos no personales pueden ser objeto de control, uso, disfrute y disposición por parte de un sujeto legitimado o que tiene acceso. Sin embargo, dicho control no configura un derecho real, sino un poder fáctico o tecnológico, dependiente de la infraestructura, de la capacidad técnica o de acuerdos contractuales que legitiman su tratamiento.

Esta analogía se explica en la existencia de una relación directa entre quien ejerce el control y el objeto, sin necesidad de una relación obligacional inmediata propia del dominio. Aunque los datos poseen un valor económico y estratégico, y pueden ser excluidos frente a terceros de forma tecnológica, asumir que ello los convierte en bienes en sentido estricto constituye en un error conceptual. Tal como advierte Jara (2021), los datos no son cosas corporales ni derechos incorporales, por lo que su relación con los sujetos que los controlan no puede ser equiparada a la de propiedad.

El derecho de propiedad recae sobre el concepto de bienes, desde la perspectiva de Ochoa, como aquello que es de utilidad para el ser humano y susceptible de apropiación (Ochoa, 2023). No basta, por tanto, que el recurso tenga valor o utilidad social, sino que además admita apropiación exclusiva. Tal como señala Ravina (1998) cuando hablamos de propiedad, se asignan derechos con la inmediata consecuencia de permitir excluir a los demás de estos y que deben reunir atributos como universalidad, exclusividad y transferibilidad (p.186).

Bajo esta premisa, aunque los datos no personales son valiosos y fuente principal para la innovación tecnológica, no cumplen con las condiciones para ser considerados como bienes pasibles de dominio. Su carácter intangible, no rival y su reproducción ilimitada impide la apropiación exclusiva y hace que la exclusividad resulte contraria a su naturaleza funcional en la economía digital. Pretender que sigan esquemas tradicionales susceptibles de dominio exclusivo como el régimen de la propiedad privada resulta una asignación forzada de las categorías tradicionales del derecho reales a un objeto que carece de corporalidad, escasez y delimitación, en otras palabras, contraria a su naturaleza.

Desde la perspectiva funcional, los derechos reales se conciben para regular la libertad y las relaciones pacíficas en una sociedad a partir de los bienes rivales y escasos, donde el control exclusivo permite garantizar su aprovechamiento máximo y ordenado de los recursos materiales limitados. Los datos, por el contrario, son no rivales y no excluyentes por naturaleza, y su valor incrementa con la circulación. En términos económicos, la propiedad real responde a la lógica de escasez, mientras que los datos, a la abundancia y replicabilidad (Drexl, 2018).

A nivel ontológico, los datos son entidades dinámicas constantemente en transformación mediante el procesamiento, y cuyo valor es contextual. La propiedad de los derechos reales exige objetos determinados e individualizados en un espacio, a diferencia de los bienes informacionales que no poseen una identidad fija ni un punto de referencia en el espacio, sino que reflejan una realidad espacial, pero su tangibilidad es información. No es posible entonces, ejercer posesión ni reivindicación sobre flujos de información o interpretación de datos.

Del mismo modo, los derechos reales se sostienen sobre el principio de publicidad y oponibilidad (erga omnes), que exige la posibilidad de identificar el bien y hacer visible la titularidad frente a terceros. Sin embargo, los datos no pueden ser publicitados sin vulnerar su propia naturaleza informacional o la confidencialidad tecnológica que los protege. En consecuencia, su apropiación es incompatible con los mecanismos que legitiman la existencia de derechos reales.

Si estos no pueden ser objeto de propiedad exclusiva por parte de los privados a través de los derechos de propiedad, entonces ¿deberían ser considerados como bienes de dominio público? Los datos no personales tienen características económicas similares a las de un bien público y ello conlleva a la errónea idea de equipararlos con estos para el uso público. Los bienes públicos se encuentran bajo esquemas de gestión estatal o son declarados como bienes de dominio público gestionados bajo sistemas de asignación, como los recursos del agua o el espectro radioeléctrico. En ese sentido, esta lógica implicaría desconocer que los bienes públicos responden a una lógica jurídica específica, sustentada en regímenes que buscan crear soportes para la prestación de servicios públicos.

2.1.1. Los datos como bienes de dominio público

Los bienes de dominio público poseen una naturaleza jurídica que se ha definido a lo largo del desarrollo de la doctrina administrativa. Bernal (2006) comparte la teoría vinculada a la función

social de la propiedad, que postula "*la subordinación de toda la riqueza del país, en sus distintas formas y sea cual fuere su titularidad, al interés general*" (p.267), lo que significa que la propiedad privada y pública siempre están subordinadas a un interés público y, por ende, la naturaleza patrimonial del dominio público es el interés público.

En base a dicha naturaleza, los bienes de dominio público se caracterizan por tener 3 elementos, según la Sentencia del Tribunal Constitucional (Exp. 0003-2007-PC/TC), configuran una relación jurídica de dominio pública. En primer lugar, la titularidad pública de los bienes deriva de la titularidad dominical de naturaleza *sui generis*, el segundo es la afectación de los bienes objeto de dominio público a una finalidad o utilidad pública y tercero, la aplicación de un régimen especial administrativo de protección y uso de bienes (fundamento 30).

Los datos no personales no cumplen con los anteriores elementos desarrollados por el TC. En primer lugar, no derivan de una titularidad originaria estatal, ya que se generan en contextos y procesos privados y a partir de técnicas o ingeniería protegida por propiedad intelectual. Tampoco existe reconocimiento de que pertenezcan a todos a través del Estado, ya sea mediante una ley que así lo determine, como sucede con los datos abiertos. En consecuencia, no tiene titularidad pública inherente.

Asimismo, los bienes de dominio público están afectados a fin de atender intereses públicos o destinados a prestar un servicio público, tales como la vía pública, la plaza para uso social y los mercados a propósito de la sentencia del TC mencionada anteriormente. Los datos no personales no están destinados al uso inmediato de la colectividad o del público general. De hecho, para que sean útiles requieren de tratamiento a través de tecnologías especializadas para que representen un valor. Sin embargo, mantienen una posible utilidad pública para mejorar los servicios, creación de políticas de cuidado y sostenibilidad, que dependen de políticas de apertura más no de su naturaleza intrínseca.

En tercer lugar, para que un bien pueda ser calificado como de dominio público, debe estar sometido a un régimen especial de utilización y protección. Esta lógica responde a un contexto histórico y cultural en el cual determinados recursos debían ser tutelados por la escasez de estos o el número limitado de agentes capaces de explotarlos. Por ello, el ordenamiento jurídico atribuyó a la Administración Pública la responsabilidad de su gestión y protección, imponiendo un régimen restrictivo y de protección forzado.

Algunos ejemplos son lo ocurrido en el sector de telecomunicaciones o en la regulación del espectro radioeléctrico. En el primer caso, los intervalos de numeración que los operadores necesitan para prestar sus servicios al público son limitados, lo que justifica la existencia de reglas de asignación específica. En el segundo caso, las frecuencias destinadas a la radiodifusión también son limitadas, de modo que se reconocen como bienes de dominio público porque puede encontrarse en que los canales utilizados para la radiodifusión de ondas son limitados.

Sin embargo, este esquema no puede trasladarse al entorno digital. De manera preliminar, se afirma que, como se ha desarrollado anteriormente, los datos no personales representan una naturaleza distinta: son infinitamente reproducibles, no rivales y su uso múltiple no afecta su calidad o disponibilidad. A diferencia de los bienes de dominio público tradicionales, marcados por su escasez material, el uso reiterado de los datos no afecta su calidad ni su disponibilidad, y los agentes que pueden utilizarlos tampoco son limitados.

En este sentido, si aplicamos criterios establecidos para la definición de bienes de dominio público, los datos no personales quedan excluidos de esta categoría. Adoptar su categorización bajo este concepto puede ser jurídicamente riesgoso, porque implicaría una estatización artificial que podría restringir la circulación de estos y, en consecuencia, la innovación. La lógica adecuada es reconocerles un régimen jurídico propio basado en un marco de gobernanza diferente, propio de los comunes digitales.

2.1.2. Los comunes digitales como categoría jurídica de gobernanza

En línea con la doctrina contemporánea, surgen aproximaciones alternativas. Autores como Mills (2019) y Viljoen (2021) proponen a los datos como recursos relacionales o comunes digitales (conocidos como "*digital commons*" en inglés) cuyo valor se potencia cuando son compartidos, reutilizados y puestos a disposición de otros actores para usos indistintos. Así, lo "patrimonial" de los datos no radica en la facultad de un agente para excluir a otros en base a la posesión de título que habilita una supuesta propiedad privada, sino en su funcionalidad económica, incluso en términos de afectación estatal.

Resulta relevante acudir al precedente de los comunes digitales, los "*commons*" (un concepto introducido por la economista Elinor Ostrom) como marcos complementarios a la propiedad, sobre los cuales sostiene que son un alternativa de componente institucional fundamental de la libertad de acción en las sociedades libres, pero se estructuran para permitir acciones que no se basan en el control exclusivo de los recursos (Benkler, 2006, p.24).

Benkler lo explica a través de ejemplos prácticos como la diferencia entre organizar un evento en un jardín privado o en un parque público, tanto la propiedad como los *commons* permiten grados de libertad de acción: la primera garantiza acceso mediante exclusividad, y el segundo, lo hace a través de reglas de acceso abierto. Esta coexistencia genera un balance entre los recursos gestionados como propiedad privada y los recursos gestionados como comunes, es decir, definir el equilibrio en aquello que depende de las transacciones en el mercado y lo que puede hacerse libremente. Este equilibrio juega un gran papel alrededor de los datos.

Para Ugo Mattei (2013), los bienes comunes son un tipo de derechos fundamentales de "última generación" que no están bajo discrecionalidad fiscal (a diferencia de los derechos sociales) o de los vaivenes del mercado, sino que implican la "satisfacción directa de las necesidades" de las personas. Pone como ejemplo cuando el Estado privatiza bienes comunes como ferrocarriles, líneas aéreas, entre otros. Los bienes comunes son una respuesta frente a la acción de los privados frente a la acción del Estado, entonces surge una tercera categoría entre la propiedad pública y la propiedad privada, adaptada a los nuevos tiempos (citado en Soto, 2022).

Siguiendo la lógica de Soto (2022), lo que define los bienes comunes no es el "libre acceso irrestricto de todos", sino la forma particular de gestión colectiva realizada por un grupo de usuarios que se consideran "propietarios" o custodios del recurso. A diferencia de la propiedad privada, que supone la exclusión a terceros y de la propiedad pública, que se centra en la administración centralizada y enajenación de bienes, los bienes comunes se estructuran a partir de cooperación voluntaria de los usuarios. En este modelo, como sostiene Ostrom, los usuarios participan directamente en la gobernanza de los recursos y, según Mattei, así se promueve la difusión del poder e inclusión participativa.

Este concepto precedente es importante para reconocer que existe un enfoque alternativo sobre la "propiedad" que trascienda la "privado o estatal". Los recursos generados en manera relacional en contextos industriales y tecnológicos, cuya gobernanza debe darse a partir de principios de colaboración, apertura regulada e interoperabilidad, permite trascender las categorías

tradicionales de apropiación y propone un modelo orientado a la gestión funcional, en donde se asignen derechos y deberes con la finalidad de aprovechar un recurso ilimitado.

En esa misma línea y en contextos más modernos, aparece la propuesta de los comunes digitales. Como señala Dulong (2020), ofrecen una alternativa de percibir los bienes desde una perspectiva social para producir y compartir recursos, organizar la acción colectiva y ampliar el acceso de manera sostenible y democrática. Si bien no todos los recursos deben gobernarse como comunes, este enfoque resulta pertinente para reconocer a los datos no personales bajo un parámetro, entendido como un "bien común digital" (Frischmann, Madison & Strandburg, 2014). Este no se enmarca en el concepto de bien con todos sus atributos, pero puede regular y fomentar el acceso, la innovación y la creación de ámbitos de gobierno colectivo a nivel nacional como internacional.

Dulong elabora una definición de los bienes comunes digitales como un "*subconjunto de los bienes comunes, donde los recursos son datos, información, cultura y conocimiento que se crean y/o mantienen en línea".* Estos se comparten de manera que evitan su confinamiento y permiten a todos acceder a ellos o usarlos para su desarrollo. La noción de bienes comunes digitales se encuentra en el corazón de los derechos digitales, la lucha política para expandir en lugar de restringir, el acceso a la información, la cultura y el conocimiento (Kapczynski y Krikorian, 2010, como se citó en Dulong 2020).

La misma autora señala que estos bienes se distinguen de los modelos tradicionales porque posee cuatro dimensiones: i) se gestionan bajo acuerdos socioeconómicos distintos de los modelos estándares de mercado y Estado, ii) hay nuevas formas de autoría que redefinen la creación y apropiación de contenidos, iii) son esquemas económicos alternativos que no se basan en la lógica de exclusividad, y iv) existen mecanismos de gobernanza social que garantiza sus sostenibilidad.

Estas dimensiones responden a la particularidad de los recursos digitales, que poseen algunas características distintivas que ya hemos evidenciado anteriormente: son no rivales, requieren de mantenimiento continuo para preservar su calidad y utilidad, se someten a riesgos de contaminación, es decir que pueden ocurrir con la proliferación de noticias falsas o alteración maliciosa de los datos, pero lo esencial, es que deben protegerse contra la subproducción, es

decir contra el desaprovechamiento de su potencial por falta de incentivos, sea para su utilización y circulación o limites a su acceso.

Esto es aplicable a los datos no personales, los cuales, no se agotan por su uso, por lo que necesitan ser gestionados, preservados y gobernados mediante reglas claras que garanticen su calidad y fomenten su aprovechamiento y eviten tanto la concentración excesiva como el desuso. La discusión sobre su naturaleza jurídica se mueve a través de dos opuestos: el de propiedad privada y el dominio público. Sin embargo, ambas categorías resultan insuficientes para capturar la esencia de un recurso que es intangible, reproducible y no rival.

De igual modo, la ONU viene trabajando a través de la Oficina de Tecnologías Digitales y Emergentes la promoción de los bienes públicos digitales. Asimismo, para el Foro Económico Mundial los bienes comunes digitales son esenciales para enfrentar las complejidades del siglo XXI. Su fortaleza radica en la capacidad de aprovechar la inteligencia de manera colectiva, esto permite el acceso sin restricciones y fomenta la participación de diferentes agentes en plataformas que pueden acumular y refinar la información, superando los sistemas cerrados tradicionales (Esposito, M. & Araral, E., 2025).

Se destaca, además, que los comunes digitales pueden institucionalizarse a través de mecanismos de gobernanza innovadores como las cooperativas de datos, incluso como sostienen algunos autores, a través de fideicomisos. Büler et al. (2023) sostiene que estas estructuras colectivas permiten a los individuos y comunidades compartir datos de manera segura y equitativa, preservando la soberanía digital y evitando concentraciones de poder en manos de pocos actores.

Más allá de concebir los datos como dominio público, que se someten a titularidad estatal y un régimen administrativo de uso, su tratamiento normativo debe orientarse hacia un régimen *sui generis,* con atribución de facultades que atiendan un propósito funcional, de gestión compartida y acceso colectivo, lo cual favorece la innovación, la equidad y la autodeterminación de los agentes intervinientes. Este planteamiento resulta relevante en entornos industriales, pues evidencia que el valor económico y social no requiere un esquema de propiedad exclusiva, sino de gobernanza colectiva propias de los comunes digitales.

Tal como señala Büler, los bienes digitales son gestionados a partir de principios de colaboración, apertura y gobierno participativos. Estos bienes representan alternativas a modelos tradicionales de propiedad, específicamente de propiedad intelectual, porque fomentan el acceso abierto, la innovación colaborativa y la promoción del conocimiento. Se realizan a través del reconocimiento a los usuarios de libertades de acción como acceso, creación, modificación y difusión de recurso dentro de un conjunto definido de reglas. De esta manera, mejora barreras de información, fomenta la propiedad comunitaria y contribuye a la democratización del conocimiento, a su vez, contribuye a que los entornos digitales sean más inclusivos y sostenibles (2023).

De igual modo, la UNESCO en sus Recomendaciones sobre la ética de la inteligencia artificial ha sugerido, respecto de la promoción del uso de datos sólidos y calidad, que los Estados Miembro deben adoptar un enfoque de patrimonio digital común. Así, se señala que, *"deberían adoptar un enfoque de* ***patrimonio digital común*** *respecto a los datos, cuando proceda, aumentar la interoperabilidad de los instrumentos y conjuntos de datos, así como las interfaces de los sistemas que albergan datos, y alentar a las empresas del sector privado a que compartan con todas las partes interesadas los datos que recopilan, en beneficio de la investigación, la innovación o el interés público"* (UNESCO, 2022, p.30) (énfasis añadido).

Esta recomendación implica la introducción de una categoría conceptual que supera el esquema tradicional de la propiedad privada y estatal entorno a recursos digitales. Si establece recomendaciones para concebir los datos como patrimonio común, son concebidos como bienes de naturaleza relacional y por ende no pueden ser objeto de apropiación exclusiva. Este planteamiento supone reconocer que, al ser generados colectivamente y de tener un valor potencial, no se agotan en la lógica de lo "privado" o lo "público", sino que forman parte de un colectivo de recursos que son compartidos. De esta gestión depende la innovación, el desarrollo económico e inclusive, si proyectamos los beneficios sociales, de justicia social.

Los bienes comunes digitales permiten justificar la creación de un régimen *sui generis* de titularidad funcional, en el que diversos agentes pueden ser titulares de derechos que se ejercen de forma limitada y correlativos a deberes, en función al rol que cumplen en la cadena de generación y uso de dato. Para ello, podemos evidenciar que se alinean con tendencias regulatorias como el Data Act, de la Unión Europea, que reconoce que el verdadero desafío no es definir "propietarios" sino garantizar un acceso equitativo, seguro y no discriminatorio que potencie la innovación y la competitividad.

Como ya hemos definido en el capítulo anterior, los datos no personales son aquellos que no identifican de manera directa ni indirectamente a una persona natural y su generación y circulación están relacionadas naturalmente a dinámicas técnicas, de la naturaleza, de entornos industrial, entre otros y con ello, su valor reside en el procesamiento y análisis de estos. Su dinamicidad en el proceso de creación, como en el procesamiento y la finalidad de su uso, refleja variables atípicas a sus atributos como bienes y trasciende las concepciones tradicionales de la propiedad en todos sus tipos, los bienes protegidos por derechos reales, la propiedad intelectual, entre otros.

Adoptar un marco en base a los bienes comunes digitales, supera la falsa dicotomía entre propiedad privada y dominio público que no encaja en los esquemas que plantean los datos no personales en contextos tecnológicos actuales. Esto abre paso a un enfoque regulatorio innovador y holístico, que responda a las particularidades de interacción que el uso de los datos no personales genera, sobre todo en entornos industriales.

Para ello, con el objetivo de conocer mejor la naturaleza económica y atribuir una relación jurídica conceptual innovadora a tales recursos, se debe identificar cuáles son las características que los dotan de ese valor y los convierten en recursos diferentes pero valiosos. Esto permitirá demostrar que sus atributos económicos y estructurales no encajan con categorías jurídicas tradicionales y por tanto requieren de una construcción de un régimen orientado a regular su acceso y explotación compartida.

2.2. Características económicas de los datos no personales

Los datos poseen ciertas características que los hacen medibles a nivel económico y se asemejan a los atributos de los bienes públicos por la serie de beneficios que estos proveen. Para Puyol (2015), estos bienes son especiales porque no cumplen con los clásicos preceptos de la oferta y la demanda y que se caracterizan principalmente por no cumplir con las 3 características intrínsecas de los bienes no son excluibles, no son rivales y el agregado especial de autor, la falta de transparencia (p.344).

Los datos son no rivales porque su uso por parte de un determinado sujeto no excluye a otros de utilizarlos nuevamente, ni se agotan o pierden su valor. Esto permite que tecnologías que

procesan datos en tiempo real o en la nube puedan utilizarlos para distintos propósitos sobre una misma estructura de datos, o que estos puedan ser reciclados y aplicados en diversas técnicas de manera simultánea, ya que son fácilmente copiables y transferibles.

Sobre la exclusión, existe poca claridad sobre si los datos pueden ser excluidos del acceso de terceros. Por un lado, cualquier persona puede captar datos a través de sensores o rastreadores en computadoras a partir del mismo entorno físico, la diferencia es que hacerlo en un mismo entorno en contextos industriales simplemente lo hace excesivamente oneroso. Por otro lado, grandes empresas de datos como Google, Facebook o X protegen activamente sus datos para evitar intrusiones, ya que el valor generado por estos activos constituye la base de su modelo de negocio (Díaz Vera, 2023).

Y sobre la poca transparencia de los datos, Puyol señala que cuando se trata de bienes con intervención tecnológica, el concepto adopta complejidad y, en ese sentido hay bienes que es necesario que se aprenda de ellos y se conozcan antes de ser consumidos, por ello es importante que se conozca lo que se está gestionando, en tanto podría tratarse de un concepto complejo, abstracto y opaco para que el consumidor tome decisiones racionales en base a su propio beneficio (2015, citado en Kahin & Varian, 2000).

Asimismo, Graux (2024) indica que hasta la fecha no existen leyes que otorguen "derechos de propiedad" específicos sobre los datos ni que los definan como tales. Sin embargo, al compararlos con los bienes patrimoniales, que son rivales, exclusivos y exhaustivos, o la lógica de la propiedad intelectual o la de los datos personales, se alejan totalmente de esa categoría.

Aplicar figuras tradicionales de derechos de propiedad a los datos no personales no resulta económicamente ni jurídicamente viable, pues no responden a una tutela específica considerando la naturaleza como activos. Implementar una regulación tradicional implicaría obstaculizar los principios del *Data Driven* necesarios para el avance tecnológico, el cual se centra en usar técnicas de interpretación y análisis de datos para la toma de decisiones.

El valor de los datos en el mercado radica en la potencialidad para generar información importante tras su análisis, lo que permite mejorar negocios, optimizar procesos y acceder a información confidencial o relevante para la toma de decisiones basadas en datos. Este valor agregado surge de las etapas de procesamiento, las cuales modifican la composición de los

datos. Con los datos en bruto, se detectan anomalías en tiempo real, como máximos de velocidad o vibración, o aplicar algoritmos de *machine learning* para identificar patrones predictivos.

Los resultados procesados se almacenan en bases de datos relacionales, donde se organizan en filas y columnas que describen características específicas, como direcciones, estados o fechas de fabricación. La estructura organizada de los datos incrementa su valor ante el posterior tratamiento, ya que facilita su acceso e interpretación tras un proceso de limpieza y filtración, resultando en información más legible y útil para fines específicos. Además, permite su representación interactiva a través de *dashboards***,** mostrando la información de manera legible, interpretable y de fácil acceso en tiempo real.

En ese sentido, la importancia de los datos reside no solo porque constituyen una fuente en el desarrollo de sistemas de inteligencia artificial y del IoT**,** sino también en su capacidad para reducir costos innecesarios y prevenir riesgos, permitiendo que las industrias se centren en la productividad sin descuidar la seguridad en los procesos productivos. Debido a ello, es fundamental establecer un marco regulatorio que reconozca a los datos no personales como activos intangibles cruciales para generar crecimiento económico en las industrias, que acompañe este proceso de transformación en condiciones idóneas, claras y equilibrando los intereses para que mucho actores puedan aprovechar su valor y seguir innovando.

2.3. Características estructurales de los datos no personales

Los datos no personales, al no estar vinculados a personas físicas, su protección jurídica se fundamenta desde una tutela basada en su valor económico y social, más que de derechos individuales. Estos datos presentan características particulares que se manifiestan a lo largo del ciclo de vida del dato en entornos AIoT, desde su generación, hasta su uso y transformación, que resultan significativas y generan impactos relevantes en los distintos actores involucrados. Su aprovechamiento compartido puede generar beneficios para diversos sectores.

Los autores Eger & Scheufen (2024) establecen factores que deben tomarse en cuenta sobre los datos en la eventual regulación de los datos no personales, dado que el diseño de la normativa que se implemente impacta directamente en la determinación de los costos y beneficios que se desprenden de los datos:

a) La diferenciación entre datos personales y no personales.

b) Los costos asociados a la recopilación y procesamiento de datos pueden ser altos, a diferencia de aquellos que se recopilan "*by product*s" o por los productos en sí mismo.
c) Por el valor social que genera o el valor aislado que podría producir para un sector específico.

Es decir, el análisis jurídico de los datos no personales en el uso del AIoT requiere identificar ciertas características particulares de los datos que los dotan de valor y los hace objetos susceptibles de tutela. Al identificarlas, es posible delimitar el ámbito de protección y regulación, especialmente en el contexto de relaciones B2B en el sector minero, donde la generación y el uso de datos, que para Eger & Scheufen constituyen la etapa con mayores costos, tienen implicaciones económicas, comerciales y legales significativas, especialmente cuando convergen múltiples actores en distintos niveles.

Por un lado, Verma & Gurtoo (2021) proponen la categorización de los datos inspirada en 3 tipos de dominio de los bienes: personal, público y privado. Los datos personales abarcan aquellos relacionados con un individuo identificado o identificable. Los datos de dominio público son aquellos que no están protegidos por derechos de propiedad intelectual u otros derechos similares, por lo que son accesibles al público y de libre reutilización.

Asimismo, los datos de dominio privado son de propiedad exclusiva. Distinguir estos dominios es crucial para el desarrollo de políticas públicas que regulen los datos con base en su origen, clasificándolos en cuatro categorías adicionales: datos proporcionados, observados, inferidos y derivados.

Estos autores destacan también diversos factores clave que deben tomarse en consideración al momento de regular los datos no personales. En primer lugar, es fundamental diferenciar entre las tipologías de datos, identificar a los actores involucrados (titulares de datos, usuarios e intermediarios), evaluar los mecanismos de acceso y estrategias de compartición de datos, y analizar los beneficios económicos y sociales que generan, así como los riesgos asociados a su uso.

Hasta este punto, las diversas características de los datos, ya sean subjetivas (datos personales, no personales o anonimizados) o relacionadas con su estado (en bruto, preprocesados o procesados), representan un desafío para la gobernanza jurídica. Es necesario considerar

además los intereses económicos y la situación jurídica en la que se han dispuesto los datos no personales en el entorno industrial, especialmente en relación con el estado de innovación en el que este se encuentra, a fin de determinar qué derechos y obligaciones se deberían atribuir sobre estos que permita generar condiciones productivas y de innovación tecnológica. A continuación, se presenta una clasificación sobre las características subjetivas de los datos no personales, que son necesarias considerar al momento de regular los datos como activos pasibles de tutela jurídica.

2.3.1. Ausencia del elemento subjetivo

Los datos no personales no han sido definidos de manera uniforme hasta la fecha, pero conocer su concepto constituye el primer filtro para delimitar el ámbito de aplicación sobre el cual aplicar un adecuado régimen. Esto se debe a que la línea entre los datos personales y no personales es delgada y existe un riesgo de confusión al momento de identificar cuándo el tratamiento recae sobre datos no personales. La primera referencia de definición de “datos no personales” es desarrollada por *ICC Policy Primer on Non-Personal Data October* (2023) que señala que el término es amplio debido a los datos no personales podría referirse a todo aquello no sea datos personales y que no represente un riesgo para estos.

Los datos personales son toda información que se refiere a un individuo identificado o identificable, es decir, que mediante uno o más datos (o “medios razonables”) sea posible identificar a la persona a quien se hace referencia. Por el contrario, los datos no personales no están vinculados a personas e incluso puede hacer referencia a datos anonimizados. En esencia, carecen de un factor de identificabilidad por sí solos o en conjunto, dado que no contienen un componente humano directo.

Los datos no personales requieren un marco regulatorio distinto, ya que su tratamiento no se encuentra bajo las prerrogativas del tratamiento de la LPDP y los riesgos de afectación a la esfera personal o privada de un sujeto, es casi nula. Por el contrario, contribuyen y benefician al sector al que se aplican, especialmente los de producción industrial, fomentando la innovación tecnológica e incluso, favoreciendo al sector público en la prestación de los servicios públicos. El valor de estos datos se manifiesta únicamente cuando son desbloqueados para su acceso, es decir, cuando son accesibles, utilizables y, eventualmente, transferibles.

Sin embargo, en la dinámica operativa, es crucial determinar que cualquier dato no personal que pueda identificar indirectamente a un sujeto o referirse a comportamientos asociados a este, automáticamente lo convierte en un dato personal, y esta línea difusa de diferenciación podría constituir un factor de riesgo para una adecuada protección de los derechos de los titulares de datos personales. No obstante, al no estar asociados a una persona natural, los datos no personales no son atribuidos a un "titular de derechos" como en el caso de los datos personales, que por su naturaleza, prevalece la perspectiva del derecho fundamental de la "autodeterminación informativa".

Sin duda, al estar ausente el elemento subjetivo, figuras como el consentimiento, el ejercicio de los derecho de olvido u oposición y otras disposiciones establecidas en la normativa de protección de datos personales, no se tomen en consideración al momento de regular los datos no personales, puesto que constituirían limites a los objetivos de crear un régimen jurídico funcional y estratégico especializado sobre los datos no personales que permita impulsar la innovación tecnológica e industrial. Tal como Finck y Pallas (2020) señalan, el límite entre ambos tipos de datos es difuso, pero jurídicamente los datos no personales carecen de una relación identitaria (p. 11), lo cual impulsa un marco regulatorio más flexible y con enfoque transaccional y enfocado en promover la innovación tecnológica.

Esto plantea grandes retos tanto legales como técnicos y prevalece el desafío de identificar y diferenciar los tipos de datos. Sin embargo, la subjetividad no debe limitarse a identificar al titular del dato personal, sino también a identificar qué sujetos están involucrados en su producción y a quienes le aporta beneficios económicos y sociales. En este contexto favorable para la promoción de innovación, figuras como la transferencia internacional de datos y el reconocimiento de responsables de tratamiento que introduce la normativa de datos personales, podrían ser aplicables a los datos no personales siempre que su aplicación favorezca la circulación de los datos no personales y promueva el desarrollo de la economía digital.

2.3.2. Según su fuente de origen

Los datos no personales utilizados en sistemas AIoT se generan, en su mayoría, a partir de procesos automatizados, principalmente mediante sensores, maquinaria, dispositivos conectados, entre otros. Su producción es resultado de la interacción de diversos actores y entornos relacionados a múltiples actividades comerciales o industriales, como análisis de

mercados, desarrollo de productos, optimización de cadenas de suministro, aplicaciones industriales o manufactureras, monitoreo ambiental, análisis de estados o movimientos financieros, entre otros.

Si bien los datos personales no se vinculan directamente a la identidad de una persona, no se excluye que conserven una dimensión subjetiva, en tanto pueden derivarse de acciones o patrones individuales, sin identificar al titular. Esta subjetividad no proviene del sujeto descrito por el dato, sino del agente que genera, interpreta o decide su recopilación y uso. En entornos de AIoT, los datos surgen de procesos técnicos, industriales o automatizados que involucra una infraestructura específica, como sensores, software, plataformas digitales, etc, cuya configuración depende de decisiones que los agentes o actores que intervienen adoptan.

Así, el proveedor tecnológico, el operador de la maquinaria o el usuario del sistema actúan como agentes, que desde sus funciones técnicas, comerciales o funcionales, determinan qué datos recopilan y para qué fines se procesan datos. Esta intervención aporta al dato una dimensión subjetiva que está relacionada primordialmente a la intervención de un agente que decide o tiene la intención de generarlos, recopilarlos y usarlos, así como definir cómo y para qué se procesan. Por ello, aunque los datos sean “no personales”, su origen está asociado a un ente subjetivo.

En el contexto de generación, es posible clasificar 2 formas de generación automática de datos no personales: (i) aquellos derivados a partir del uso que le asigna un usuario y (ii) aquellos generados automáticamente (“*by product*”) de una fuente tecnológica. La primera categoría comprende datos que surgen de la interacción de un usuario con un dispositivo, pero no contienen información personal identificable o desvinculados de información personal, como variaciones del estado del equipo o rendimiento del equipo. Estos datos, por sí solos, no permiten identificar a un sujeto o titular.

Sin embargo, si dicha interacción incorpora elementos suficientes que permitan identificar al sujeto de forma directa o indirecta, por ejemplo, al personalizar el sistema o al cruzarse con otros conjuntos de datos, entonces estos datos pasarán a concretarse el tratamiento de datos personales en la medida que, mediante el uso de medios razonables sea posible identificar a una persona.

La segunda categoría incluye datos generados automáticamente sin la intervención directa de un usuario, que surgen de la operación de sistemas IoT, esta categoría se le denomina “*by*

products", es decir que el objetivo no es la recopilación de datos sino que se recopilan de manera residual o por defecto durante la operación. Por ejemplo, en el uso de maquinarias se pueden recopilar, tiempos de espera, kilometraje recorrido, temperatura del ambiente, y todo ello a partir de los sensores instalados en una máquina, En ambos casos, el carácter no personal del dato depende no solo de su contenido, sino también del contexto técnico y funcional en el que se produce.

Sobre el término "*by products"* se refiere *a* aquellos datos que se generan a partir de un dispositivo pero que no fueron previstos originalmente como objetivo del sistema. Es decir, no se instaló un dispositivo con el propósito específico de recolectar dichos datos, sino que estos emergen de manera automática a partir del funcionamiento y uso de los dispositivos y por ende tienen un carácter "residual". Por ejemplo, en una flota minera de carguío y transporte, los sensores que posee la maquinaria miden la temperatura de la maquinaria y controlan el nivel de carga, pero podrían generar adicionalmente datos sobre los tiempos de operación, ciclos de trabajo o rutas recorridas, sin que esto haya sido parte de la finalidad inicial.

Desde una perspectiva técnica y jurídica, es importante que se considere la existencia y diferencia de este tipo de datos respecto de los datos intencionales, que son aquellos que provienen de dispositivos que han sido diseñados específicamente para recolectar datos con una finalidad predeterminada. Por ello, los datos generados como *by products* tienen un carácter incidental o residual, aunque su aprovechamiento representa una fuente emergente de valor económico y estratégico que es importante considerar en la creación de un marco regulatorio.

Esta clasificación evidencia que, los datos no personales no son neutros, ni son ajenos a contextos de producción complejos. Por el contrario, emergen de contextos donde interactúan múltiples actores o agentes, cuyas decisiones técnicas, comerciales o funcionales inciden en la forma en cómo se generan, recolectan y estructuran los datos.

En esa línea, Tarkowski & Vogelezang (2021) destacan que los datos se perciben como un recurso relacional y de co-generación, es decir de la intervención de múltiples agentes que influyen en la recolección y en la estructuración de estos. Esta visión es reforzada por, Viljoen (2021) en su obra "*A Relational Theory of Data Governance*", donde argumenta que los datos no deben interpretarse únicamente desde una perspectiva individual, ya que cualquier intercambio de datos implica un interés general de los colectivos que no puede reducirse a intereses exclusivamente individuales.

Del mismo modo, *Open Future Policy* sostiene que, a nivel gubernamental, los datos están siendo reconocidos como productos de creación conjunta o co-generación por parte de diferentes entidades. Estas características implican la interacción de diversos actores en la economía de los datos, lo que significa que la asignación de derechos exclusivos podría perjudicar los intereses de otros actores. Según Viljoen (2021), este enfoque resalta la importancia de una gobernanza de datos que considere la naturaleza compartida de los mismos y no priorice exclusivamente a un solo grupo de beneficiarios.

Bajo este enfoque, resulta indispensable repensar los modelos tradicionales que se plantea imponer en la gobernanza de los datos, y se vuelve demandante incorporar mecanismos que reconozcan la complejidad inherente a su generación y su carácter compartido, contextual y relacional. Esta perspectiva resulta especialmente relevante en entornos colaborativos como los sistemas de AIoT implementados en el sector minero, donde múltiples actores intervienen en su producción, procesamiento y aprovechamiento de los datos.

2.3.3. Según su grado de accesibilidad

Los datos no personales son, por naturaleza, activos no rivales. La rivalidad consiste en que los datos no personales como activos pueden ser utilizados por múltiples actores sin impedir su disponibilidad o impedir que otros lo usen de manera simultánea. Por ejemplo, los datos producidos por una máquina constituyen un activo que puede ser aprovechado por un número ilimitado de usuarios. Esto no solo genera beneficios para un sector específico, sino que también permite que otras empresas puedan procesar información a partir de ellos, fomentando la innovación y el desarrollo tecnológico.

Por ello, la capacidad de acceso a los datos se determina tanto por factores técnicos como contractuales que establecen o no limitaciones para acceder a los datos y promover condiciones de disponibilidad. Comúnmente se establecen a través de regulación contractual en modalidad de exclusividad, es decir en aquellas situaciones donde solo un agente puede acceder a estos datos o solo un agente puede disponer de estos. Esto se debe a que existen restricciones de diseño o técnicas que “encapsulan” los datos en un dispositivo y solo un agente tiene posesión total y control sobre estos.

En los casos en que únicamente el fabricante del dispositivo tiene acceso a los datos y es quien decide qué información compartir al usuario, los datos generados por la maquinaria minera, suele almacenarse en servidores locales o en la nube del fabricante, quien tiene control total sobre ellos. Esto impide que los usuarios puedan acceder fácilmente a los datos, solo pueden acceder a través de las plataformas que el fabricante ha dispuesto y puede ser información limitada o poco legible. Desde una perspectiva competitiva, esta práctica obliga a los consumidores a utilizar exclusivamente los servicios de mantenimiento del fabricante, ya que solo este tiene acceso a los datos necesarios para proporcionar dicho servicio (Eger & Scheufen, 2024).

Por otro lado, el acceso compartido a los datos puede limitarse mediante acuerdos de licencias u otras formas específicas de uso. La capacidad de acceso condiciona el ejercicio de otras facultades como el uso o la transferencia de datos, y plantea retos relacionados al abuso de posición dominante de grandes plataformas que incluyen este tipo de cláusulas por *default*. Esta situación se evidencia como un problema a la competitividad que puede reforzarse o disuadir en la aplicación de las leyes de competencia desleal o crear un marco regulatorio aplicable, ya que las exclusividades injustificadas pueden limitar la innovación tecnológica. En este sentido, permitir que los usuarios accedan, utilicen y transfieran datos no personales es clave para fomentar una economía de datos más equitativa y dinámica.

Según Hirshleifer (1971, citado en Eger & Scheufen, 2024), desde un punto de vista económico, el acceso a datos con valor social estaría justificado siempre que no implique un costo adicional significativo para quienes los poseen. Esta regla sugiere asignar una menor carga a quien dispone o tiene posesión sobre los datos y asigna una mayor carga a quien desea acceder a ellos. Sin embargo, esta lógica conlleva riesgos de comportamiento estratégico anticompetitivo, especialmente cuando la existencia de “altos costos” para compartir los datos es un término amplio y no definido. Por ello, resulta necesario exigir la incorporación de condiciones de interoperabilidad desde el diseño en la construcción de una normativa, así como establecer límites claros a lo que se considera un “costo adicional significativo”. De este modo, se evitará el uso de este supuesto como una barrera “artificial” al acceso, es decir, que se utilice como un cajón de sastre.

Cabe precisar que, tampoco se pretende exigir gratuidad y negar el capital invertido por alguna de las partes para generar acceso a los datos, por lo que todo costo adicional que implique poner a disposición los datos o que se exceda de los márgenes razonables bien definidos, es un

supuesto que perfectamente puede ser acordado y distribuido a discreción de las partes interesadas.

Verma & Gurtoo (2021), señalan que existen mecanismos y estrategias técnicas para facilitar el acceso y la compartición de datos. Entre estos se encuentran la disponibilidad para descarga directa, las *Application Programming Interfaces* (conocidas también como “APIs”), permiten la comunicación entre aplicaciones de software, y los sandboxes, que garantizan la legibilidad de datos en infraestructuras predeterminadas. Esta afirmación del autor, indica que la transferencia de datos puede implicar diversas cargas técnicas y económicas.

En muchos casos, se requiere complementar estas estrategias con acuerdos contractuales, políticas sobre datos abiertos y promoción de mercados de datos para facilitar su disponibilidad. Aunque cada mecanismo tiene sus propios riesgos y costos, una regulación de los datos no personales debe buscar que se dispongan de condiciones de acceso equitativas y que fomenten la innovación tecnológica, sin que ello implique amedrentar el capital invertido, ni limitar los fines mercantilistas que los agentes del mercado dispongan.

En este sentido, si el acceso a los datos se restringe mediante la atribución de derechos exclusivos de propiedad, se podría contravenir la finalidad de estos en los sistemas de IA. Los datos son esenciales no solo para garantizar el correcto funcionamiento de la inteligencia artificial, sino también para promover la interoperabilidad entre sistemas, mejorar el acceso a diferentes servicios, promover la competitividad en el desarrollo de industrias digitalizadas y beneficiarse de ello.

2.3.4. Adaptabilidad

La valorización de los datos en función a la finalidad que se les asigna, también es un factor esencial en la regulación de su uso, considerando su especial relevancia económica como bienes estratégicos para innovar y generar productividad en diferentes sectores. Los datos adquieren un valor especial cuando se les asigna una finalidad específica, es decir cuando su procesamiento comprende una capacidad relacional amplia. La regulación de los datos no debe centrarse exclusivamente en la propiedad o el acceso, sino también en cómo se maximiza su impacto si se orienta a una finalidad específica.

Según Coyle & Manley (2022), el valor de los datos no reside en su estado bruto, sino en las decisiones y acciones que se generan a partir de ellos. Por ejemplo, en sectores como el energético, los datos permiten tomar decisiones que generan un impacto tangible en los usuarios y en la eficiencia de los sistemas. Esto requiere de una inversión intelectual para obtener los datos, relacionarlos y generar mejores condiciones de relación para extraer información valiosa, lo cual se puede realizar a través de analítica de datos.

Regular los datos desde esta perspectiva implica reconocer que su valor depende de los objetivos que se pretenden asignar y si ello implica una alta especialización o personalización en una industria. En este sentido, el valor que se desea proteger radica en cómo se logra dicha personalización o cómo se produce un tipo de información diferenciada. Vincular los datos con su finalidad establece un criterio delimitante para determinar qué aspectos de los datos requieren mayor protección o acceso preferente. Por ejemplo, los datos utilizados para mejorar una infraestructura pública deberían tener prioridad, ya que representan un valor colectivo que justifica, en cierto modo, su accesibilidad.

Otra idea que desarrollan las autoras es que maximizar el valor de los datos no solo beneficia a las empresas que los controlan, sino también a la sociedad. Esto se traduce en mejores decisiones de políticas públicas y en el desarrollo económico sostenible, generando impacto positivo en diversas áreas. Por ello, es necesario implementar marcos regulatorios que aseguren tanto la protección de los datos como su acceso suficiente, fomentando la competitividad en el mercado y designando responsabilidades claras ante posibles riesgos anticompetitivos.

El carácter relacional de los datos y la posibilidad que estos se usen de manera simultánea, hacen visible su potencial para generar externalidades positivas en otras industrias (Coyle & Manley, 2022). Sin embargo, esta característica plantea desafíos regulatorios, ya que la falta de acceso adecuado puede limitar la capacidad de otros actores de otros ámbitos para innovar. Las autoras destacan que la regulación debe equilibrar los intereses privados con el beneficio colectivo, promoviendo la interoperabilidad y reduciendo las barreras para el intercambio de datos en sectores clave.

Tal como se advierte de la clasificación de los datos de Eger & Scheufen, estos también adquieren un valor adicional una vez procesados. Pueden aportar valor de manera aislada a un sector específico, pero también representan un valor social común (2024). En el caso de la industria minera, los datos recopilados no solo contribuyen a mejorar los procesos internos o la

producción, sino que, dependiendo de la finalidad atribuida, pueden crear valor colectivo y contribuir con un fin social. Esto puede incluir la mejora de las condiciones ambientales, la reestructuración de servicios a las comunidades o el desarrollo de nuevas iniciativas sociales.

Las partes interesadas pueden optimizar procesos operativos, emplear los datos en investigación y desarrollo, generar nuevos modelos predictivos o desarrollar tecnologías más personalizadas y precisas ampliándose a diferentes contextos, estructuras, etc. La comercialización es un uso adicional que muchas plataformas aplican a los datos que recopilan, ya que al combinar datos con *know-how* aplicado a una industria, pueden ofrecer soluciones útiles para otros sectores.

2.3.5. Según el nivel de tratamiento de los datos no personales

Otra dimensión estructural que adquiere importancia para comprender la naturaleza jurídica de los datos no personales es aquella que distingue a los datos según su nivel de tratamiento, esto es, según el grado de aplicación técnica sobre estos, desde la captación hasta su interpretación final como parte del ciclo de vida de los sistemas AIoT. Esta clasificación se ha hecho visible en el marco de la economía digital y es particularmente significativo para los contextos industriales.

Para ello se identifican al menos 3 categorías funcionales de los datos y se delimitan conforme al nivel del procesamiento o en qué etapa de encuentran dentro del ciclo del dato: datos en bruto, datos preprocesados y datos procesados o derivados.

2.3.5.1. Datos en bruto (“raw data”)

Los datos en bruto son aquellos que se capturan directamente de la fuente, sin haber aplicado algún tipo de mecanismo o técnica de procesamiento. Normalmente, se encuentran en un estado “crudo”, tal como la materia prima, sin contextualización, sin valor agregado, pero su valor es potencial porque pueden utilizarse para múltiples finalidades. En entornos industriales, suelen ser generados por los sensores o dispositivos que captan señales y están conectados a internet.

Natalia Jara (2021) elabora una clasificación sobre los datos, destacando los datos en bruto o “primarios” como aquellos que representan simbólicamente la realidad en virtud de una fuente directa, por ejemplo de artículos, escritos, videos, fotografías. (p.107).

Corrado et al. (2022) propone una clasificación que, si bien la denomina “cadena de valor de los activos de datos”, siguen la línea de los tipos de datos, vinculados con su procesamiento y transformación. Para los autores, los datos en bruto son un conjunto de bits y bytes que han sido

almacenados, pero no han sido aún limpiados, estructurados o transformados para su análisis, por ejemplo, aquellos que se recolectan de sensores, transacciones económicas. Es decir, son simples registros digitalizados que pueden acumularse a un ritmo asombrosos y almacenarse con poco o ningún coste (p.5)

A modo de ejemplo, los autores señalan que, los soportes de datos o "*data stores*" son registros brutos que se han almacenado, pero aún no se han limpiado, formateado o transformado para su análisis a diferencia de las bases de datos o "*database*", por ejemplo, datos extraídos de la red o del sensor y datos económicos capturados de actividades de producción o transacciones. Los registros brutos incluyen también los datos brutos recogidos de experimentos, encuestas estadísticas o registros administrativos (p.6).

Para Timonera, los datos en bruto son definidos como datos que reflejan exactamente su estado en la realidad física, son datos no procesados, codificados o analizados, y son difíciles de leer, visualizar e interpretar si es que no es ordenada o clasificada bajo un cierta cohesión y coherencia (2024).

El Data Act de la Unión Europea conceptualiza a los datos en bruto como datos que no han sido modificados sustancialmente, es decir, datos en forma bruta, también conocidos como *datos primarios o datos de origen* que se refieren a puntos de datos generados automáticamente sin ningún otro tipo de tratamiento, por ejemplo aquellos determinando una cantidad física o calidad o el cambio en una cantidad física, como la temperatura, la presión, caudal, audio, valor de pH, nivel de líquido, posición, aceleración o velocidad (acápite 15).

En el caso de datos situacionales o experimentales, que no poseen un valor agregado *per se*, en comparación con la data agregada, derivada, inferida que sí genera valor para un determinado sector, la discusión sobre el nivel de tratamiento que deben recibir también repercute directamente en la lógica de su posible apropiación exclusiva. Cuestionar si es viable atribuir derechos exclusivos sobre datos que, en principio, adquieren valor solo en contextos posteriores o a través de procesos de análisis rigurosos, pone en tela de juicio la coherencia de aplicar esquemas de apropiación tradicional a este tipo de activos informacionales.

Esta preocupación se advierte en un informe de *Open Future* (2021) en el cual se observa que el derecho *sui generis* (atribuible a las bases de datos) no promueve el uso de los datos, sino que introduce un resguardo adicional de una capa de exclusividad que dificulta la circulación de

los datos y la aplicación de la regulación establecida por la Unión Europea en el *Data Act*. En su crítica a la posible producción de este enfoque en la nueva legislación sobre datos no personales de la UE, se afirma:

> *"Al redactar el Data Act, se enfrenta a una elección fundamental tanto en lo que respecta a los derechos sui generis existentes sobre las bases de datos como a la introducción de un derecho similar a los datos brutos generados por máquinas. Existe el riesgo de que un enfoque que trate los datos como propiedad se vea reforzado por un nuevo derecho del productor de datos. […] Un nuevo derecho de propiedad no garantizará los objetivos definidos en la estrategia europea de datos: garantizar el acceso y el uso de los datos, en una economía de datos construida alrededor de espacios comunes de datos. En lugar de ello, reforzarán los monopolios existentes en la economía de datos."* (2021, p. 4).

De ahí se evidencia que el tratamiento jurídico de los datos en bruto no debe ser objeto de apropiación exclusiva sin considerar que sus implicancias estructurales y potenciales como activo intangible de alto valor económico puede generar mayores beneficios en la medida que se dispongan al público o se generen en contextos compartidos.

Además, tal como señalan Maharana, Monda & Nemade (2022), los datos pueden estar disponibles en tablas estructuradas, tablas no estructuradas, imágenes, archivos de audio, vídeos. etc. Como tal, no pueden alimentar directamente un modelo de inteligencia artificial para su procesamiento o entrenamiento, sino que necesitan ser tratados mediante limpieza y orden si es que se pretende aplicar a un sector o circunstancia específica para mejorar un proceso operativo, es necesario convertir los datos dados en 1s y 0s (p. 92), para ello es necesario la fase de preprocesamiento, que describiremos a continuación.

2.3.5.2. Datos pre-procesados

Los datos preprocesados son aquellos generados en una segunda "fase" en el tratamiento de los datos. Son los conjuntos de datos que se transforman a través de un proceso de limpieza, formateo y estructura, con el fin de ser utilizables por herramientas de análisis o visualización. Este tipo de datos facilitan el análisis y permiten hacer consultas y visualizaciones preliminares (Corrado et al., 2020). Es decir, convierten los datos dispersos en "*datasets*" estructurados y consistentes.

El preprocesamiento de datos constituye una etapa fundamental en los sistemas de aprendizaje automático, mediante la cual los datos brutos son transformados, limpiados o reestructurados con el fin de adecuarlos a un formato óptimo para su análisis automatizado. Este proceso permite que los algoritmos puedan procesar la información de manera más eficiente y precisa, maximizando así el rendimiento del modelo. En otras palabras, también puede interpretarse como que el algoritmo del modelo puede analizar rápidamente las características de los datos (Maharana, Monda & Nemade, 2022).

La fase de organización o estandarización de los datos no implica una interpretación compleja ni un análisis profundo, pero sí comprende operaciones relevantes como validación, eliminación de datos con errores, clasificación de datos, etc. El objetivo es optimizar la calidad de los datos para someterlos a análisis posteriores en óptimas condiciones, por lo que representa una capa intermedia entre el proceso de recopilación y de procesamiento del dato. Para Drexl, es una fase de interpretación, que alcanza un nivel semántico y por ello, abre la posibilidad de atribuir derechos de propiedad sobre los datos resultantes, en la medida que reflejen ciertos niveles de originalidad o impronta de la personalidad de quien desarrolla las técnicas de tratamiento (2018).

El *Data Act* define a los datos preprocesados como aquellos datos que han sido procesados previamente con el fin de hacerlos comprensibles y utilizables antes del procesamiento y análisis subsiguientes y que ha dispuesto que están dentro del ámbito de aplicación de la presente regulación (acápite 15). Sin embargo, precisa que, en esta fase, los datos no deben interpretarse como una imposición para realizar inversiones sustanciales, sino debe interpretarse como el formato exigible para que puedan ser utilizables, combinados con otros datos.

En esta etapa los datos son valiosos para el usuario y para sacar mayor provecho de estos, es necesario que se acompañen de *metadata*[3] con la finalidad de facilitar el proceso de interpretación y procesamiento al momento de brindar acceso a estos. En consecuencia, al ser valioso en su estado de preprocesamiento, su acceso contribuye directamente a la mejora de un nuevos servicios o productos y más aún, pueden aportar significativamente a otros sectores como salud, ambiente, entre otros.

En industrias como la minería, el preprocesamiento filtra o anonimiza datos sensibles antes de su almacenamiento o intercambio, por lo cual constituye una etapa crítica en la definición de la

[3] Infraestructura de Datos Espaciales del Perú (IDEP) los define como “Datos acerca de los datos” y sirven para suministrar información sobre los datos producidos.

normativa aplicable a los tipos de datos, a fin de evitar riesgos de privacidad y de exposición de información estratégica.

Una vez realizada esta fase, los datos adquieren calidad necesaria para constituirse en insumos válidos para someterse a análisis. Sin embargo, este paso es intermedio porque los datos preprocesados aún representan información en bruto y parcial, pero al menos se encuentra estructurada y limpia. Es recién en la etapa del procesamiento cuando los datos se someten a modelos algorítmicos o sistemas de IA que permiten transformarlo en resultados interpretables, patrones significativos y conocimiento aplicable a la toma de decisiones.

2.3.5.3. Datos procesados

Los datos procesados son el resultado de la aplicación de análisis, visualizaciones, inferencias y de la aplicación de modelos predictivos. Son enriquecidos mediante la aplicación de algoritmos, modelos o análisis de su totalidad o parcialidad, permitiendo la producción de inferencias, predicciones que contribuyen a un sector o proceso en específico. Usualmente, al ser información disgregada y concluyente, es fácilmente transmitible a través de *dashboards*, informes, alertas, indicadores, entre otros. Los datos, una vez estudiados y analizados, producen información. Trabajar con datos en IoT requiere menos tiempo que los datos brutos recopilados de las personas y posteriormente transformados en información (Molaei et al., 2020)

Para Jara, esta segmentación resulta relevante desde el punto de vista jurídico porque cada nivel de tratamiento puede implicar distintos derechos de acceso, control y uso, así como diversas responsabilidades y márgenes de reutilización. Como señala la doctrina, el dato en su estado más primario puede no tener valor jurídico autónomo, pero su “refinamiento”, mediante técnicas de análisis, genera productos informacionales que pueden acercarse a formas de protección como el secreto empresarial, la confidencialidad contractual o incluso, pasible de protección de la propiedad intelectual (2021, p.131-132). Esta fase es la que denomina Drexl como el aspecto semántico que adquiere valor real y potencial en cuanto es aplicado a una industria (2018).

En ese sentido, mientras el dato sea controlado por quien usa el dispositivo conectado, los datos procesados pueden generarse por terceros y por el propio fabricante del equipo (OEM). Esto plantea un debate sobre quién ostenta la titularidad o control sobre los datos, especialmente cuando un actor realiza esfuerzos significativos para obtener y extraer el mayor valor posible de ellos. La cuestión se centra en si dicho derecho funcional puede proyectarse sobre los distintos tipos de datos según su nivel de procesamiento a lo largo del ciclo de vida del dato.

Por ende, esta dimensión estructural debe ser considerada tanto en la formulación de cláusulas contractuales entre empresas del ecosistema industrial, como en el diseño de políticas públicas que buscan equilibrar innovación, competencia y gobernanza de datos. No reconocer las diferencias entre los niveles de procesamiento del dato y sus características económicas y estructurales, puede generar inequidades regulatorias, afectar la interoperabilidad o consolidar asimetrías informacionales difíciles de corregir *a posteriori*.

Para Corrado et al. (2024) indica que cuando los activos de conocimiento derivados de datos se protegen bajo regímenes de propiedad (por ejemplo, mediante exclusividad o secretos comerciales), la difusión de ese conocimiento se reduce. Esto genera problemas en materia de crecimiento económico e innovación y difusión del conocimiento puesto que son condiciones clave para que otras empresas o sectores reutilicen ese conocimiento, aprendan de él o lo mejoren.

Los autores señalan que se puede producir un efecto de "apropiación del capital de datos", es decir, que los beneficios del uso de los datos se limitan al beneficio de un solo actor. Si no se toman medidas a fin de fomentar la puesta en disposición común de los datos, el capital de datos se convierte en un activo privado con escasos beneficios sociales, lo que genera efectos directos como el freno a la innovación y estancamiento de la productividad en las industrias, límites a la competitividad en el sector. En consecuencia, si no se adoptan mecanismos de circulación continua los datos, se reduce la eficiencia compartida y restringe la posibilidad del aprovechamiento social de los datos.

Hasta este punto, habiendo abordado las diferentes características de los datos y su naturaleza que los hace un activo pasible de tutela jurídica deriva la cuestión de si resulta conveniente establecer modelos de propiedad exclusivos y que ejerzan controles absolutos sobre los datos en contextos plurales como los del sector minero en donde predominan las relaciones B2B y la multiplicidad de actores intervinientes.

Los datos no personales representan un insumo valioso, sobre todo en contextos industriales, por lo que otorgar derechos absolutos podría generar externalidades negativas a largo plazo. Por ello, es necesario buscar mecanismos alternativos de atribución de derechos que permitan equilibrar intereses y proteger aquellos que son legítimos en la búsqueda por promover la innovación tecnológica. Por ello, en la siguiente sección, se abordan sistemas propuestos para

atribuir titularidad o control sobre estos datos considerando los contextos industriales complejos como en la minería.

2.4. ¿Titulares o propietarios?: la necesidad de una precisión conceptual

Antes de analizar las doctrinas jurídicas que han intentado fundamentar derechos patrimoniales exclusivos sobre los datos no personales, desde el punto de vista civil, propiedad intelectual y protección de datos personales, resulta necesario aclarar el lenguaje jurídico adecuado para referir a los agentes que ostentan derechos sobre ellos.

¿Es jurídicamente correcto llamar “propietarios” a los sujetos que ostentan derechos de acceso, compartición y reutilización (explotación) sobre los datos no personales? ¿Corresponde hablar de “titularidad” de derechos o facultades? Estas interrogantes son muy interesantes cuando el uso del término “propiedad” trae consigo conceptos de exclusividad, perpetuidad y libre disposición bajo el régimen de los derechos reales. Por su parte, los datos, poseen una naturaleza, no rival, parcialmente excluible y tienen un valor dinámico y temporal, lo cual no merece asignarlos en tal categoría.

El término titularidad, desde la perspectiva del derecho civil, hace referencia a la condición de ser un sujeto activo de un derecho subjetivo, es decir la titularidad existe porque es la atribución jurídica de un derecho y el ejercicio de la titularidad es el despliegue de todas las acciones que se pueden realizar en base a ese derecho. Por otro lado, desde un enfoque constitucional, la noción de “titular de derechos” fundamentales hace referencia a que las personas no son propietarios sino que ostentan una condición en forma de destinatarios de una norma protectora como lo es la Constitución (Aldunate, 2003).

Siguiendo lo planteado por García de Enterría explica que la titularidad de derechos fundamentales no supone un derecho de dominio sobre algo, sino la condición subjetiva de ser destinatario de una norma de protección (2001), lo cual es aplicable a los agentes que intervienen en la generación de los datos no personales, puesto que no habría propietarios, sino titulares de una serie de facultades (o derechos) que el ordenamiento reconoce para regular de mejor manera su uso en la economía digital.

De manera preliminar, se afirma que la opción más viable es atribuir “titularidad” y no derechos de “propiedad” sobre los datos, puesto que permite proteger los datos no personales en razones de utilidad y valor en el mundo económico digital actual, respetando sus características dinámicas y modernas. Según la RAE un “titular” se refiere a la atribución de una cualidad o condición de titular, a la cual se le otorga un derecho, la propiedad de algo o le impone una obligación.

Es posible que en ocasiones, los términos “titularidad” y “propiedad” se usen indistintamente. Sin embargo, para diferenciar y establecer un marco regulatorio que tenga en cuenta las particularidades de los datos y su interacción en la economía digital, es importante determinar si corresponde designar “propietarios” *per se* o” “titulares” como concepciones jurídicas con una connotación de exclusividad. Mientras que la propiedad de los derechos reales se usa para diferenciar los poderes y facultades de un bien físico o inmaterial, e implica un control total y exclusivo sobre el bien, el concepto de titularidad denota una noción de atribución de facultades respecto de derechos atribuidos y que también contrae deberes.

Aplicar la noción de la titularidad desde una perspectiva funcional, resulta más coherente con la naturaleza de los datos no personales. El uso del término “propietario” tiende a remitirse de manera automática al régimen tradicional del régimen de los reales en su concepción exclusivista. Si se trasladan estos conceptos a la lógica de los datos no personales, existen riesgos de legitimar posiciones de dominio que se contraponga a los intereses de regular el acceso sobre los datos no personales, y que eventualmente, desincentiven la innovación hacia el conocimiento.

En ausencia de una regulación específica, resulta contraproducente a los fines ya mencionados, reconocer como “propietarios” a quienes ostentan ciertas facultades sobre los datos no personales, básicamente porque es disfuncional en relación a sus características jurídicas. Hablar por el contrario de “titulares” permite establecer sistemas más flexibles y funcionales de las facultades del dato: pueden desarrollarse sistemas de licencias, crear obligaciones compartidas y deberes más amplios orientados a proteger un interés general y sobre todo la innovación. La titularidad, al no presumir un poder exclusivo absoluto, reduce la concentración de la información y favorece ecosistemas más abiertos para la entrada de diferentes agentes en condiciones de igualdad y potenciando los beneficios económicos y sociales del uso de los datos.

3. Doctrinas sobre la atribución de propiedad sobre los datos no personales

A partir de la identificación de las características de los datos no personales se ha evidenciado que existe una diferencia sustancial en comparación con otros bienes que resultan compatibles con la lógica de la propiedad privada o bajo el dominio público. Ante dicha cuestión, se plantean tensiones jurídicas al momento de definir un derecho *sui generis* que atribuya a distintos agentes, derechos y deberes referidos al acceso, uso y compartición. Es decir, el debate que se presenta a continuación busca refutar la titularidad exclusiva en sentido estricto y argumenta a favor de crear condiciones efectivas para el ejercicio de derechos funcionales, específicamente en las relaciones B2B.

El debate sobre la “apropiación” de los datos en el plano material, se intensifica porque su valor no radica solo en la recopilación de forma aislada, sino en la capacidad de combinar y reutilizar estratégicamente los datos de diferentes fuentes para elaborar información relevante para las industrias. Así lo evidencian Hughes-Cromwich y Coronado, quienes realizaron una evaluación del valor de los datos gubernamentales de los Estados Unidos en las decisiones de los negocios y se determina que el valor de estos datos aumenta significativamente cuando se emplean en decisiones empresariales, concluyendo que la combinación de estos datos generados por compañías y datos gubernamentales podrían crear beneficios estratégicos considerables (2019).

En el contexto minero, la recopilación de los datos industriales implica inversión sustancial tanto en el desarrollo de tecnologías como en la instalación de soluciones en la infraestructura. Una vez que se generan los datos, pueden ser utilizados en sectores complementarios como el ambiental, social y educacional, lo que evidencia su naturaleza no rival. Este carácter permite su aprovechamiento simultáneo por distintos actores sin que ello implique una alteración o afectación en su valor o calidad, con ello adquieren la característica de bienes intangibles de alto valor estratégico para las organizaciones.

No obstante, el intercambio y acceso a datos puede generar desacuerdos sobre quién puede utilizarlos y en qué condiciones, debido a que existe la posibilidad de generar intereses que colisionan entre las partes involucradas. Como consecuencia, a nivel legal y técnico, se producen riesgos que desafían la utilidad de aplicar los esquemas tradicionales de propiedad a bienes que evolucionan en el entorno digital.

Tal como lo señala El-Khoury & Lacin (2021) "*la propiedad como construcción legal se ve afectada por el mundo digital que impregna el IoT. Una empresa que comercializa dispositivos IoT ejerce un control significativo sobre el producto, y esto limita en gran medida lo que un consumidor puede hacer con el dispositivo de maneras que, hace 20 años, hubieran parecido escandalosas*" (p. 309).

Los conceptos clásicos de propiedad, incluido aquellos de la propiedad intelectual, resultan insuficientes para explicar las dinámicas actuales de control sobre los bienes. Actualmente, no basta con la posesión física para ejercer propiedad exclusiva sobre un dispositivo, pues los fabricantes mantienen un control continuo, incluso después de haber adquirido el bien, limitando así la capacidad para ejercer plenamente los derechos asociados a la propiedad.

Esto modifica las expectativas históricas del dominio que estaban estrechamente ligadas al concepto de la propiedad de los bienes intangibles. El-Khoury y Lacin nos muestran que la propiedad en el mundo digital no implica necesariamente control ni libertad total por el adquirente de un bien, y por el contrario, desafía la concepción de la propiedad como poder pleno y exclusivo (2021).

La creación de valor económico a partir de los datos no personales depende de la transformación de los datos en bruto a información estratégica mediante la aplicación de tecnologías como el AIoT. Su valor económico y organizacional lo convierte en un activo intangible crucial para diversas organizaciones públicas y privadas. Heverly (2003) señala que la característica de ser fácilmente reproducidos y transferidos a un costo marginal cero, los hacen adaptarse al concepto de otros bienes intangibles relacionados a la información. Esto se diferencia de los bienes tangibles, donde la propiedad se asigna en términos de exclusividad y control absoluto sobre el bien o le brinda capacidad para disponer de este o incluso destruirlo (p. 1140).

Del mismo modo, Corrado, Hulten y Sichel (2005, citado en OECD, 2022) sostienen que los activos de datos están dentro de lo que se considera como "capital intangible". Ello se debe a que la inversión en activos intangibles conlleva necesariamente a la asunción de diversos costos asociados, como las bases de datos, el costo del procesamiento, la ingeniería, el diseño, el estudio del mercado, la creación del hardware, entre otros. Estos son aspectos que se deben considerar al momento de determinar la posible asignación de derechos de propiedad, ya sea en su forma tradicional o también con la creación de nuevos conceptos que contemplen el ámbito subjetivo en términos de titularidad y no desde la exclusividad.

La inversión en activos intangibles es crucial para generar retornos favorables y beneficios a nivel privado y también público. Esta inversión no solo refiere a la infraestructura de AIoT para la recolección de los datos, sino también los costos asociados a su transformación y generación de valor traducido en información en base a la aplicación de las tecnologías avanzadas, planteando interrogantes sobre qué tipo de datos realmente son pasibles de crear un marco normativo de protección bajo los parámetros de “comunes digitales” que se enfrenta a un interés económico superior de un agente frente a otro y si tal disputa merecen tutela.

Ese valor económico adicional obtenido, determina la construcción de categorías de derechos que protejan las relaciones y situaciones que se generan alrededor de los datos y también cuestiona la forma y sujetos que pueden acceder a ellos, explotarlos y compartirlos. Una omisión a la diversidad sobre los datos podría convertir un marco regulatorio en un vil instrumento para concentrar poderes sobre quienes tienen ventaja competitiva, tiempos de recolección más prolongados o red más amplia para la recolección de los datos y perpetuar situaciones de monopolio.

La cuestión sobre la titularidad de los datos no personales sigue siendo un debate, especialmente en contextos donde intervienen una pluralidad de agentes. Esta incertidumbre se acentúa por inexistencia de una legislación especializada que regule su propiedad, a pesar de la creciente necesidad de establecer reglas precisas en torno a un activo de elevado valor comercial y a los beneficios derivados de su utilización.

Para abordar esta problemática, es necesario analizar el *status quo* del uso de los datos no personales en la actualidad y examinar diversas perspectivas sobre la atribución de derechos de propiedad. Esto incluye abordar las perspectivas sobre las nociones de “propiedad” en nuestro ordenamiento jurídico, tanto nacional como internacional, y determinar sobre si las formas de propiedad existentes son aplicables a los datos de manera funcional y eficiente. Asimismo, se debe evaluar la viabilidad de utilizar términos como "propiedad" o "titularidad" para referirse a quienes ostentan derechos sobre los mismos.

3.1. Concepto de la propiedad tradicional (derechos reales)

La definición de “propiedad”, en su sentido jurídico, hace referencia a los poderes que ejerce un propietario respecto de cierta cosa y no hace referencia al objeto sobre el cual se ejerce el dominio, sino del cual la cosa es su objeto (Barrios & Espinoza, 2006). Al respecto, Deternmann añade que existen 3 categorías generales de la propiedad: la de los bienes inmuebles, bienes muebles y la propiedad intelectual. Los derechos de propiedad tienen reglas para gobernar el acceso y el control a la propiedad a través de derechos como la posesión, exclusión y transferencia. Este último es el más importante y lo que comúnmente caracteriza la propiedad (2019). A esto se le llaman los poderes jurídicos que el propietario ejerce sobre la cosa.

Avendaño señala que la propiedad es un “*poder jurídico, el más amplio y perpetuo que las personas pueden tener, en virtud del cual un bien o conjunto de bienes quedan sometido de manera absoluta al señorío de una persona*” (2019). Además, se refiere a la propiedad como el derecho que tiene todo propietario a "poseer" el bien y le asigna 4 atributos a la propiedad: es un derecho real, exclusivo, absoluto y perpetuo (1984). Al ser un derecho real, la propiedad le otorga facultades de persecución y preferencias a un titular, lo cual establece una relación con la “cosa” de manera directa e inmediata. En consecuencia, es *erga omnes* (oponible) y excluyente, es decir que puede tener todas las facultades sobre un bien y ser perpetuo, porque este derecho solo se extingue con la desaparición o destrucción total.

Para Cordero (2020) el concepto de propiedad en sí mismo denota aspectos difusos, llegando incluso a confundirse con el ejercicio de la libertad económica, estableciendo que “*la propiedad, al menos en cuanto dominio, esto es, sobre bienes corporales, es decir que brinda libertades para actuar sobre una parte del mundo físico, revestida por el derecho de un carácter de exclusividad legítima*”. En este modelo, el dominio sobre bienes corporales se entiende como una libertad revestida de exclusividad legítima, limitada solo por la ley y por el interés social (p.76). Esto permite afirmar que la propiedad no ofrece una categoría conceptual plenamente delimitada lo que genera dificultad cuando se pretende extender a realidades inmateriales potencialmente materializables, como los datos no personales.

El concepto de propiedad de los derechos reales abarca la idea de que el propietario posee derechos absolutos y total control sobre la *res* (cosa). Este poder jurídico, en el derecho civil peruano, se ejerce sobre bienes muebles o inmuebles, tal como se interpreta de los artículos 881° del Código Civil Peruano (CCP), que señala que los derechos reales se aplican a aquellos señalados en los artículos 885° y 886° (bienes muebles y inmuebles).

No obstante, en el artículo 2093° del CCP, se excluyen a los bienes incorporales porque se rigen bajo una legislación especial. Entonces, queda claro que la forma tradicional de la propiedad hace referencia a un poder jurídico que concede a los propietarios la capacidad de usar, disfrutar y reivindicar el bien, o como podría llamarse, la dimensión más amplia de la titularidad.

Desde la noción clásica de la propiedad como situación de pertenencia estrictamente individual, centrada en la exclusión de terceros y el ejercicio de un control exclusivo sobre el bien por parte de un único titular, es una concepción que ha dominado históricamente el discurso jurídico, especialmente a partir del sistema liberal. Esta concepción que Moccia (2010) denomina "propiedad individual o privada en sentido subjetivo", es lo que ha estructurado los sistemas modernos de propiedad incluso cuando han sido aplicados a bienes que no responden a la lógica exclusivista.

Sin embargo, la funcionalidad o eficiencia de este modelo viene siendo cuestionada por las tendencias actuales alrededor de la era digital. Como sostiene nuevamente Moccia, la historia jurídica ofrece variedades de apropiación no individual, como la copropiedad o la "propiedad pública" y especialmente la propiedad colectiva o común (*commons),* lo que hoy en día se reconoce como una contribución al desarrollo sostenible y la aparición de nuevas tendencias de protección de los recursos de valor ambiental y cultural.

Bajo esa misma perspectiva, los datos no personales en contextos de AIoT industriales, no se subsumen bajo el paradigma exclusivo de la propiedad individual, debido que su valor colectivo y sus características económicas y estructurales lo dotan de capacidades plenas para ser un activo potencial de reutilización y de ser compartidos por diferentes agentes en el mercado, promoviendo la innovación tecnológica. Además de su impacto en el bienestar general, a través una posible contribución como fuente a la mejora de servicios públicos, son una invitación a explorar nuevas formas jurídicas de atribución de funcional de derechos que no restrinjan su aprovechamiento.

Continuando con Moccia (2010), este autor critica la idea de que la propiedad siempre debe implicar exclusividad ("*ius excludendi alios")* como un rasgo esencial y además, señala que el control sobre una cosa o bien no se presenta de forma unitaria, sino también como una fuente pasible de poderes o facultades. Distingue el lado subjetivo y objetivo, donde el primero permite

la conjunción de múltiples sujetos titulares de derechos de un mismo bien y el segundo, refiere a que los poderes sobre el bien pueden estar distribuidos entre distintos sujetos, ya sea para el uso, la gestión o el disfrute (p. 49).

En ese sentido, esta perspectiva resulta útil para conceptualizar el régimen de los datos no personales como un sistema de titularidad funcional y distribuida, donde distintos agentes pueden tener derechos de acceso, compartición y reutilización, sin que ninguno ostente una propiedad absoluta o excluyente. Así, se entienden como un recurso compartido y de general usp, dando lugar a modelos de gobernanza colaborativa y más abiertos.

Es verdad que los datos son bienes incorpóreos y, técnicamente, son parcialmente excluibles. Poseen una naturaleza dinámica porque presentan características únicas que difieren significativamente de los bienes tradicionales como los tangibles, intangibles, muebles o inmuebles, con características no fungibles. Precisamente por ello, es necesario recurrir a una categoría más amplia, entendidos como derechos subjetivos con contenido patrimonial y pasible de responder a un interés económico que permita captar el valor y las facultades de aprovechamiento de los datos sin implantar figuras exclusivistas como el de la propiedad.

A diferencia de los bienes tangibles, cuyo valor intrínseco suele verse afectado por su temporalidad o durabilidad, los datos no personales al poseer características de los bienes intangibles pueden no estar sujetos a la escasez física ni deteriorarse materialmente. Por ello, su valor si depende de la temporalidad porque puede ser efímero o estratégico. Por ejemplo, debido a la aparición de nuevas tecnologías o metodologías de procesamiento, el dato puede perder valor por la exactitud que se disipa con el tiempo.

Sin embargo, si se analizan desde el conjunto, podrían ser útiles al constituir información histórica que podría ser relevante para el análisis. Este fenómeno es especialmente evidente en sectores industriales como la minería, donde los datos históricos adquieren relevancia dependiendo de cómo se pretende aplicar la data histórica porque aportan información como valores históricos, patrones de cambio, entre otros. Al margen de ello, el contexto de uso es importante, pero en mucho casos, pierde valor con el tiempo porque no son actualizados.

Como señala Atik (2023), el avance en técnicas de analítica de datos y *machine learning* implica que el valor de los datos no radica únicamente en su recopilación, sino también en su potencial

para ser transformados y utilizados en tiempo real. Además, la *International Chamber of Commerce* (2023) subraya que los costos decrecientes de almacenamiento han hecho que los datos puedan acumularse indefinidamente, pero su utilidad práctica sigue estando condicionada a la capacidad de procesarlos con tecnologías modernas y, por último, están sujetos a condiciones variables. De este modo, la temporalidad de los datos no se ajusta al concepto de perpetuidad que caracteriza a los atributos de la propiedad.

Si bien las características y atributos de la propiedad aportan herramientas claves para interpretar el tratamiento jurídico de los datos no personales, permitiendo reconocer y resaltar la importancia económica de estos, es importante advertir los límites del enfoque del Análisis Económico del Derecho (AED). Tal como advierte Gutter Gonzales (2022), este enfoque tiende a reducir el análisis jurídico a una lógica instrumental centrada en la maximización de utilidades, basada exclusivamente en el análisis costo-beneficio y prescinden de consideraciones esenciales como la equidad, la justifica distributiva y los costos sociales que implica la apropiación y uso de determinados activos jurídicos.

En particular, cuando se aplica esta lógica al ámbito de los datos no personales, existe el riesgo de centrar la utilidad y potencial para aquel individuo o entidad que lo genera, recopila y procesa y se pueden invisibilizar las externalidades positivas que su uso y circulación generan en diversos sectores y en colectivos, tanto públicos como privados, y una incorrecta interpretación de estos podría consolidar esquemas de apropiación asimétricos en el mercado digital.

Desde una perspectiva jurídica, esta limitación adquiere especial relevancia en contextos B2B, donde los derechos sobre los datos tienden a concentrarse en quienes controlan la infraestructura tecnológica o el diseño del dispositivo, relegando a otros actores de la cadena de valor que se genera. Este modelo de gobernanza, centrado en apropiación exclusiva, compromete el interés común, inhibiendo la innovación, restringiendo la posibilidad de aprovechamiento colectivo de los datos, pero sobre todo generando límites al acceso al conocimiento.

Si consideramos que el proveedor de AIoT es propietario exclusivo y ejerce posesión absoluta sobre los datos no personales, bajo una interpretación de propiedad en su concepción primitiva, similar a los conceptos tradicionales de propiedad de los derechos reales, se estaría creando una situación de desventaja frente a otros agentes que podrían brindar posibilidad de uso a tales

datos a través del acceso, y la promoción de estos en mercados complementarios que beneficien a una variedad de agentes en el mercado.

Para Gutter Gonzales (2022), la propiedad no puede concebirse como una facultad absoluta, individual y excluyente, sino como una institución jurídica funcional, cuyo ejercicio debe armonizarse con el bien social, tal como se concibe en el artículo 70° de la Constitución Política del Perú. El autor plantea que el derecho de propiedad no es puramente individualista, sino incorpora un componente social estructural que da lugar a una interpretación desde un punto de vista colectivo.

Aunque las figuras de posesión son aplicables al uso de AIoT en relación con los datos no personales, aplicar los conceptos tradicionales de propiedad de los derechos reales no compatibiliza con los objetivos de una transformación digital sostenible, equitativa y accesible. Dado que los datos constituyen bienes intangibles y no corpóreos, su regulación no puede depender de criterios tradicionales como la posesión física, por lo que garantizar acceso y promover su uso es crucial para fomentar la interoperabilidad, ejercer efectivamente el derecho a la información, promover el mercado de libre competencia y fomentar la innovación tecnológica.

En este marco, resulta pertinente transcender el enfoque funcional del derecho de propiedad hacia los datos no personales, no como activos exclusivos de quien los genera o procesa, sino como bienes cuyo uso, acceso y reutilización deben estructurarse en base al interés o beneficio común que pueden producir. Esta medida, hace posible atribuir a los datos un “atributo de utilidad”, sustentando los mecanismos de acceso compartido o formas de cotitularidad de derechos, siempre que ello esté en armonía con otros derechos fundamentales y legítimos intereses.

La gobernanza de los datos no personales debe superar el dilema público-privado, y debe orientarse a modelos jurídicos que se basen en una distribución equilibrada del valor y de la obtención de este mediante el acceso, a partir del enfoque de responsabilidad, proactividad y que predomine la función social. Urge una revisión con detenimiento la aplicación de marcos jurídicos actuales que directa o indirectamente representan una relación economicista, y avanzar a modelos más distributivos. Ello requiere adoptar esquemas que reflejen que aún en la

complejidad, los intereses plurales subyacen al ecosistema de datos personales y deben proteger de manera equitativa.

3.2. Concepto de la propiedad de la propiedad intelectual

El régimen de la propiedad intelectual se remonta desde el arquitecto Filippo Brunelleschi creador de la cúpula de Santa María del Fiore en Florencia, en el Siglo XI, que señaló haber inventado una embarcación de hierro que podría reducir los costos de transporte de mármol por los ríos; sin embargo, a pesar de ello se negó a publicar su creación a menos que Florencia le diera derechos sobre tal creación y pudiera garantizar la explotación exclusiva de dicho bien (Diaz, 2022). Esta situación de Brunelleschi, basada en la exclusividad de la explotación de un bien inmaterial que se produce a partir del intelecto humano, es lo que establece los cimientos del sistema de protección de la propiedad intelectual junto con la exigencia de otros derechos exclusivos que se otorgaban como un premio al fomento de la innovación humana.

Para Lohmann (2004), todas las creaciones derivan del intelecto humano, tanto las obras artísticas como las invenciones técnicas. Todas poseen un origen común: son producto del intelecto. Aunque sus funciones y aplicaciones pueden ser distintas, ambas encuentran su origen en la creatividad del ser. Sin embargo, señala que es una “restricción impropia” usar la expresión de propiedad intelectual únicamente para las obras literarias o artísticas y no a las invenciones técnicas, cuando ambas comparten el mismo origen intelectual (p. 94).

Este sistema de propiedad, a diferencia de los derechos reales, no implica un dominio absoluto sobre un bien, sino el reconocimiento de ciertos derechos específicos sobre una creación intelectual que reúna condiciones alrededor del concepto de la originalidad. Estos derechos, que recaen sobre bienes intangibles, son de naturaleza temporal, pueden ser atribuidos a más de una persona y se dividen en dimensiones morales y patrimoniales.

Además, solo los derechos patrimoniales que recaen sobre un bien inmaterial son pasibles de uso, explotación o transferencia, ya que tienen un contenido económico que se flexibiliza, a diferencia de los derechos morales que poseen un objeto de protección más amplio e íntegro, centrado en la atribución de autoría y el reconocimiento de originalidad a un sujeto. A diferencia de los derechos reales, que son plenos, exclusivos u perpetuos, la propiedad intelectual se

caracteriza por su alcance limitado y funcional, evidenciando que el carácter absoluto del derecho de propiedad no es un requisito esencial en este ámbito.

La titularidad, como se ha desarrollado en el Decreto Legislativo No. 822 Ley de Derechos de Autor, es la calidad del titular de derechos reconocidos por una ley en específico y se divide en la titularidad originaria y derivada. Este concepto de titularidad destaca una característica que atribuye un factor de poder sobre un bien intangible y permite exigir garantías sobre una invención. A comparación de los derechos reales, donde es el propietario quien tiene título sobre una cosa o la posee en un sentido físico, siendo la cosa un ente material pasible de ser percibido por los sentidos.

Es importante destacar que aunque ambos conceptos otorgan ciertos derechos sobre una cosa en su forma material o inmaterial, la propiedad intelectual refiere a bienes intangibles y temporales, mientras que los derechos reales suelen estar vinculados a bienes físicos y de carácter perpetuo. Además, aunque los datos no personales puedan ser valiosos, no tienen características necesarias para ser tratados o protegidos bajo las prerrogativas de los derechos de autor o como invenciones. Por el contrario, son totalmente dinámicos, cambiantes, sujetos a modificaciones y pueden ser generados de múltiples fuentes lo que dificulta la atribución exclusiva a un titular.

En el sector minero, por ejemplo, los datos no personales obtenidos a partir de sensores de los equipos o procesos, no constituyen como tal “una obra” en sentido estricto de los derechos de autor. Ello se debe a que carecen de creatividad y originalidad que exige la normativa, sino que se limitan a reflejar hecho o mediciones del entorno de manera objetiva. Por ello, dichos datos no personales no conllevan al otorgamiento de un derecho exclusivo a favor de un solo sujeto, pues su contenido fáctico los posiciona fuera del ámbito de protección propia de la propiedad intelectual. Por ejemplo, aquellos datos generados por las perforadoras o excavadoras durante el proceso de extracción de mineral, que recopilan y procesan datos continuamente. Estos datos son esenciales para que otros actores, como los proveedores de mantenimiento o desarrolladores de software analicen el rendimiento de los equipos y puedan realizar recomendaciones para hacer más eficiente la operación, mas no contienen un grado de invención importante o relevante que genere conocimiento sobre un proceso como tal y, en consecuencia no es un objeto protegible por la propiedad intelectual.

La idea de que los datos puedan ser utilizados y compartidos por diferentes actores para diferentes fines, como en el caso propuesto, por ejemplo para el mantenimiento predictivo y optimización de la producción, demuestra que no es necesario un único titular o propietario, con mayor razón cuando la generación de estos se da en contextos de pluralidad de agentes. Implementar un enfoque colaborativo promueve el acceso a la información, la interoperabilidad de los sistemas y permite explotar el valor de los datos.

Esto contrasta con el sistema de propiedad intelectual, el cual se sustenta en derechos exclusivos y restricciones de uso. De aplicar este sistema de protección a los datos no personales, obstaculizaría seriamente el desarrollo tecnológico y la innovación. En lugar de fomentar el acceso, la interoperabilidad y la reutilización (condiciones esenciales para el aprovechamiento de los datos en entornos de inteligencia artificial o AIoT), este sistema podría conducir a una privatización excesiva de los datos, generando lo que la literatura denomina *anti-commons*, donde múltiples derechos con propiedades de “exclusión” se manifiesta en un bloqueo del uso eficiente de un recurso.

Para Lohmann, existe una dificultad por concebir una disciplina jurídica unitaria que agrupe todas las modalidades de creación, debido a la heterogeneidad de las formas y objetos creativos. A pesar de ello, sostiene que es posible identificar ciertos elementos comunes en los derechos intelectuales, como el sujeto creador, el objeto protegido y el contenido del derecho, siempre que se proceda por "vía de reducción y abstracción" de sus características esenciales. En palabras del autor, lo que da unidad al régimen jurídico de los derechos intelectuales es "la tutela de la inteligencia y habilidad humana en ciertas de sus manifestaciones" y, en consecuencia, su finalidad es la "protección contra la no autorizada utilización del fruto del intelecto ajeno" (2004, p. 94).

Este fundamento esencial de los derechos intelectuales dificulta e impide extender su aplicación a los datos no personales, porque no siempre son fruto directo del intelecto o creatividad humana. Muchos son generados de forma automática y en grandes cantidades, por lo que no tienen un origen derivado de un proceso de creación intelectual propia de un individuo, sino que son recopilados por instrumentos o técnicas, condiciones del entorno, etc.

En ese sentido, se hace cada vez más evidente que aplicar el sistema de propiedad intelectual no puede ser el marco normativo adecuado para regular el uso y acceso a los datos no personales, justamente porque su estructura excluyente contradice los principios de apertura y

reutilización que subyace al ecosistema digital contemporáneo y porque supondría confundir el objeto final de tutela de este régimen. Si la finalidad del derecho de autor o propiedad industrial es proteger las creaciones originales, entonces no puede ser trasladada a objetos que carecen de manifestación original.

La exploración de los derechos de propiedad intelectual como una forma de regulación para los datos no personales ha sido una tendencia que buscaba brindar mayor seguridad jurídica a quienes invierten en los procesos de recopilación y el procesamiento de estos datos. En este contexto, es importante analizar cómo podrían establecerse derechos sobre los datos no personales en el AIoT, bajo una categoría diferenciada y más adecuada a la que plantea el sistema de derechos de propiedad intelectual**.**

Como se desarrolla en un artículo Eckardt & Kerber, en el estado actual de las cosas se ha reconocido un control de facto de los datos no personales por parte del "titular de datos" (o "*data holder*" como concepto abordado por el *Data Act* de la Unión Europea) quien ostenta la posesión exclusiva de los datos a un nivel técnico, puede compartirla con otros a través de un contrato de licencia para extraer valor, tal y como un titular de una invención ejerce sus derechos de propiedad intelectual (2024).

Este intento por replicar los conceptos de propiedad intelectual a los datos no personales podría tener implicaciones económicas y tecnológicas contraproducentes. La restricción en el acceso a los datos, a través de derechos exclusivos y licencias, podría obstaculizar la competencia y la innovación. Si solo unos pocos actores tienen acceso a los datos necesarios para desarrollar nuevas tecnologías o mejorar los procesos existentes, esto podría crear barreras de entrada para nuevos agentes que pretenden dar uso a los datos y de empresas tecnológicas que no tengan acceso a datos clave o específicos.

También se ha dado la posibilidad de reconocer los derechos *sui generis* a los llamados "productores de datos", es decir, quien tiene control, los recopila o almacena a partir de un primer contacto con los datos, lo cual genera algunas limitaciones técnicas como jurídicas. La lógica de propiedad intelectual se basa en la originalidad, la creatividad o el esfuerzo sustancial en la compilación de la información, elementos que los datos generados automáticamente por dispositivos industriales no cumplen.

Además como advierten algunos autores, la creación de un derecho de productores de datos podría no ser eficiente, e incluso contraproducente, porque el reconocimiento de un derecho de propiedad intelectual a favor del usuario o propietario de un dispositivo conectado (a Internet, como lo puede ser el AIoT) introduciría cargas excesivas en los procesos de licencia sobre los fabricantes, al obligar a negociar licencias individuales con cada “supuesto productos” de datos (Drexl, 2020, p.4).

Eso evidencia que extender la lógica de la propiedad intelectual a los datos no personales no solo genera disputas jurídicas y económicas, sino que consolida la asimetría de poder en mercados de datos. En lugar de promover el acceso, refuerza mecanismos de exclusión bajo cláusulas contractuales de cesión total o licencias restrictivas. Resulta más coherente optar por el diseño de derechos de acceso que no sean renunciables, que sean funcionales e ignoren la lógica patrimonial de la propiedad intelectual.

Asimismo, extender estos mecanismos de los derechos de propiedad intelectual a los datos no personales, sin considerar su origen y naturaleza particular, no solo desvirtúa el objeto de protección de la propiedad intelectual, sino que además afecta negativamente el ecosistema de innovación, sobre todo cuando el valor se genera a partir de la circulación libre y la reutilización e interoperabilidad de grandes volúmenes de datos.

Esta enmarcación forzosa podría crear monopolios sobre los datos, en el cual pocos tendrían dominio del mercado y control exclusivo de estos, perjudicando la competencia y la evolución de las nuevas tecnologías en tanto no existirían datos disponibles. Así también, se generan menos fuentes de datos y la obtención de estos sería altamente costosa. Pretender institucionalizar la figura de los datos no personales bajo los parámetros del sistema de propiedad intelectual carece de fundamento conceptual y práctico.

Por ello, es necesario fomentar la creación de un nuevo marco regulatorio que se enfoque en promover el acceso abierto a los datos no personales bajo estándares de interoperabilidad y que distribuya los derechos de manera equitativa, permitiendo una utilización eficiente, ética y transparente, maximizando su valor e impacto a la economía y sociedad.

3.3. Concepto de titularidad desde la perspectiva del derecho de protección de datos personales

En el ámbito del derecho de protección de datos personales, el concepto de “titularidad” representa el poder jurídico concedido al sujeto sobre el cual se recopilan sus datos relacionados a su esfera más íntima y personal. No obstante, este concepto no equivale a un derecho de propiedad en el sentido tradicional, ya que los datos permanecen en posesión de una persona o entidad distinta a la del titular del dato, aún si el dato personal es intrínseco a la existencia de una persona. Así, se concede al titular un derecho de autodeterminación informativa, es decir la capacidad que le permite controlar la recolección, el almacenamiento y en general, el uso de sus datos personales sin que ello constituya una propiedad absoluta sobre ellos cuando se establecen excepciones a la autodeterminación.

Desde luego, la postura que establece la delimitación del régimen diferenciador aplicable a los datos no personales se debe basar en la distinción del objeto de protección del derecho fundamental de protección de datos personales. Se debe, además, clarificar los conceptos alrededor del dato personal y sus alcances. Es decir, si el objeto de protección o la finalidad del derecho existente es el mismo para ambas categorías de datos y si el contenido de la regulación es aplicable en igual condiciones para ambos tipos de datos, personales y no personales.

En primer lugar, Para Guichot (2005), el objetivo del derecho de protección de datos personales es la protección de la vida privada y el libre desarrollo de la personalidad y su objeto de protección son los datos personales. Pero es en la determinación del objeto que existen mayores dificultades conceptuales. Esto es, en el caso de la protección de la vida privada por la acumulación de información al que se realiza tratamiento para la generación de perfiles, ¿conlleva a determinar que todo lo que diga o refiera a algo de un sujeto, es dato personal?

Para Hert y Gutwirth (2006) el derecho a la protección de datos no debe confundirse con el derecho a la vida privada. Aunque históricamente fueron tratados como equivalentes, la protección de datos personales tiene una dimensión autónoma que abarca más que la privacidad. También se refiere a la gobernanza del tratamiento de la información personal, incluyendo decisiones automatizadas, vigilancia, perfiles, y poder informacional y permitiendo que el control sobre estos inhiba a quienes se encuentran en el poder para usarlos indiscriminadamente.

Además, Lynskey (2015) argumenta que el objeto protegido en el derecho a la protección de datos no es solo la privacidad, sino también la autonomía, la libertad individual y la limitación del

poder estructural que deriva del control de datos personales. Su enfoque se centra en cómo los datos permiten influir en comportamientos, decisiones y derechos, más allá de si afectan la "vida íntima". Por su parte Weber (2013) advierte que la definición de dato personal es cada vez más ambigua, debido a las tecnologías emergentes como la IA y el *Big data*, por lo que es difícil establecer límites claros al objeto protegido y esto genera riesgos de sobreprotección (paralización de actividades legítimas) o desprotección.

Por otro lado, respecto al concepto de los datos personales como tal, el autor también señala que el derecho europeo, el concepto de dato personal es objeto de una interpretación más alta que ha asumido el Tribunal Constitucional de España. También sigue la tendencia que ya no hay datos sueltos y que no solo se protege la privacidad de la persona sino también otros derechos fundamentales (Guichot, 2005, p. 146). Esta doctrina confirma que existen datos que exceden la esfera del derecho de protección de datos personales y por ello, puede y debe ser regulado bajo exigencias que limitan el tratamiento al consentimiento y la aplicación de principios restrictivos.

Tal como señala Nelson Remolina (2012), el tratamiento de los datos personales se sustenta en un conjunto de principios rectores que derivan de la protección constitucional del derecho fundamental al habeas data. Esta categoría de información que permite identificar o asociar a una persona natural "determinada o determinable" afín al concepto desarrollado por la normativa colombiana, está sujeto a un régimen jurídico restrictivo. Este régimen solo legitima el tratamiento de los datos, siempre que se obtenga un consentimiento previo, expreso e informado del titular, o en mandatos legales basados en principios de proporcionalidad, legalidad, minimización y otros (p. 133).

Este modelo concibe la "titularidad" sobre los datos personales como una facultad y no como propiedad, consecuente al ejercicio de un derecho fundamental de carácter personalísimo, cuyo objetivo es proteger la autodeterminación informativa, así como la intimidad y la dignidad humana. No obstante, los datos no personales no poseen la misma protección constitucional ni mucho menos son objeto de protección de la normativa de protección de datos personales, en tanto su tratamiento no se determina por la titularidad de una persona natural, sino por su utilidad en los procesos tecnológicos o industriales.

Ahora bien, por regla general, el tratamiento de datos y las normas que regulan el tratamiento son de carácter restrictivo, porque se limita a establecer supuestos en los que se pueden tratar los datos personales y bajo qué límites y parámetros. Más aún en el caso del tratamiento de datos sensibles, al ser una categoría especial de datos personales que requiere una protección especial. En consecuencia, el conocimiento y consentimiento del titular del dato es la base para que se permita el tratamiento de estos, y dicho mandato legal está expresamente previsto tanto en normas nacionales como en derecho comparado. El consentimiento informado por parte del titular es el título jurídico habilitante y primordial que permitirá el tratamiento de los datos y únicamente no se requiere consentimiento en una lista taxativa y supuestos limitados, que exige un mandato legal y que no se inhibe del deber de informar que es necesario contar con un sistema transparente en el tratamiento de estos datos.

En el caso del Reglamento General de Protección de Datos de la Unión Europea (RGDP), se reconocen derechos a los titulares de los datos, pero este reglamento no regula la propiedad de los datos en sí. En su lugar, se enfoca en regular las relaciones entre titulares de los datos y los responsables del tratamiento, que puede ser persona o entidad que gestiona y define su tratamiento. El RGPD promueve el control sobre los datos personales mediante el derecho a la autodeterminación informativa, que protege el control de los titulares sobre sus propios datos pero no busca establecer una categoría jurídica que permita la explotación económica de los datos personales en contextos de uso de tecnologías emergentes.

En cuanto al concepto de autodeterminación informativa, el Tribunal Constitucional Peruano ha determinado en el Expediente N.° 02140-2020-PHD/TC que consiste en:

> *"Una serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal"* (fundamento 7).

Este concepto de titularidad que se aplica específicamente a datos personales, ha sido objeto de debate en su posible extensión a los datos no personales, con la idea de que los usuarios pueden ser titulares de derechos sobre los datos no personales. Los datos no personales tienen características que no los hacen aptos para ser considerados como propiedad exclusiva de un

sujeto o inherentes a su persona o su personalidad, por su dinamicidad y características económicas y estructurales que se han desarrollado de manera precedente.

En base a lo expuesto por diversos autores, el concepto de dato personal trasciende la protección de la vida privada, abarcando toda información que permita identificar a una persona. Esta ampliación conceptual genera desafíos normativos, especialmente cuando se contrapone a datos de naturaleza técnica o industrial que, por no estar vinculados a un sujeto o la esfera personal de un individuo, no califican como datos personales.

En este contexto, no resulta adecuado otorgar a los datos no personales una lógica basada en garantías de derechos fundamentales. Su regulación debe orientarse hacia fines funcionales, estratégicos y económicos, promoviendo la distribución equitativa del valor generado, sin reducir su utilidad exclusivamente a criterios de rentabilidad, sino reconociendo su impacto en el beneficio colectivo. Este reto exige delimitar claramente el objeto protegido por el derecho a la protección de datos personales y diferenciarlo de los datos no personales, a fin de evitar traslaciones indebidas de nociones estrictamente proteccionistas.

Por tanto, se requiere un marco normativo autónomo aplicable a los datos no personales, que fundamente la titularidad en principios de acceso seguro, reutilización responsable, interoperabilidad, transparencia y equidad bajo un marco regulatorio flexible y dinámico. Mientras que el tratamiento de datos personales responde a la necesidad de proteger al individuo frente al poder informacional bajo un sistema tutelar de derechos y restrictivo, el régimen de los datos no personales debe enfocarse en su valor estratégico dentro del ecosistema digital, habilitando modelos de titularidad compartida y gobernanza en beneficio colectivo.

3.4. Necesidad de un marco regulatorio que supere los conceptos tradicionales de propiedad

En base a lo expuesto hasta ahora, se evidencia la necesidad de una regulación específica para la atribución de derechos sobre los datos no personales que contemple la disponibilidad de los datos en término de acceso y uso no restringido, intercambio y explotación económica compartida, sin que predomine un enfoque restrictivo en las regulaciones o en la apropiación exclusiva de los datos.

Con un modelo equilibrado, los datos no personales se utilizarían en el mercado bajo parámetros de disponibilidad en términos de acceso e interoperabilidad, permitiendo que los usuarios y fabricantes del AIoT u otros proveedores estén facultados a compartir datos con terceros (privados o públicos), independientemente de la relación de competencia directa o indirecta. Con la asignación equilibrada de titularidad y tomando en consideración los intereses de los diversos actores intervinientes, se podría generar una situación de bienestar compartido en el mercado digital y sobre todo en el fomento de la innovación y competitividad en igualdad de condiciones.

Dado que los datos no personales tienen una naturaleza no rival, es necesario promover esquemas funcionales regulatorios mediante disposiciones que asignen equitativamente el valor de los datos y la posibilidad de beneficiarse de ellos, pero estableciendo definiciones claras y límites razonables que no desincentiven la inversión y el progreso a nivel de tecnología. Para ello, en lugar de adoptar un enfoque de propiedad exclusiva o excluyente, se requiere un modelo que asigne derechos específicos, referidos al acceso, uso, intercambio y explotación económica, bajo condiciones que aseguren una distribución justa, equitativa y no discriminatoria, especialmente en contextos tecnológicos altamente competitivos.

Ahora bien, los datos no personales son intangibles, fácilmente reproducibles, no rivales en su uso y no excluibles, diferenciándolos de los bienes tradicionales. Al respecto Cat Atik, señala que la propiedad como concepto jurídico implica exclusividad y control absoluto, lo que no se adecua a la naturaleza de los datos no personales. Según el marco tradicional, la propiedad no es fácilmente adaptable a recursos que pueden ser utilizados simultáneamente por múltiples actores sin que ello implique su pérdida o agotamiento (2020).

Por ello, el término “titularidad” se alinea mejor a la naturaleza compartida y no rival de los datos no personales, lo que permite establecer derechos específicos como el acceso, uso, intercambio, explotación y control sin que se configuren limitaciones absolutas. Este término además facilitaría la gobernanza compartida entre diferentes actores, es decir que un sistema de titularidad podría otorgarse a múltiples individuos derechos bajo ciertos criterios, adoptando la naturaleza múltiple de la propiedad intelectual, pero atribuyendo los derechos específicos a las necesidades regulatorias de las que se aborda en el presente trabajo.

Para Eckardt & Kerber tratar los datos como un activo de propiedad exclusiva puede llevar a la monopolización y al acceso restringido, limitando la innovación y la competencia. Un modelo

basado en el "titular de datos", en cambio, reconoce que múltiples actores (como fabricantes de dispositivos, usuarios y terceros) pueden tener intereses legítimos en acceder y utilizar los datos no personales, promoviendo la colaboración y la innovación (2024).

De igual modo, estos autores opinan que si los datos del IoT se tratan como propiedad exclusiva, los fabricantes o proveedores de plataformas pueden imponer acuerdos de licencia restrictivos, lo que genera bloqueo de datos y reduce la interoperabilidad. Un marco basado en el "titular de datos" puede mitigar estos riesgos garantizando derechos de acceso a datos para las partes interesadas, promoviendo la competencia justa y evitando comportamientos monopolísticos.

En la misma línea crítica, Jara (2021) comenta que los datos no personales no pueden ser objeto de un derecho de dominio conforme lo establece el Código Civil (haciendo referencia a los derechos reales), puesto que no encaja en la clasificación de bienes corporales e incorporales. No obstante, deja abierto el análisis sobre si estos pueden estar comprendido en el ámbito de protección que se le otorga a las bases de datos o procesos analíticos que sí son protegidos por los derechos sui generis o inclusive a través de los secretos industriales.

En esta línea, el concepto de "titular de datos" ha sido defendido como un instrumento que permite desplazar el enfoque normativo desde la propiedad hacia la responsabilidad, al posibilitar que los marcos regulatorios impongan deberes de transparencia, el intercambio de datos y la seguridad, asegurando un uso ético y legal. Este modelo facilita una mejor gobernanza, ya que desplaza el enfoque de la propiedad de los datos hacia la responsabilidad en su manejo y utilización (Díaz Vera, 2023).

En conjunto, estas consideraciones revelan la necesidad de desarrollar un marco normativo especializado que se aparte de los esquemas tradicionales de la propiedad, para adoptar la nueva regulación a criterios de interoperabilidad, acceso, promoción de la competencia y el incentivo de la innovación. Es pertinente que se adopten conceptos uniformes basados en regulaciones internacionales en la medida que puedan alinearse y aplicarse de manera idónea, priorizando el acceso controlado y justo, por encima de la propiedad exclusiva, dejando margen para permitir acuerdos dinámicos y flexibles sin crear restricciones al flujo de la información.

4. Análisis sobre la propiedad de los datos no personales

En el contexto económico y jurídico, los datos representan un valor auténtico y tutelable, aunque su valoración puede medirse desde diferentes enfoques por ellos se les otorga un carácter heterogéneo. Como se ha advertido, Coyle sustenta también que los datos son un recurso económico clave con características únicas: no rivalidad, intangibilidad y la posibilidad de ser utilizados múltiples veces sin agotarse. Estas propiedades generan un valor social significativo, siempre que los datos sean gestionados de manera adecuada (2022).

Al no adaptarse a los marcos preestablecidos, es necesario crear marcos regulatorios para fomentar la utilización eficiente de los datos, ya que son propensos a acumularse en manos privadas, generando efectos de bloqueo y reduciendo su potencial social y económico. A partir de ahí se evidencia la necesidad de garantizar un acceso equitativo a los datos para prevenir la concentración en los mercados de datos o la formación de monopolios que limitan su aprovechamiento por parte de otros actores

Además, el valor social y económico que los datos representan como recursos estratégicos para la innovación, la eficiencia económica y la creación de nuevos mercados, justifica plenamente la necesidad de tutela jurídica. A esto se suma la participación de múltiples actores (usuarios, proveedores, fabricantes), quienes contribuyen económica e intelectualmente a la generación de estos datos y pueden tener intereses legítimos sobre su uso y explotación comercial que beneficia a particulares y al público en general.

Por lo tanto, resulta indispensable contar con una regulación clara y especializada que evite que los actores en posiciones dominantes en la generación, uso y procesamiento de datos restrinjan el acceso o uso de estos. Esto es fundamental para prevenir la creación de barreras de entrada y garantizar la competencia justa, promoviendo así la innovación y el desarrollo tecnológico en el mercado de datos.

Ahora bien, como ya hemos mencionado, las características de no rivalidad, reproducibilidad e intangibilidad de los datos no personales plantean cuestionamientos y desafíos significativos para la atribución de tutela jurídica mediante derechos de “propiedad” sobre ellos. Por su naturaleza, los datos no personales son fácilmente reproducibles y pueden ser utilizados simultáneamente por múltiples actores, lo que dificulta la aplicación de un concepto tradicional de exclusividad asociado a la propiedad, puesto su apropiación bajo ese régimen constituye .

Autores como Drexl argumenta que regular los datos no personales permite romper los esquemas de bloqueo o "*data locked-in*"**,** y para ello propone establecer un acceso regulado que considere las características técnicas de los datos y su potencial para generar beneficios sociales. Según el autor, los principales desafíos de atribuir derechos de propiedad a los datos no personales son la dificultad para intercambiarlos y las barreras a la competencia que podrían generarse. Dado que los datos poseen un valor intrínseco para la sociedad, imponer exclusividad limitaría la obtención de estos beneficios (2018).

La posición de Drexl es crítica, ya que considera que atribuir derechos de propiedad exclusiva a los datos restringiría su acceso incluso desde su generación, lo que resultaría en altos costos de transacción, sofoca la innovación y dificultaría la competencia en mercados secundarios. En contrapartida, el autor propone establecer derechos de acceso, diseñados específicamente para sectores donde los datos no personales son esenciales. Esto permitiría que múltiples actores se beneficien de los datos mediante una gobernanza compartida, fomentando un acceso más eficiente y con menos restricciones.

A su vez, Eger & Scheufen comparan los datos con un motor clave para la economía digital. Señalan que los mercados tienden a concentrarse en grandes actores, como Meta o Google, debido a los *network effects*, donde el valor de los datos aumenta proporcionalmente al volumen de usuarios que los utilizan. Asimismo, destacan que las economías de escala juegan un papel importante: aunque los costos iniciales de recolección y procesamiento de datos son altos, el costo marginal de replicarlos o procesarlos adicionalmente es muy bajo. Por ello, los autores proponen una regulación que garantice un acceso justo y evite una concentración excesiva de poder de mercado, fomentando así un ecosistema más competitivo e inclusivo (2024).

En tanto, estos últimos autores reconocen que los derechos de propiedad pueden tener sentido en situaciones particulares, como cuando los costos de generación de datos son elevados. Sin embargo, advierten que la exclusividad puede generar problemas de concentración de mercados. Por ello, proponen que los derechos de acceso se establezcan de manera que fomenten el intercambio y aseguren la disponibilidad de datos, promoviendo así la innovación y la competencia.

La atribución de propiedad sobre los datos no personales constituye un desafío jurídico y económico, especialmente en contextos como el uso del AIoT o productos conectados que se

producen en las relaciones B2B. Este análisis es fundamental para delimitar los derechos y responsabilidades de los actores involucrados, promoviendo tanto la innovación como la competencia justa.

Desde una perspectiva de una posible regulación a través de la atribución de propiedad, Drexl (2018) ha abordado la cuestión como una discusión entre los conceptos titulares de datos y propietarios. El autor señala que si bien los fabricantes de AIoT u otros productos conectados pueden comercializar los datos en calidad de titulares también pueden excluirlos a terceros. Esto se debe a que existe un control de facto que faculta la exclusividad, también de facto, aún si no exista contrato de licencia, regulación o acuerdo de exclusión que le atribuya un derecho de propiedad sobre los datos.

Este mismo autor introduce una idea relevante que ya hemos abordado previamente: propone dejar en segundo plano la cuestión de quién debería ser el propietario de los datos y centrarse en estos, como bienes no rivales, que pueden ser objeto de derechos. Según el autor, los datos, al ser información no rival que puede generar beneficios sociales, deberían estar sujetos a derechos de acceso, en lugar de derechos de propiedad. Esto se justifica desde un interés público en garantizar el acceso a la información (2018).

Por otro lado, aunque los datos personales pueden estar asociados a una titularidad atribuida a la persona sobre quien recae la información, su regulación no les otorga derechos de propiedad formal. En su lugar, garantizan cierta autodeterminación informativa y un control sobre estos datos. Es destacable que los datos personales, al ser utilizados de manera legítima y masificada, permiten la generación de derechos atribuibles en contextos específicos.

Eckardt y Kerber han analizado doctrinas actuales relacionadas con la autorregulación de los privados en el flujo de datos no personales en las industrias. Sus estudios revelan una tendencia significativa hacia el control exclusivo de facto sobre estos datos por parte de los actores privados.

Asimismo, aunque el Data Act de la Unión Europea, sobre el cual se basa parte de este análisis, no aborda específicamente la "propiedad" de los datos no personales, sí regula aspectos clave relacionados con el acceso, uso y explotación de estos datos. En particular, interviene en cinco

áreas cruciales dentro del contexto del intercambio de datos generados por productos conectados en el Internet de las Cosas (IoT).

Finalmente, parte de la gobernanza de los datos implica crear condiciones que no solo aseguren una estructura estandarizada y equilibrada para el flujo de datos, sino también una delimitación clara de los derechos, su ejercicio y los actores legitimados. Esto permite mapear el impacto de los incentivos en la dinámica de compartir y utilizar los datos, promoviendo la interoperabilidad.

Para la OECD (2015), se necesitan mejores regímenes de gestión de datos para superar las barreras al acceso, intercambio e interoperabilidad. Los elementos clave para una gobernanza eficaz incluyen el acceso y la reutilización de los datos, la portabilidad e interoperabilidad, la vinculación e integración, la calidad y conservación, la "propiedad" y el control, así como el valor y la fijación de precios.

La cuestión de la "propiedad" es especialmente controvertida cuando se trata de datos, y más aún en el caso de los datos personales. A diferencia de otros intangibles, los datos suelen implicar la asignación compleja de derechos entre múltiples partes interesadas. Estas partes tienen, normalmente, diferentes niveles de poder sobre los datos, dependiendo de su rol (2015).

En Loshin (2002, citado en OECD, 2015) identifica algunos *stakeholders* que podrían reclamar la propiedad de los datos:

- Creador: quien crea o genera los datos, o quien los utiliza.
- Recopilador: quien selecciona y recopila la información de diferentes fuentes.
- Empresa: aquella que genera o recibe datos dentro de sus operaciones y que los considera de su propiedad.
- Decodificador: en entornos donde los datos están bloqueados o en formatos codificados, la parte que desbloquea dicha información podría reclamar la propiedad.
- Empaquetador de datos: quien recopila información específica para venderla en mercados concretos o a consumidores particulares.
- Lector como propietario: el valor de cualquier dato leído es absorbido por el lector, quien agrega esta información a un repositorio propio, ganando valor en el proceso.
- Sujeto de los datos: quien reclama la propiedad de los datos relacionados consigo mismo, generalmente en respuesta a otra parte que también reclama derechos sobre los mismos datos.

- Comprador o licenciatario como propietario: quien compra o adquiere una licencia para los datos podría reclamar derechos de propiedad sobre estos.

Hasta aquí, podemos concluir que los derechos de “propiedad exclusiva” generan mayores externalidades negativas sobre el uso conjunto, libre y equitativo de los datos. Estas tensiones entre los actores intervinientes conducen a restricciones en el acceso efectivo, lo que impactaría negativamente en los avances de la innovación tecnológica y en la competitividad de los mercados. Por ello, nuevamente reafirma la posición de que resulta necesario excluir los derechos de propiedad exclusiva como concepto regulatorio en materia de datos, priorizando en su lugar derechos de acceso, gobernanza compartida e interoperabilidad que promuevan un ecosistema más equilibrado y eficiente.

4.1. Titularidad de los usuarios

La relevancia de los datos generados en las relaciones B2B que involucran el uso de tecnologías AIoT plantea interrogantes sobre la titularidad de los datos y la atribución de derechos sobre los datos no personales generados. Esta situación se ve influenciada por diversos factores, como la disposición del lugar donde se recopilan los datos, el pago realizado por los servicios prestados y/o la disposición de los equipos necesarios para la ejecución de los dispositivos.

Desde la perspectiva de los derechos exclusivos y la concepción tradicional de la propiedad, en las relaciones B2B el usuario suele considerarse como el titular de los datos no personales. Esto se debe a que el usuario adquiere el producto o servicio y, en consecuencia, lo utiliza en calidad de propietario. Por ejemplo, en el sector minero, las minas adquieren servicios o productos de AIoT para integrarlos en su infraestructura. Los datos capturados por estos dispositivos son analizados y transformados en información útil, lo que permite generar gráficos y resultados basados en necesidades específicas.

Particularmente, en las relaciones B2B, los datos no personales que se generan a partir de la implementación de sistemas AIoT o similares, no son producidos de forma aislada, por el contrario, requieren de la intervención conjunta entre usuarios y dispositivos. Esta dinámica se posiciona como un argumento a favor de los usuarios de tecnologías para legitimarse como titulares de los datos no personales.

Atribuir la titularidad de los datos a los usuarios también podría fomentar la innovación y el desarrollo de nuevas aplicaciones a partir de la puesta en disposición de los datos no personales a otras industrias o incluso a proveedores que proponen alternativas innovadoras. Si los usuarios tienen control sobre los datos generados, podrían explorar formas más eficientes de utilizarlos, adaptándolos a las necesidades específicas de su negocio y sector (Eger & Scheufen, 2024). Este control permite a los usuarios personalizar la tecnología, maximizando así los beneficios económicos y sociales, además resulta especialmente relevante en mercados competitivos, donde la capacidad de innovar utilizando datos propios puede convertirse en un diferenciador clave.

Por otro lado, como se mencionó anteriormente, los usuarios de dispositivos AIoT usualmente realizan inversiones significativas en la adquisición, instalación y mantenimiento de los dispositivos, así como la adaptación de los espacios a una infraestructura idónea para procesar y analizar los datos. En el caso del sector minero, estos instalan dispositivos para responder a las condiciones de dificultad de las minas, pero es indispensable que, ante estos desafíos de infraestructura, puedan contar con redes que provean de conexión adecuada o tecnologías que permita contar con servidores de capacidad suficiente para almacenar la información.

En consecuencia, como manifiestan Coyle & Diepeveen, los usuarios desempeñan un papel crucial como co-generadores de datos, dado que proporcionan el entorno y las actividades que originan esta información en el uso de los sistemas de tecnología. Por tanto, tanto los proveedores de tecnología como los usuarios contribuyen directamente a la creación de los datos. Aplicar el principio de justicia distributiva sugiere que quienes hacen inversiones sustanciales en la producción de datos deben tener derecho a beneficiarse de ellos (2021). No obstante, ese principio no se reduce únicamente a un agente, sino que es posible que más de un actor interviniente realice inversiones igual de sustanciales y que posea también derechos sobre los beneficios o la expectativa.

Otro motivo por el cual en el derecho comparado, normativa como el Data Act de la Unión Europea y otras normas que forman parte del paquete de leyes para promover la economía digital, han empoderado a los usuarios, se debe a que al mantener la posesión exclusiva de los datos en manos de los fabricantes, los usuarios quedan en una posición vulnerable (Kerber, 2019) o asimétrica. Los usuarios, dependen enteramente del fabricante para acceder y utilizar los datos puesto que usualmente no poseen acceso directo. De este modo, se limita la libertad

de los usuarios para desarrollar o decidir innovar a partir de datos que sus propios equipos generan o desde infraestructura incorporada por proveedores en el despliegue de nuevas tecnologías y, en consecuencia, se limita el aprovechamiento y beneficio del uso de los datos a los diferentes actores intervinientes.

Asimismo, en relaciones B2B, los datos generados por dispositivos AIoT suelen ser altamente específicos y de gran relevancia para los procesos y operaciones estratégicas de los usuarios en contextos particulares. Otorgar titularidad a los usuarios permitiría que éstos aseguren que los datos sean utilizados para satisfacer sus necesidades específicas, protegiendo al mismo tiempo la información estratégica derivada de estos.

Por consiguiente, la titularidad de los datos para los usuarios de dispositivos AIoT permite explorar directamente el valor de los datos no personales generados a partir del contexto de sus operaciones, actividades, procesos y decisiones comerciales. Esto no solo mejora su eficiencia sino también la ventaja competitiva de ajustar y compatibilizar la información producida a sus objetivos estratégicos. De este modo, se refuerza la idea de que la titularidad compartida y el acceso a los datos no personales o industriales en contextos de AIoT son esenciales para desbloquear todo el potencial de los datos en relaciones B2B.

Ahora bien, partiendo de la idea que los datos emergen como un recurso indispensable en el uso de tecnologías AIoT, su naturaleza difiere de los recursos tangibles tradicionales como el petróleo, porque a diferencia de este, los conjuntos de datos pueden utilizarse múltiples veces y en diversas combinaciones para generar un valor adicional (Nanda & Kapoor, 2021). Esta distinción es crucial al momento de determinar los derechos de acceso de los usuarios de dispositivos conectados.

Sin embargo, el valor de los datos no es intrínseco a estos ni uniforme, ya que depende de su origen, uso y aplicación. Los datos en bruto que se recopilan en un estado original y que son almacenados en servidores sin ninguna estructura como tal, son útiles y adquieren valor únicamente en la medida que se extraiga información valiosa a través de la aplicación de algoritmos. Por lo tanto, una fase posterior de procesamiento, potencian su valor al integrarse con herramientas de análisis avanzadas, como la inteligencia artificial, que genera predicciones o provee información de alta precisión y efectividad.

Por otro lado, otorgar propiedad exclusiva sobre los datos no personales, ya sea en bruto o procesados, pondría en riesgo las iniciativas de acceso a los datos y creando prácticas anticompetitivas o discriminatorias. Esto podría ocurrir si los usuarios priorizan el uso de los datos exclusivamente con proveedores tecnológicos que ofrezcan condiciones más favorables, limitando el acceso de otros actores en el mercado que podrían desarrollar soluciones similares o para casos de investigación, entrenamiento o por último para el uso de las *startups*.

Las empresas usuarias no tendrían incentivos adicionales para compartir los datos, salvo para obtener beneficios en precios o maximizar el retorno de la inversión realizada en la adquisición de productos AIoT. Esto se debe a que, en este tipo de relaciones, los usuarios de ciertas industrias poseen necesidades específicas que estiman abordar con tecnología, y el tratamiento de datos no siempre forma parte del objeto principal de su negocio. Como resultado, esta falta de capacidad para utilizar los datos a gran escala, como lo hacen las empresas tecnológicas especializadas, deriva en la tercerización de estos servicios con proveedores, pero al limitar el uso de los datos, se produce un estancamiento en el flujo, limitando su potencial y aprovechamiento en el sector en específico.

Además, dada la ausencia de regulación específica sobre los datos no personales y el predominio de la normativa enfocada en los datos personales en el contexto digital, existe un consenso entre diferentes legislaciones en todo el mundo sobre la importancia de proteger los datos personales. En este sentido, establecer responsables de la gestión de los datos con un rol de garante fiduciario, es decir, que el gestor actúe en beneficio y concordancia con los intereses, la privacidad y otros derechos de los involucrados, podría representar un modelo viable para garantizar un equilibrio adecuado entre acceso, protección y uso de los datos.

El cuestionamiento entonces se centra en si este rol fiduciario y todas las disposiciones de la normativa de protección de datos deberían trasladarse a los datos no personales y quien debería ejercer tal control. Según señala Stuart, la idea de los derechos de “propiedad” sobre los datos no personales recae en 2 argumentos: en la “labor” y “el capital” que reclaman los datos. El primero sostiene que el dueño de la tecnología que recopila los datos es dueño también de los datos en bruto debido a que, gracias a su inversión, se generó el valor y, por otro lado, el segundo argumento que el derecho sobre los datos no debe recaer solo en el dueño de la tecnología, sino que debe estar designado en función al uso repetido de los datos y su valor se utiliza en relación con un interesado (2019, citado en Diaz, 2023).

Wiebe (2017) destaca que la legislación actual de protección de datos se aplica únicamente a la información vinculada con personas físicas, lo que excluye una gran parte de los datos no personales. Además, resalta que esta protección es un derecho relativo que no garantiza control absoluto sobre la información. En Alemania, por ejemplo, se ha planteado la posibilidad de ampliar esta legislación para convertirla en un derecho exclusivo y negociable, aunque ello entra en conflicto con el enfoque predominante que prioriza los derechos individuales sobre los datos personales.

La capacidad de los datos procesados para generar valor adicional resalta la relevancia de diferenciar entre el potencial de los datos en bruto y el valor agregado derivado del procesamiento. Es esta distinción la que permite generar información útil (Díaz, 2023). Sobre la base de dicha diferencia, se puede lograr un equilibrio entre la innovación tecnológica, la equidad y los intereses económicos de las partes involucradas.

Finalmente, si los derechos sobre los datos no personales se atribuyen únicamente a un usuario, en calidad de titular, responsable y con un rol fiduciario, las decisiones sobre el destino de los datos responderían a los intereses de una sola parte. Esto generaría un desbalance en el poder de entrada al mercado y exacerbaría la asimetría de la información, reduciendo su valor potencial por el bloqueo al acceso. Por lo tanto, para salvaguardar otros derechos fundamentales de carácter económico e incentivar la innovación tecnológica, es crucial que los datos sean accesibles y que el sector funcione bajo principios que puedan consolidar un ambiente con alta disposición de compartir datos y en condiciones de interoperabilidad.

4.2. Titularidad exclusiva de los fabricantes y/o proveedores tecnológicos

El cada vez más frecuente uso de los dispositivos y/o sistemas basados en AIoT en las industrias, acentúa el debate sobre la titularidad y el control de los datos generados a partir de estos. Los fabricantes de estos dispositivos suelen legitimar su control sobre los datos a partir de diferentes posiciones como la inversión que han realizado para obtener los datos y en la capacidad tecnológica intelectual que hace inherente la exclusividad y protección de la innovación, incluso por un tema de seguridad y confidencialidad de la tecnología que manejan en calidad de “invención”, etc.

Los actuales regímenes legales y reglamentarios asignan la propiedad a las plataformas u organizaciones que acumulan los datos en materia de datos no personales, y esto genera un

interés por otorgar derechos individuales. De esta manera, se otorga a las plataformas facultades para transferir tales datos a cambio de una compensación. Del mismo modo, buscan mantener intransferibles otros derechos, bajo la concepción de que la tecnología que aplican es protegible por propiedad intelectual y por ende, solo es posible transferir derechos económicos pero ejercer el control a partir de los derechos morales, los cuales son inalienables al autor o inventor y protegen su uso y explotación.

Los fabricantes o proveedores tecnológicos podrían mantener el control exclusivo sobre los datos que les permite desarrollar productos y o servicios, implementar mejoras, crear nuevas líneas, personalizarlos, mejorar algoritmos y garantizar eficacia y calidad de sus sistemas. Dicha exclusividad ejercida a partir de la propiedad intelectual asegura que otros competidores no puedan utilizarlo sin su autorización. En otras palabras, se vienen ejerciendo derechos de propiedad a través de licencias, en tanto esta figura concibe una solicitud de autorización de uso al titular del activo intangible y, comúnmente, una contraprestación monetaria.

Sobre esta noción de titularidad, Díaz Vera (2023) afirma que a partir del concepto de "*capital claim*" se justifica que los fabricantes y/o proveedores sean propietarios de la tecnología que recopila datos, puesto que estos poseen los datos en bruto generados por dichos sistemas y sin aquella infraestructura tecnológica que permitió la recopilación, los datos no existirían y, en consecuencia, el control exclusivo de estos datos es una forma de recuperar la inversión y fomentar la innovación.

En la misma posición, Eckardt & Kerber explican que se ha instalado un control exclusivo de facto sobre los datos no personales en el AIoT como un resultado de una configuración técnica preestablecida por los fabricantes, lo que permite excluir a otros capturar el valor de los datos, teniendo facultades para usar, compartir y monetizar los datos, así como vender esta posesión técnica.

Obtener derechos exclusivos sobre los datos del AIoT no es necesario para los fabricantes siempre que el control tecnológico a través de facultades técnicas les sirva para funcionar como si tales derechos existieran. Nuevamente, estos controles se han ejercido bajo la idea que tecnología está protegida por derechos exclusivos que se extienden de la protección de las invenciones mediante patentes o derechos de autor y, en consecuencia, también los datos que esta recopila o de las cuales se genera (Eckardt & Kerber, 2024).

Mantener el control técnico sobre los datos es esencial para garantizar la seguridad de los sistemas y la privacidad de los usuarios. Sin embargo, aunque los proveedores de tecnologías justifican dicho control por su inversión y exclusividad para fomentar la innovación, surgen limitaciones al analizar los derechos de propiedad aplicables a los datos no personales, pues estos no siempre fomentan la colaboración y el equilibrio en el mercado (Eger & Scheufen, 2024).

Además, los derechos de propiedad actuales, como los derechos de autor y los secretos comerciales, presentan limitaciones para proteger adecuadamente los datos generados por dispositivos AIoT de tal forma que puedan estar a disposición en forma de acceso por los agentes del mercado que tienen intereses sobre ellos para innovar. Trascendiendo estas limitaciones, el control de facto por los fabricantes destaca los diversos riesgos a la competencia de los mercados y a la innovación. Como señala Kerber (2024), el diseño técnico de los dispositivos AIoT facilita la posición de "*gatekeepers*" (guardianes o custodios) a los fabricantes, lo cual les permite monopolizar los mercados secundarios sobre los datos y limita el desarrollo de servicios complementarios como mantenimiento u otros, evitando la creación de ecosistemas diversos, dinámicos o inclusivos.

Los derechos de autor, aunque ofrecen garantías amplias, enfrentan desafíos que son estrictos y limitativos en la regulación. Si bien existen características que pueden considerarse beneficiosas para la protección de datos como las garantías *ex ante o* el plazo extenso de protección bajo exclusividad de un titular, las desventajas prevalecen en este tipo de propiedad porque dificultan una protección idónea de los datos no personales, tales como los requisitos de originalidad que no resulta viable a nivel técnico y por ende, la ley de derechos de autor, al ser taxativa, no se aplicaría en esta categoría de activo.

A su vez, Wiebe afirma que, si bien los derechos de autor se limitan a proteger información creada por el ser humano que contenga mandatoriamente un mínimo de creatividad o individualidad, se atribuyen derechos de "propiedad" a los fabricantes del AIoT. Sin embargo, los datos en bruto captados por sensores en las máquinas no estarían incluidos, a pesar que son el tipo de datos que más relevancia tiene en el proceso de captación de datos. Por ello, regular su libre y equilibrado acceso es crucial para la promoción de la innovación, a excepción de los casos en donde la producción automática de estos (implica recolección y procesamiento automático) implica una elemento de creatividad suficiente asignada al desarrollador de software (2017).

En lo que se refiere a los derechos de bases de datos, la actual economía de los datos tiene dificultades para adaptarse a la doble protección existente en la UE (derechos de autor y derechos *sui generis*). Por un lado, la protección de los derechos de autor sobre la estructura de los datos es discutible, por otro, la protección *sui generis* concedida para la inversión no protege los datos como tal. También, la protección de los secretos comerciales no es adecuada para el propósito, ya que se creó por razones distintas a la protección general de todos los datos y requiere que la información permanezca secreta (Van Asbroeck et al., 2017).

Asimismo, si los derechos de propiedad intelectual otorgan un derecho exclusivo a una persona o varias, en función de los derechos patrimoniales o morales que resulten de la obra o invención, entonces les permite ejercer un “monopolio” temporal sobre el activo. Esta exclusividad estimula la actividad creativa e innovativa, porque a través de las regalías del intangible, el control exclusivo es capaz de compensar otros costos sociales.

Una crítica realizada por La Diega (2022) se centra en cómo la propiedad intelectual se utiliza como un mecanismo de alquiler perpetuo, mediante estrategias de ''acumulación de derechos de propiedad intelectual'', el control de facto sobre los datos y servicios, los contratos, y las medidas técnicas de protección. Esta dinámica se ve favorecida por una regulación que tiende a inclinarse positivamente para quienes innovan y buscan proteger sus invenciones a través de la propiedad intelectual (p.281).

El concepto tradicional de propiedad, sujeto a dominio pleno que otorga al titular el uso y disfrute de un bien, se encuentra en crisis frente a los modelos digitales. En lugar de una transferencia absoluta de bienes, muchas tecnologías innovadoras, como los dispositivo IoT, se ofrecen bajo esquemas de suscripción o “*renting*” que viene a ser una suerte de “alquiler”, en los que el comprador del dispositivo adquiere el producto pero no posee control total sobre su funcionamiento ni sobre los datos que este genera.

En efecto, aunque formalmente los usuarios se presenten como propietarios del *hardware*, su acceso está restringido al servicio que el proveedor decide dar acceso o permite utilizar. Esta “limitación” se manifiesta en la inaccesibilidad a los datos capturados por el dispositivo o la dependencia de las plataformas cerradas. Similar situación se produce con los servicios de

streaming, donde el consumidor no adquiere el contenido, sino el derecho de acceso pero condicionado.

Estas estructuras contractuales redefinen los márgenes de control individual, debilitando los atributos clásicos de la propiedad y trasladando el poder efectivo al proveedor. Si aplicamos dicho modelo a los entornos industriales, en donde el proveedor de tecnología vende dispositivos inteligentes o autónomos y los usuarios no pueden acceder a dicha información sino de manera limitada, como advierte La Diega, se tolera un control absoluto sobre los datos y perpetua esquemas de exclusividad, incluso si esto amenaza la innovación y limita la entrada de nuevos competidores al mercado (2022).

A pesar de los fundamentos a favor de la posición exclusiva de los fabricantes o proveedores, existen algunos factores que ponen en cuestionamiento la adopción de una posición como esta, que podría implicar perspectivas económicas, legales e incluso éticas. En primer lugar, la limitación de la competencia. La monopolización de los datos por parte de los fabricantes o proveedores se constituye como una barrera de entrada nuevos competidores, ya sea porque no pueden competir con los precios de adquirir los datos o porque son pequeñas empresas o *startups*. Según Diaz Vera se genera una cuestión que afianza las dinámicas "*winner-takes-all*", en donde las empresas dominantes alcanzan ventajas insuperables al acumular grandes volúmenes de datos, impidiendo que empresas más pequeñas compitan en igualdad de condiciones (2023), tales como los efectos que producen plataformas como Amazon, Google, etc.

A su vez, al mantener un contacto directo bajo control técnico de los datos, se podrían limitar o rechazar el acceso a otros competidores u otras empresas que deseen utilizar los datos para finalidades específicas. Esto claramente vulnera principios de equidad, derechos de libre empresa y generan un desequilibrio en el ecosistema digital. El Data Act de la UE, por ejemplo, permite a los usuarios finales acceder a los datos que generan sus dispositivos para fomentar la innovación y el desarrollo de nuevos servicios puesto que podrán disponer de estos conforme a sus intereses y finalidades.

La falta de transparencia en el uso de los datos constituye un factor crítico en este enfoque, ya que impide conocer cómo se toman decisiones relacionadas con el procesamiento de dichos datos. Si bien los datos personales representan un desafío significativo en términos de

transparencia, los datos no personales también deben estar sujetos a este principio. Esto es especialmente relevante en cuestiones éticas y de privacidad, dado que el riesgo de un uso indebido sigue siendo potencial. Por tanto, garantizar la transparencia en el manejo de los datos no personales resulta indispensable para mitigar estos riesgos y promover un entorno de confianza en su gestión.

En contextos mineros, el ejercicio del control técnico sobre los datos, el proveedor tecnológico impone condiciones de uso y licencias restrictivas a las empresas mineras y las colocan en una situación de dependencia tecnológica, obstaculizando portabilidad minera, dificultando el cambio de proveedor o limitando la interoperabilidad con otros sistemas. Esta situación produce una clara situación de desequilibrio contractual y de los servicios tecnológicos como tal, constituyendo prácticas anticompetitivas.

Este control exclusivo desincentiva la creación de espacios colaborativos en el proceso de transformación digital, contradiciendo los modelos del "*Data Trust*" que promueven el acceso compartido y gestionado por múltiples partes interesadas para maximizar el valor de los datos. Esto restringe las posibilidades de reutilización de los datos en otros sectores, limitando el potencial valor y el impacto positivo reflejado en bienestar social.

En consecuencia, a pesar de que los datos no personales a la fecha han sido "por defecto" atribuidos a los fabricantes de AIoT, aún supone un problema latente en relación al impacto en la competencia de los mercados, la economía y, sobre todo, los efectos en la innovación a partir de la disponibilidad de los datos y la facilidad de acceso a los mismos. Un enfoque equilibrado sería aquel que garantice un acceso equitativo, que fomente la competencia y promueva un uso responsable, transparente y colaborativo para obtener beneficios comunes.

4.3. Autorregulación del mercado

En la actualidad, aunque los sistemas de inteligencia artificial utilizan datos no personales para su entrenamiento o la innovación, no se reconocen derechos de propiedad exclusivos o de otro tipo. Algunos autores defienden la postura de dejar a los mercados el establecimiento de las condiciones de acceso y otros, ante la falta de regulación, los agentes intervinientes vienen actualmente regulando la situación bajo la suscripción de contratos que establecen condiciones

en la prestación del servicio, con lo cual consideran que es suficiente para generar un ecosistema equilibrado.

Como sostiene Determann (2018), los marcos normativos actuales no reconocen una titularidad jurídica sobre los datos en tanto contenido informativo. Si bien existen ciertas protecciones sobre las manifestaciones físicas de la información (como bases de datos estructuradas) o sobre conjuntos que han requerido inversiones significativas, estas no alcanzan a los elementos individuales de datos. Así, la cuestión de quién es el propietario de los datos generados por dispositivos conectados o maquinaria inteligente, como los sistemas utilizados en el sector minero, suele responderse con un “nadie lo es realmente” (p. 26).

Desde esta perspectiva, la implementación de derechos adicionales sobre los datos podría generar efectos adversos al reprimir la innovación y restringir la libertad de información. El autor destaca que en la práctica, la regulación de los agentes se realiza mediante acuerdos contractuales. Esto les permite negociar y adaptar soluciones específicas a sus intereses y necesidades, evitando la rigidez y posibles externalidades de una regulación excesiva. Este enfoque fomenta flexibilidad y adaptabilidad en un entorno donde los datos son fundamentales para la innovación y el crecimiento. Sin embargo, implica que quien está en condiciones para pactar se debe a que ostenta una capacidad técnica o contractual en el mercado.

Por su parte, Minero (2021) argumenta que los derechos existentes, como el derecho *sui generis* sobre las bases de datos ofrecen protección suficiente para las inversiones sobre los datos estructurados. Los derechos que se brindan equilibran la protección de los intereses de los creadores o quienes desarrollan las bases de datos con la posibilidad de permitir el acceso a terceros dentro de esta cadena de valor, pero ejerciendo derechos de propiedad intelectual. En consecuencia, para este autor, crear otros derechos podría limitar las capacidades de innovación.

Asimismo, Kerber (2016) se cuestiona si es necesaria un nuevo derecho de propiedad intelectual para estimular la producción de datos, a lo cual concluye que, si bien se evidencia que los datos ya se generan masivamente sin incentivos adicionales, un derecho exclusivo podría reducir costos de transacción en mercados de datos. En contraposición, propone soluciones alternativas como restricciones contractuales o técnicas que considera han funcionado hasta la fecha.
Por ejemplo, el derecho de acceso es una categoría importante sobre los datos industriales, porque prevé un intercambio de los datos y el compartir libremente, sin injerencias entre

diferentes actores aún con intervención del sector público. Tal como señala Tarkowski & Vogelezang, esto debería darse inicialmente a través de “disposiciones tanto voluntarias como obligatorias para compartir datos” (2021).

Estos autores señalan que, respecto el derecho de acceso permite a las empresas y otras entidades gubernamentales adaptarse progresivamente a los diferentes requisitos del acceso en cuestiones técnicas, organizativas y legales. Este enfoque busca reducir tensiones entre los interesados y fomentar la colaboración entre las partes sin imponer requisitos regulatorios adicionales. Una implementación progresiva supone una aceptación gradual y cumplimiento asegurado.

Pero esta noción también tiene un componente social, porque podrían asegurar la capacidad de todos los miembros de la sociedad a beneficiarse de los datos fomentando la innovación en la mejora de los servicios públicos, optimizar procesos en el sector público o privado para que los datos sean percibidos como un recurso de interés público, y son más adecuados para desarrollar modelos de gobernanza que tengan en cuenta la naturaleza relacional e intereses colectivos de los datos. Por ende, no sería ideal que existen barreras sancionatorias si lo que se busca es fomentar que más actores compartan o hagan accesibles sus datos no personales o que esto implique un sobrecosto que no todas las empresas puedan asumir.

Aunque dejar que los agentes del mercado regulen el acceso a los datos basados en sus propios intereses podría parecer una solución sencilla, este enfoque puede generar desigualdades de poder en las negociaciones, especialmente por los efectos de redes que posicionan ventajosamente a ciertas empresas o establecen ventajas por el tamaño y poder adquisitivo que poseen. En consecuencia, las condiciones de acceso podrían volverse innegociables, representando barreras de entrada para nuevos competidores.

A su vez, esta autorregulación presenta serios desafíos: favorece la concentración de datos en pocos actores, dificulta el acceso equitativo a información estratégica y genera incertidumbre jurídica sobre los límites del uso legítimo. En respuesta, propuestas como el Data Act de la Unión Europea buscan transitar desde una lógica de exclusividad basada en el control tecnológico hacia un modelo de gobernanza que priorice el acceso justo, la interoperabilidad y la compartición equitativa**,** especialmente en entornos B2B como el industrial minero.

La autorregulación puede conducir a una fragmentación del mercado, ya que cada actor define sus propias reglas y condiciones de acceso, priorizando intereses individuales en lugar de un equilibrio colectivo. Esto no solo dificulta el acceso a los datos para fines como pruebas, entrenamiento, desarrollo o mejora de productos, sino que también frena la innovación de nuevas tecnologías y se retrase uno de los objetivos claves que es la interoperabilidad, viéndose afectada por la segmentación de decisiones en el mercado y limitando la creación de ecosistemas inclusivos y dinámicos.

En relación a lo señalado por Díaz Vera (2023), si los datos no son rivales pero excluibles, la mera asignación de derechos de propiedad no es del todo útil para que el mercado distribuya eficientemente dichos bienes y que los estudios económicos muestran las ineficiencias y pérdidas de bienestar de la asignación de derechos de propiedad sobre datos a empresas o consumidores, pues es evidente que la generación de un derecho de propiedad sobre los mismo generaría de por si la sola exclusión a terceros bajo condiciones del titular.

En efecto, la ausencia de regulaciones que orienten las relaciones y establezcan principios basados en *data trust* y *open data* para promover la innovación y la competencia podría derivar en que los actores del mercado adopten estándares técnicos cerrados para restringir el acceso a sus sistemas. Esto no solo aumentaría significativamente los costos, sino que también establece barreras para la innovación. Si las relaciones contractuales sobre el uso de los datos se limitan a acuerdos entre competidores o posibles colaboradores, se deja de lado la posición de los usuarios, ignorando aspectos fundamentales como su privacidad, la transparencia en el manejo de los datos y su acceso a estos, a pesar de que son también parte clave en el ecosistema de datos.

Son un número reducido de compañías que acumulan grandes cantidades de datos, sea por el tiempo que desempeñan en el mercado o por los *network effects* (mayores usuarios de la plataforma, mayor el beneficio), sin embargo, a la fecha no existe exigencia alguna u obligación de compartir los datos con terceros. Por ello, es evidente que existen problemas de igualdad de condiciones de acceso a los datos entre empresas y en casos de monopolización y/o prácticas desleales, el derecho de la competencia no es suficiente para abordar tal situación, debido a la acción *a posteriori* de su intervención y por consiguiente, ineficiente.

4.4. Cotitularidad de los datos no personales

El mayor valor de los datos en el mercado radica en su estado colectivo y en grandes volúmenes que sustenta la mayoría de los análisis de datos y la IA. La principal solución para romper los monopolios mundiales de datos se ha identificado como el intercambio de datos a diversos sectores de la sociedad (Singh & Gurumurthy, 2021). Otorgar derechos que protejan los conjuntos de datos, ya sea con el control absoluto por parte de los usuarios o consignar propietarios exclusivos a los productores o fabricantes de los dispositivos de AIoT, constituye una limitación de por sí al acceso a los datos.

La titularidad compartida o cotitularidad emerge como una alternativa eficiente para equilibrar derechos y también responsabilidad entre los actores que se involucran en la producción y procesamiento de los datos. Reconocer el ámbito colaborativo en la producción de los datos es importante en tanto fabricantes, operadores y/o usuarios finales portan consigo intereses legítimos respecto al uso de los datos y la generación surge a partir de ellos en conjunto.

En esa línea, Eckardt & Kerber (2024) introducen un concepto que subyace a la discusión fomentada por Metzger and Schweitzer, la cual se centra en que "*los titulares de datos (fabricantes del AIoT) y los usuarios deberían tener los mismos derechos para usar, compartir y divulgar los datos no personales que han sido co-generados de manera independiente y paralela entre sí*" (2023). En consecuencia, evita la monopolización de los datos y se estimula la competencia mediante el suministro en los mercados secundarios.

Asimismo, estos autores enfatizan en que los proveedores tecnológicos (llamados "*data holders*" o también "titulares de datos" en el *Data Act* de la UE) y los usuarios, en principio, deberían tomar en consideración los "intereses legítimos" de los co-generadores de los datos no personales al momento de ejercer el conjunto de derechos (acceso, uso y compartición), como la protección de la información confidencial, los secretos industriales, entre otros. No obstante, al prever una situación como tal, es posible que sea necesario recurrir a solicitudes previas u obtener autorización para ejercer tales derechos, lo que significa que el derecho no puede ser ejercido de manera libre y por la mera atribución de este.

En suma, este enfoque pretende reconocer que los datos del AIoT se generan a partir de la contribución de diferentes usuarios o actores, y por este motivo, los actores que intervienen en

estos procesos deberían poseer derechos de uso, acceso y compartición de manera independiente, pero bajo ciertas limitaciones.

Ahora bien, la designación de qué actores están involucrados en la “co-generación” de los datos aún sigue siendo un reto, pero este sistema de cotitularidad podría ofrecer criterios para identificar a generadores de los datos y en consecuencia, asignarles derechos. En el caso de los datos del AIoT, el Data Act dispone que la intervención económica y esfuerzo en la producción de los datos se realiza entre los usuarios y fabricantes y su inversión es suficiente para identificar que forma parte de la producción de los mismos.

Como señala además, Tarkowski & Vogelezang, este concepto reconoce el valor que cada uno de los actores intervinientes aporta en el ciclo de vida del dato. En ese sentido, es una solución asignar derechos compartidos proporcionales a la inversión, ya sea económicos, técnicos o intelectuales (2021). Esto permite distribuir el control de los datos, reduciendo el riesgo *lock-in* o monopolización de los datos y favorece la colaboración entre empresas, evitando infracciones, barreras entre sí y haciendo más competitivo el sector.

Asimismo, este panorama es conveniente de manera tal que al distribuir los derechos, existe la posibilidad que los datos no personales puedan ser compartidos en la búsqueda de satisfacer intereses diversos, no siempre contrapuestos. El proveedor de tecnología incentiva compartir datos con servicios complementarios y, por el lado de los usuarios, fomenta la innovación y competencia en los mercados.

En ambas partes, la competencia y la inversión en innovación son factores requisito que restablecen el equilibrio con el que se usan los datos, aún si el proveedor de tecnología tiene mayores facilidades para disponer datos en bruto y procesados, el usuario tiene la plena capacidad y posibilidad de utilizar, compartir y explotar igualmente tales datos no personales.

No obstante lo anterior, Eckardt & Kerber han previsto consecuencias tanto positivas como negativas en el establecimiento de derechos compartidos sobre los datos. El impacto positivo se centra en eliminar la exigencia de establecer acuerdos contractuales previos con los usuarios para el uso de los datos no personales, que se dispone en el artículo 4.13 y 4.14 del Data Act de la UE (2024). Esto se debe a que repercute significativamente en los costes asociados por la disposición de estos, lo que podría generar una disminución considerable en las transacciones e

incluso, eliminarlos. Esto permite también a las *startups*, pequeñas y medianas empresas acceder sin barreras de entrada a los mercados, creando espacios con conceptos de gestión de datos "*open Data"* o *"data as a common",* como bienes compartidos.

Por otro lado, los autores señalan que la creación de mercados de datos en la actualidad se sustenta en relaciones de compra y venta. En este contexto, el valor reside en la posibilidad de combinarlos con otras fuentes, lo que permite generar correlaciones, identificar nuevas variables y obtener hallazgos más relevantes que pueden dar lugar a modelos de negocio específicos para distintas industrias. Esta situación impulsa la innovación porque permite desarrollar nuevas tecnologías, ampliar los sectores de uso, mejorar las innovaciones ya existentes y fomentar la creación de nuevas aplicaciones. Con un sistema de distribución de la titularidad se invierte en estrategias para prevenir prácticas anticompetitivas y proteger la competencia en los mercados secundarios (2024).

Por el contrario, esta concepción implica el riesgo de que las empresas justifiquen su negativa a compartir datos, argumentando que los mismos se encuentran comprendidos dentro de los límites de la información confidencial o que revisten la naturaleza de secretos industriales. Tal enfoque podría ser utilizado estratégicamente para restringir el acceso a los datos por parte de terceros, consolidando posiciones de control exclusivo bajo el amparo de figuras jurídicas diseñadas para tutelar intereses legítimos en contextos distintos al de la circulación de datos no personales. De igual modo, existe el riesgo latente de que se generen barreras técnicas (o tecnológicas) que dificulten la legibilidad total de los datos. Y, como se ha mencionado anteriormente, resulta fundamental delimitar la atribución de titularidad de acuerdo con la categoría del dato y el valor que este adquiere a partir de la aplicación de diversas tecnologías.

Estas amenazas podrían manifestarse como comportamientos recurrentes entre los fabricantes o, ciertamente, entre los OEM, ya que resulta menos gravoso para un fabricante tecnológico otorgar acceso a datos en bruto que a datos derivados o procesados. Esto se debe a que los datos derivados implican una actividad que requiere mayores esfuerzos, debido a la intervención de múltiples actores, inversiones en tecnología, y la aplicación de capital, tiempo e intelecto. Por ende, ante una eventual exigencia u obligación de dar acceso a este tipo de datos derivados, se plantea una amenaza al valor sustancial, así como al potencial económico e intelectual, que podría afectar de manera significativa el modelo de negocio de las compañías.

Es posible considerar la posibilidad de otorgar derechos de acceso, uso y compartición de datos personales entre fabricantes y usuarios dentro de una relación B2B de forma equilibrada y razonable. Esto representa una ventaja significativa en el mercado de datos industriales, ya que permite generar y recopilar datos de manera conjunta, maximizando las oportunidades de identificar diferentes motivos para fomentar el flujo de datos y habilitando fuentes diversas. Estos derechos deben percibirse como un canal para facilitar la entrada a este mercado, eliminando barreras de acceso.

A su vez, es pertinente considerar que las condiciones para los derechos de acceso y compartición deben responder a la naturaleza no rival de los datos. Un derecho que implique un costo social elevado no debería afectar gravemente la forma en que se realizan los negocios con estos datos. Es decir, es posible habilitar un derecho sobre los datos no personales para garantizar su accesibilidad, pero este no debería representar un costo adicional o irracional que deban asumir los proveedores o fabricantes tecnológicos, ni mucho menos si no existen límites o parámetros que establezcan mínimos.

A modo de ejemplo, Atik (2022) critica la idea de la propiedad exclusiva de los datos, particularmente en el sector agrícola, sobre todo por la concentración de poder. En su lugar, sugiere que haya un enfoque de derechos de acceso inalienables para poder desbloquear el potencial de los datos no personales, fomentar la interoperabilidad técnica y la gobernanza específica garantizando la innovación y la distribución justa de los beneficios, junto con el crecimiento del sector que genera un beneficio común.

Existen muchas críticas sobre la concepción de accesibilidad que se ha percibido del Data Act de la UE, y es que para hablar de “acceso libre” a los datos, estos puedan ser accesibles en términos de la facultad de solicitarlo y que al momento de la entrega de estos puedan ser técnicamente accesibles y legibles para cumplir con una función en concreto, ya sea que represente información relevante o que busque la interoperabilidad.

En este sentido, es necesario aclarar algunos aspectos relacionados a la co-generación de datos no personales y, por ende, prever la asignación de titularidad para los derechos de uso, compartición y explotación de los datos bajo un esquema de “cotitularidad”. En primer lugar, el acceso debe garantizarse sobre los datos en bruto. En segundo lugar, no deben existir intereses que perjudiquen gravemente a la contraparte (como exponer información sensible o secretos

industriales), ni se deben realizar acuerdos que busquen monopolizar o restringir el acceso a terceros.

Por último, el mercado debería autorregular el monto correspondiente a la transmisión de datos – en la medida que generen costos relevantes adicionales o no previstos – de acuerdo con el nivel de procesamiento de estos, el tiempo invertido por las partes y las características del sector específico. Estos aspectos son cruciales para la elaboración de una normativa que permita regular la atribución de derechos y el acceso y gestión de los datos no personales en el sector industrial, todo ello acompañado de una estrategia de *enforcement* o refuerzo que permita supervisar las consecuencias de su implementación.

Finalmente, la accesibilidad como derecho no aborda de manera completa el aspecto de la interoperabilidad. Si bien esta es un ideal, todavía no se han establecido condiciones de obligatoriedad sobre este punto. Aunque la Unión Europea, a través de su *Data Act*, introduce el concepto, aún no se define claramente si la interoperabilidad es una obligación para quien ejerce el derecho de acceso o para quien lo concede. El reto radica en definir la interoperabilidad como un requisito esencial que complementa el derecho de acceso, asegurando así un ecosistema más cohesivo y eficiente y evitando costos adicionales para hacer posible el acceso.

5. Alcance de protección de los datos no personales generados a partir del AIoT en el sector minero

Una vez analizadas las diferentes posiciones respecto de la titularidad o supuesta atribución de derechos sobre los datos no personales podemos inferir que estos no se ajustan a las concepciones tradicionales de derechos de propiedad y que, por ello, es necesario que su regulación los conceptualice como bienes intangibles pasibles de tutela especial. Esta protección no debería depender de una asignación exclusiva de derechos, sino construir un marco que garantice la disponibilidad, uso eficiente y limitaciones de prácticas anticompetitivas.

De hecho, a pesar de que las leyes de protección de datos personales confieren a los titulares un poder claramente establecido a través de reglas definidas, estos derechos están basados en la protección del derecho a la privacidad, fundamentado en muchos países como un derecho constitucional, y no necesariamente en el derecho de propiedad. Estas garantías suelen entrar en colisión con otros derechos, como el de la libre expresión, lo cual ha generado que se generen equilibrios cuando más de un derecho colisiona.

Como ha señalado Drexl (2018), el derecho de protección de datos, considerado un derecho fundamental, protege principalmente contra usos que puedan generar un daño potencial a la persona natural, más que el uso en sí por parte de terceros. Esto demuestra que dicho derecho podría incluso prevalecer frente a otros, como los de propiedad intelectual. Asimismo, dado que los datos personales no han requerido la creación de derechos de propiedad específicos para su protección, se argumenta que una regulación de los datos no personales también debería mantenerse al margen de esta perspectiva.

En la medida en que existe un objetivo común que trasciende el control exclusivo de quien recopila o genera los datos, dicho objetivo debe centrarse en garantizar el libre flujo de los datos mediante el acceso de múltiples actores, promoviendo la interoperabilidad y fomentando la innovación tecnológica.

Considerando que no existe una legislación que proteja los datos no personales de manera efectiva, los derechos de propiedad intelectual, como los derechos *sui generis*, son descartados como mecanismos adecuados de protección para esta tarea. Aunque ofrecen protección a estructuras de datos, su aplicación puede no ser adecuada en casos de uso de *big data*, donde se procesan volúmenes masivos de datos. Al respecto, la Corte de Justicia de la Unión Europea, en los casos *Fixture Marketing* y *British Horseracing*, determinó que los derechos *sui generis* solo aplican a la "creación" de bases de datos, pero no a la "obtención" de los datos. Sin embargo, este tema sigue siendo objeto de debate.

En el caso de productos conectados que buscan generar beneficios a partir de su uso prolongado, como sucede en la minería o en otras industrias, donde el valor del dato se maximiza cuando es compartido, un derecho *sui generis* sobre los datos representaría un problema de acceso. Esto afectaría no solo a los usuarios, sino también a terceros actores como competidores, otros proveedores o innovadores de diferentes sectores, quienes podrían enfrentarse a un "bloqueo" o efecto *lock-in* de los datos, puesto que la estructura de datos protegida responde a una configuración particular a un objetivo y que no es estandarizada a todo tipo de aplicación.

Las APIs, que son las interfaces de programación de aplicaciones, son el recurso técnicamente idóneo para garantizar la disponibilidad y legibilidad de los datos, fomentando la interoperabilidad entre sistemas (Drexl, 2018). Los derechos de autor o incluso las patentes sobre estas pueden

convertirse en una amenaza para el flujo adecuado de los datos en entornos de productos conectados en relaciones B2B. Esto ocurre especialmente si no se conceden derechos que limiten el ejercicio de otros derechos que obstaculicen el aprovechamiento de los beneficios de los datos.

Sin dejar atrás que el sector minero enfrenta desafíos únicos relacionados al manejo de los datos no personales en su transformación digital que usa tecnologías como la IA y IoT, es necesario prever formas de maximización de beneficios que contribuyan con el desarrollo no solo del sector minero, sino que impulse además la innovación tecnológica y que esta permita beneficiar otros sectores dentro de la cadena de valor minera.

Asimismo, el sector minero busca implementar cada vez más flotas modernas, compuestas en gran parte por dispositivos conectados a internet que proporcionan información detallada tanto del equipo como del entorno que los rodea. No obstante, las restricciones al acceso a estos datos podrían justificarse por los costos asociados a su recopilación y procesamiento, lo que abre la posibilidad de establecer mecanismos de compensación, como licencias de uso (Eger & Scheufen, 2024). Estas restricciones resultan económicamente injustificadas, ya que limitan el uso de otros dispositivos que podrían ofrecer servicios complementarios, como el mantenimiento de equipos de la flota minera o la adaptación de ciertos datos operativos de la maquinaria para analizar otros factores relacionados como medio ambiente, cuestiones laborales, etc.

En el caso de la maquinaria utilizada en minas, que incluye principalmente sensores y cámaras, los fabricantes de los vehículos son quienes controlan el acceso a los datos generados por estos dispositivos. Generalmente, estos datos se almacenan en servidores propios de los fabricantes y no están disponibles de forma abierta. Solo los usuarios, es decir las minas, pueden acceder a ellos en condiciones limitadas, en ocasiones de manera gratuita y, en otras, bajo un costo adicional. Aun así, terceros pueden acceder a esta información con condiciones de limitaciones operativas o a cambio de altos costos.

En este contexto, es evidente que, ante una posible negociación sobre el acceso a los datos de estos equipos, tanto los usuarios como los terceros no estarían en igualdad de condiciones para negociar el acceso a estos. Esto se debe a que consideran las condiciones de acceso como amenaza a los derechos de propiedad intelectual o, incluso, su posición en el mercado. Por ejemplo, si un tercero solicita acceso a los datos, podría utilizar esa información para ofrecer productos o servicios que compitan directamente con quienes ejercen el control de facto de los

datos, como servicios de mantenimiento, monitoreo de equipos, análisis de su estado, entre otros.

Como se ha señalado, la creciente generación de datos no personales en entornos complejos y dinámicos como los sistemas AIoT implementados en la industria minera exige una revisión crítica sobre el tipo de derechos que podrían atribuirse a los distintos actores involucrados. Esta atribución no puede asumirse de forma automática ni absoluta: resulta necesario delimitar con claridad el contenido, el alcance y las restricciones de tales derechos, considerando que toda prerrogativa jurídica opera dentro de un marco de intereses concurrentes.

En efecto, reconocer derechos sobre los datos no personales debe ir acompañado de una crítica y reflexión sobre sus eventuales riesgos con otros objetivos de interés público, como la promoción de la innovación tecnológica, la interoperabilidad y la equidad en el acceso al conocimiento. A continuación, se analizarán los posibles derechos que podrían ser reconocidos (como el acceso, el uso y la compartición de datos) enfatizando en que la formulación debe ser objeto de debate crítico y susceptible de ajustes que garanticen una regulación equilibrada y orientada al desarrollo sostenible de la economía digital.

5.1. Derecho de Acceso

En el marco del uso cada vez más recurrente de tecnologías como el AIoT en entornos industriales, el derecho de acceso a los datos no personales se constituye como una herramienta jurídica fundamental para encontrar el equilibrio relacional entre los actores que lo generan, capturan o procesan. A diferencia de los modelos de atribución exclusiva de derechos que predomina la exclusión de quien posee la cosa respecto de otros, el derecho de acceso no concibe la facultad de exclusión, sino se orienta a habilitar el uso legítimo, compartido pero controlado de los datos generados por dispositivos conectados a internet.

Este derecho podría definirse como una facultad que posee un sujeto legitimado para acceder técnica y legalmente a estos, siendo una garantía para ellos sin necesidad de poseer título de propietario de los datos. Así, trascienda la lógica posesoria que predomina en los activos tradicionales, a fin de lograr un régimen más justo y sobre todo, más adecuado a la eficiencia operativa de los datos no personales, a su interoperabilidad, transparencia y a la promoción de la innovación tecnológica.

En ese sentido, desde una perspectiva legal, el derecho de acceso posee algunas diferencias de las licencias de uso o contratos de cesión de datos porque no depende de la voluntad exclusiva de un titular previamente reconocido, sino que emerge como un derecho previsto por disposiciones normativas que buscan que el acceso sea a solicitud simple, que se prohíba la negativa al acceso salvo por razones legítimamente sustentadas y evitar el abuso de posiciones dominantes u otras prácticas anticompetitivas en la cadena de valor digital.

Asimismo, bajo la perspectiva del acceso, es necesario considerar que actualmente las industrias presentan algunas limitaciones sobre el acceso a los datos no personales por parte de algunos agentes intervinientes, sean en calidad de fabricantes o de procesadores. Los fabricantes suelen usar medidas técnicas que restrinjan el acceso directo a los datos en las industrias, y solo es posible acceder a estos mediante plataformas como parte de un servicio adicional o a través de una solicitud formal de acceso que pasa por una evaluación previa. En general, muchas veces responde a intereses económicos para poner a disposición los datos.

Para ejercer este derecho, en el marco de una gobernanza sobre los datos de manera justa y equitativa, Tarkowski & Vogelezang (2021) propone la adopción de principios que hagan de los datos: Localizables, Accesibles, Interoperables y Reutilizables (Principios FAIR*, Findable, Accessible, Interoperable, Reusable* por sus siglas en inglés) (Wilkinson, M, et al, 2016), con el objetivo de maximizar su valor social y económico, se abordan desde una perspectiva útil de la gobernanza de los datos.

Wilkinson desarrolla cada uno de estos principios indicando que, los datos deben ser localizables de manera que permitan ser ubicados o localizados fácilmente, ya sea a partir de la estandarización de metadatos que brinda información o descripción clara adicional para identificar correctamente los datos o con sistemas abiertos de datos en donde su registro involucre interoperabilidad inherente.

La accesibilidad debe garantizarse de forma controlada bajo condiciones de acceso claras. Es decir, que se establezcan los acuerdos mínimos para el uso posterior de los datos en donde las condiciones deben ser explícitas, desde el intercambio, las medidas de seguridad, los usos previstos, la contraprestación por el paquete de los datos, el tipo de datos a compartir, etc.

Deberá exigirse el almacenamiento seguro para garantizar que la privacidad, integridad y confidencialidad de la información no se ponga en riesgo, pero se debe tomar en consideración

que la regulación no debe poner responsabilidades sobre quienes comparten los datos pero sí un deber de diligencia que debe ser asumido por alguna de las partes en la medida que supone un riesgo latente.

Asimismo, la interoperabilidad es clave para promover la colaboración y reutilización de los datos entre los diferentes actores, por ello es necesario utilizar protocolos compatibles entre sistemas y que sea transversal a los sectores. De lo contrario, es necesario que puedan estandarizarlos para hacer del flujo de los datos mucho más rápido, legible, eficiente, que permita la comunicación entre sistemas y también independientemente de la operación y la plataforma de procesamiento.

La reutilización de los datos es clave para generar valor agregado en diferentes industrias, el cual da origen al enfoque *data driven* de las economías, es decir, que la toma de decisiones en un negocio se basa en datos y para ellos es necesario la disponibilidad de estos. Los derechos de uso y restricciones deben estar delimitadas con el objetivo de promover confianza en las transacciones de datos y deben mantenerse bajo formatos que aseguren su integridad y sean legibles a fin de que permanezcan útiles para ser reutilizados en otros sectores y destinarlos a múltiples propósitos.

Además, este derecho de acceso se diferencia de las licencias de uso o contratos de cesión en tanto no depende de la voluntad exclusiva del titular del dispositivo o proveedor de la tecnología, sino que emerge como un derecho garantizado por disposiciones normativas que buscan evitar el abuso de posiciones dominantes en la cadena de valor digital.

En este sentido, el reconocimiento de este derecho adquiere especial relevancia cuando la información es obtenida en entornos de producción industrial mediante sensores, cámaras u otros mecanismos automáticos de recolección, y cuya disponibilidad resulta esencial para el funcionamiento de servicios asociados, la toma de decisiones operativas o la generación de soluciones complementarias.

El derecho de acceso, por tanto, no pretende instaurar un régimen de titularidad absoluta ni generar nuevas formas de propiedad sobre los datos no personales, sino permitir su circulación controlada bajo criterios de transparencia, interoperabilidad y no discriminación, contribuyendo con ello a la configuración de un marco normativo más equitativo y tecnológicamente inclusivo.

La configuración del derecho de acceso como un instrumento funcional para el tratamiento de los datos no personales en entornos industriales responde a la necesidad de corregir desequilibrios estructurales en la economía de los datos, especialmente en contextos B2B donde se observa una fuerte asimetría en el control y disponibilidad de la información. En el caso del sector minero, los dispositivos AIoT implementados por proveedores tecnológicos tienden a operar bajo arquitecturas cerradas que consolidan un control exclusivo de facto sobre los datos generados, restringiendo el acceso tanto de los usuarios finales como de terceros que podrían ofrecer servicios complementarios. Esta práctica configura lo que Eckardt y Kerber denominan una “captura tecnológica de los datos”, mediante la cual el diseño técnico del dispositivo se convierte en un mecanismo de exclusión económica (Eckardt & Kerber, 2024).

Desde una perspectiva económica, el derecho de acceso se justifica por la naturaleza no rival y fácilmente reproducible de los datos. A diferencia de los bienes materiales, el uso de un conjunto de datos por parte de un actor no impide su utilización simultánea por otros, lo que permite que múltiples agentes extraigan valor a partir del mismo insumo informacional sin agotarlo. Este rasgo económico ha sido ampliamente reconocido en la literatura, que destaca que el otorgamiento de derechos exclusivos sobre datos no personales puede generar efectos de acaparamiento o fragmentación del valor, afectando negativamente la innovación y la eficiencia de los mercados digitales (Duch-Brown, Martens & Mueller-Langer, 2017).

Asimismo, el derecho de acceso encuentra sustento normativo en iniciativas regulatorias como el Data Act, que dispone en su artículo 4, el derecho del usuario de un producto conectado a acceder a los datos generados por su uso, así como la facultad de compartirlos con terceros autorizados, en condiciones “justas, razonables y no discriminatorias”. Esta disposición se fundamenta en el reconocimiento de que, en la mayoría de los casos, los fabricantes de dispositivos ostentan una posición privilegiada para restringir el acceso a la información, lo que puede obstaculizar el surgimiento de nuevos modelos de negocio, la interoperabilidad y la prestación de servicios posventa o de mantenimiento.

En términos prácticos, el derecho de acceso contribuye a la apertura de los ecosistemas digitales, permitiendo que los actores que no participan directamente en la fabricación o configuración del *hardware* puedan integrarse en la cadena de valor de los datos mediante servicios de análisis, diagnóstico, mantenimiento predictivo o retroalimentación algorítmica. Esto no solo amplía las posibilidades de innovación en el sector, sino que también mitiga los riesgos asociados a

prácticas anticompetitivas, como el cierre de mercado mediante cláusulas técnicas (*technical lock-in*) o el establecimiento de barreras artificiales a la portabilidad y reutilización de datos.

En suma, la consolidación del derecho de acceso no solo atiende a una función correctiva frente a las asimetrías en el mercado, sino que responde a una necesidad de establecer una gobernanza de los datos orientada al interés general, la eficiencia sistémica y el aprovechamiento colectivo del valor generado por tecnologías emergentes como el AIoT. Lejos de obstaculizar la inversión o la protección de los legítimos intereses del proveedor, este derecho consolida las bases para un marco equitativo que fomenta una competencia leal, habilita servicios derivados y promueve un entorno de innovación abierta.

Ahora bien, el diseño normativo de este derecho ha sido abordado por el Data Act como pioneros de esta regulación, la cual ha establecido una clara delimitación de los sujetos legitimados para ejercerlo, así como de las condiciones bajo las cuales dicho ejercicio puede tener lugar. En este, el sujeto principal del derecho de acceso es el usuario del producto conectado o del servicio relacionado, definido como la persona física o jurídica que posee, alquila o explota legítimamente el producto o servicio en cuestión (art. 2, inc. 7).

En el caso de la industria minera, este sujeto corresponde típicamente a la empresa minera que integra en sus procesos maquinaria integrada con sensores, sistemas de visión, monitoreo de estado, o análisis predictivo, desarrollados por un proveedor tecnológico. Sin embargo, el ejercicio del derecho de acceso no se agota en la relación bilateral entre usuario y fabricante.

La normativa europea permite que el usuario autorice a un tercero para que acceda directamente a los datos generados, lo cual habilita modelos de negocios (por ejemplo, empresas de mantenimiento predictivo, aseguradoras, o desarrolladores de software de optimización) puedan utilizar los datos como insumo para ofrecer soluciones complementarias. Este acceso por terceros se supedita al cumplimiento de principios de equidad, transparencia, confidencialidad y ciberseguridad, garantizando la compatibilidad con otras normativas, como la protección de secretos empresariales y la propiedad intelectual.

En el caso particular del ecosistema AIoT minero, la identificación de los sujetos legitimados debe considerar al menos tres niveles: i) el usuario operativo (las minas): que emplea la tecnología en campo y genera los datos durante el uso del dispositivo, ii) la el proveedor tecnológico, que actúa como responsable estratégico del sistema productivo y que concentra los derechos contractuales

sobre los activos que recopilan y procesan los datos y iii) los terceros, que pueden incluir empresas de análisis, investigadores, organismos reguladores o auditores, que acceden a los datos con fines específicos autorizados por el usuario.

Si bien el fabricante o proveedor tecnológico ostenta el control técnico de los datos mediante el diseño del dispositivo y la arquitectura del sistema, el reconocimiento de su rol como "*data holder*" bajo el Data Act no implica que se le atribuya como tal un derecho de propiedad sobre los datos en sí, sino se le atribuye la obligación de permitir el acceso bajo ciertas condiciones. De hecho, el artículo 4.13 del Data Act dispone que “el proveedor solo podrá utilizar los datos previa celebración de un acuerdo con el usuario”, lo que revierte el supuesto general de control unilateral sobre la información.

Esta redistribución de facultades entre los distintos actores responde al propósito de democratizar el ecosistema de datos industriales, garantizando que los datos generados no permanezcan capturados en un modelo vertical de exclusión, sino que puedan ser reutilizados para fines legítimos y competitivos. Al mismo tiempo, esta estructura favorece la trazabilidad del acceso, el establecimiento de condiciones contractuales claras, y el respeto a principios de proporcionalidad y finalidad.

A fin de cuentas, la definición de los sujetos legitimados para ejercer el derecho de acceso requiere una lectura amplia, contextualizada y operativa, que permita atender a la complejidad del entorno AIoT, donde los flujos de datos involucran múltiples actores interdependientes, y donde la apertura controlada de información puede traducirse en una mayor eficiencia, innovación y competitividad.

Por su parte, el alcance de este derecho, a partir del análisis del Data Act, se centra en 3 grandes cuestiones: los tipos de datos que comprende, las condiciones técnicas de interoperabilidad y las finalidades de su ejercicio, lo cual representa tanto las fortalezas como oportunidades de mejora en su aplicación.

El Data Act limita el derecho de acceso a los *datos generados por el uso* de productos conectados o servicios relacionados, precisando que deben tratarse de datos *observados* o *preprocesados* por el dispositivo durante su operación (artículo 2.1 y Recital 15). Esta definición excluye de forma expresa los datos *inferidos* o *derivados*, es decir, aquellos

que resultan del tratamiento, estructuración o análisis avanzado aplicado sobre los datos primarios.

El derecho de acceso no solo supone la habilitación jurídica para solicitar los datos, sino que conlleva también la obligación del proveedor (*data holder*) de facilitar el acceso de forma que sea técnicamente viable y funcional. Conforme al artículo 4.2 del Data Act, los datos deben entregarse en un formato estructurado, comúnmente utilizado, legible por máquina y, en la medida de lo posible, accesible en tiempo real.

Esto implica que el acceso debe ser facilitado mediante medios interoperables (por ejemplo, APIs abiertas o interfaces estandarizadas) y sin introducir obstáculos artificiales que dificulten el uso eficaz de los datos. No obstante, como destacan Graef y Husovec (2022), en la práctica muchos dispositivos AIoT en el mercado industrial actual funcionan con arquitecturas cerradas o formatos propietarios que obstaculizan la interoperabilidad, lo que puede desnaturalizar el ejercicio del derecho.

Por ello, para garantizar un acceso significativo, resulta indispensable complementar el marco normativo con estándares técnicos obligatorios o mecanismos de certificación de conformidad técnica, que eviten que los titulares de los dispositivos mantengan un control técnico indirecto aun cuando estén legalmente obligados a abrir el acceso.

Y por último, la finalidad de este derecho no solo contempla el uso directo por parte de los usuarios sino también su facultad para compartirlos con terceros (Art. 5 del Data Act), fundamental para establecer entornos colaborativos como el sector minero donde son más de un agente que intervienen en la dinámica de recolección y procesamiento de los datos no personales.

Sin embargo, esta capacidad se ve limitada el artículo 5.8, que establece que el uso de los datos por parte del tercero autorizado debe respetar la finalidad definida por el usuario y no excederla. Además, el acceso no debe violar la protección de datos personales ni los secretos comerciales del *data holder*, lo cual puede generar tensiones interpretativas respecto al alcance de los datos disponibles, como se ha analizado en el apartado anterior.

Sobre esta apertura “limitada” puede inhibir la creación y desarrollo de mercados complementarios o de servicios basados en datos, restringiendo el efecto dinámico que se esperaba al dejar intervenir a más de un actor interviniente. Así lo advierten Duch-Brown,

Martens y Mueller-Langer (2017), quienes destacan que un acceso condicionado a negociaciones bilaterales fragmentadas puede generar nuevas formas de concentración informacional y *lock-in* funcional.

Ahora bien, a pesar que las intenciones de la Unión Europea posicionan una enorme atención en la importancia de los datos no personales en el mundo de la innovación y mercados de datos, los esfuerzos aún tienen un camino muy largo para adoptar mejoras. Por un lado, uno de los principales límites radica en su decisión de restringir el derecho de acceso únicamente a los datos en bruto y preprocesados generados por el uso de productos conectados, excluyendo expresamente los datos derivados o procesados (Recital 15, art. 2.1 del Data Act).

Esta distinción, aunque técnicamente es razonable para proteger el valor agregado sobre los datos que se genera por la aplicación de algoritmos o modelos analíticos por parte del proveedor tecnológico, genera una brecha importante en sectores como el minero, donde el valor operativo real se encuentra muchas veces en el conocimiento que se deriva del análisis continuo de grandes volúmenes de datos brutos. Como observan Eckardt y Kerber (2024), esta exclusión puede limitar el impacto del acceso, especialmente cuando el usuario necesita comprender patrones o correlaciones operacionales que solo están disponibles en los datos derivados.

Asimismo, Can Atik (2022), al analizar la gobernanza de los datos en el sector agrícola en Europa, advierte que excluir los datos procesados impide abordar uno de los principales fallos de mercado: la dependencia estructural de los usuarios respecto de los proveedores que controlan el procesamiento avanzado de datos. Por tanto, permitir un acceso más amplio – al menos sujeto a condiciones específicas – podría fomentar mayor competencia y autonomía para los usuarios industriales.

El derecho de acceso se encuentra limitado por salvaguardas orientadas a proteger los secretos comerciales y la propiedad intelectual de los *data holders* (arts. 4.6, 4.9 y 8 del Data Act) que, si bien puede justificarse en el *"capital claim*" y los esfuerzos intelectuales en materia de propiedad intelectual, el valor se encuentra predominantemente en la disponibilidad de datos en una estructura específica y que sean reutilizables a nivel técnico. No obstante, el reglamento no establece criterios para delimitar cuándo un conjunto de datos constituye un secreto comercial, ni tampoco son abordados por la propiedad intelectual. Como advierten Duch-Brown, Martens y Mueller-Langer (2017), esta falta de delimitación conceptual permite que los proveedores

tecnológicos amplíen injustificadamente el ámbito de protección, utilizando cláusulas contractuales o estructuras técnicas para evitar la compartición.

En esa misma línea, Graef y Husovec (2022) destacan que, si bien el Data Act intenta equilibrar los intereses comerciales legítimos con la apertura de datos, su redacción ambigua abre la puerta a interpretaciones extensivas por parte de los *data holders*, generando bloqueos informativos en mercados que frenan críticamente la reutilización de datos, como el mantenimiento predictivo en maquinaria pesada. Para superar este reto, los autores proponen establecer guías técnicas o decisiones vinculantes por parte de autoridades competentes.

Sin embargo, desde la perspectiva del presente trabajo, el límite establecido por el Data Act, que restringe el derecho de acceso a los datos en bruto o preprocesados, excluyendo los derivados o procesados, constituye una delimitación justa y adecuada. Si bien la apertura de los datos busca fomentar la interoperabilidad y la competencia, no puede desconocer que los datos derivados son, en muchos casos, el resultado directo de inversiones significativas en investigación, desarrollo e innovación tecnológica. Estos datos son elaborados a partir de modelos analíticos, algoritmos y procesos de inteligencia artificial que se encuentran protegidos por derechos de propiedad intelectual y que forman parte de la ventaja competitiva legítima de quienes los desarrollan. Por tanto, permitir el acceso indiscriminado a estos resultados equivaldría a forzar la cesión de activos intangibles sin la debida compensación, lo cual podría desincentivar la innovación en lugar de promoverla.

Al reconocer los datos en estado bruto como el núcleo del derecho de acceso, se mantiene una base sólida y neutral que permite su aprovechamiento no solo por otros proveedores tecnológicos del sector minero, sino también por actores de sectores diversos, como el ambiental, el sanitario o el geográfico, que pueden aplicar sus propios modelos de análisis sobre una misma fuente primaria de datos. Esta apertura genera un escenario de pluralidad técnica e interdisciplinariedad sin comprometer los activos protegidos por la propiedad intelectual.

En consecuencia, sostengo que el límite fijado por el Data Act no solo respeta el equilibrio entre acceso e incentivo a la inversión, sino que también reafirma que el verdadero valor estructural de los datos radica en su forma original y no procesada, desde la cual puede construirse conocimiento adaptado a múltiples propósitos de interés público y privado.

Finalmente, si bien el Data Act reconoce el derecho de acceso como una obligación legal del *data holder,* no contempla mecanismos procesales que permitan a los usuarios hacer valer dicho derecho de manera eficaz cuando es denegado. Esto genera lo que Specht-Riemenschneider (2023) describe como una "asimetría institucional", en la que los usuarios carecen de herramientas efectivas y/o garantías para para hacer valer su posición frente a proveedores tecnológicamente dominantes. En entornos industriales complejos, como el minero, la situación se agrava por la existencia de acuerdos contractuales con cláusulas de confidencialidad, formatos cerrados o estándares que pueden retrasar o incluso neutralizar este derecho.

Desde una óptica funcional, Kerber (2023) argumenta que sin remedios procesales efectivos, como sistemas de mediación especializados, autoridades sectoriales de supervisión o sanciones por denegación injustificada, el derecho de acceso corre el riesgo de convertirse en una expectativa programática sin eficacia práctica. De allí que uno de los principales desafíos regulatorios del futuro será transformar este derecho en un instrumento operativo y verificable, especialmente en sectores donde el uso de datos constituye una ventaja competitiva clave.

La consolidación del derecho de acceso a los datos no personales generados por dispositivos AIoT y otros dispositivos inteligentes representaría un avance normativo significativo en la búsqueda de un marco jurídico más equitativo y funcional para la economía digital industrial. Este derecho, concebido no como una forma de apropiación exclusiva, sino como una herramienta habilitante de uso, reutilización y compartición de datos, permite equilibrar las relaciones entre los distintos actores del ecosistema AIoT, especialmente en contextos B2B como el sector minero, donde se evidencian asimetrías estructurales en el control de la información.

5.2. Derecho de Uso

El derecho de uso hace referencia a la facultad de procesar los datos no personales generados por productos o servicios conectados, con la finalidad de destinarlos a propósitos específicos como análisis, entrenamiento de algoritmos, optimización operativa, o desarrollo de nuevos productos. A diferencia del derecho de acceso, que hace posible la obtención técnica de los datos, el derecho de uso se orienta hacia su explotación funcional, siendo esta el motivo por el cual justifica el interés por acceder a los datos en primer lugar.

En el marco del Data Act (UE) 2023/2854, este derecho no se configura como una prerrogativa absoluta, sino que está supeditado a acuerdos contractuales entre las partes involucradas, especialmente entre el usuario del dispositivo y el proveedor tecnológico *(data holder*). En ese

sentido, el proveedor o fabricante del dispositivo solo puede hacer uso de los datos si existe una base contractual habilitante suscrita con el usuario (art. 4.13), quien se reconoce como actor central en la generación de valor a través del uso legítimo de la tecnología.

Jurídicamente el derecho de uso puede concebirse como una extensión del derecho de acceso habilitada mediante contrato entre las partes. Asimismo, se instaura como una respuesta normativa para corregir la situación de control exclusivo de facto que ostentan los fabricantes de dispositivos IoT sobre los datos no personales generados.

Como explica Specht-Riemenschneider (2022), este control no proviene de un derecho legal formal, sino de la arquitectura técnica del dispositivo, que permite a los fabricantes excluir a otros (incluidos los propios usuarios) del acceso, uso y monetización de los datos. Esta situación convierte a los fabricantes en “propietarios de facto” de los datos, lo que les permite utilizarlos, compartirlos o incluso transferir esa posición de control técnico a terceros, sin requerir formalmente derechos legales exclusivos (citado en Eckardt & Kerber, 2024).

No obstante, el Data Act plantea un cambio al establecer, en sus artículos 4(13) y 4(14), que los *data holders* ya no pueden utilizar, compartir o extraer valor de los datos sin el consentimiento del usuario. Este giro normativo implica una reasignación del conjunto de facultades para empoderar a los usuarios legítimos de los dispositivos, quienes pasan a ocupar el centro del enfoque de la gobernanza de datos no personales. En ese sentido, el derecho de uso reconocido en el Data Act deja de estar condicionado por la posición técnica de control y pasa a depender de la voluntad y legitimación del usuario, reforzando una idea de una redistribución estructural del poder informacional en entornos industriales conectados.

El reconocimiento de un derecho de uso condicionado permite fomentar un modelo de gobernanza de los datos que promueva la eficiencia sin comprometer la competencia ni el reparto justo del valor generado. En entornos como el sector minero, esta regulación garantiza que los proveedores tecnológicos puedan seguir desarrollando soluciones avanzadas a partir de los datos operativos, pero sin apropiarse unilateralmente de la información ni impedir que los usuarios o terceros autorizados también la utilicen.

De igual modo, siguiendo la línea de Specht-Riemenschneider (2023) y Graef y Husovec (2022), este enfoque funcionalista genera un entorno más equilibrado donde los datos pueden circular, reutilizarse y potenciarse en distintos niveles, respetando siempre la voluntad y el interés de

quienes los generan. De este modo, el derecho de uso se articula como una herramienta de gobernanza técnica y económica, y no como una manifestación de propiedad exclusiva.

Aunque el *Data Act* representa un avance significativo en el reequilibrio del control sobre los datos no personales generados por dispositivos inteligentes, la solución normativa que se propone al pretender centralizar la titularidad funcional del acceso, uso y compartición en el usuario del dispositivo, no está exenta de tensiones. Si bien esta redistribución busca corregir el control de facto ejercido por los fabricantes, puede generar un nuevo desequilibrio al otorgar al usuario un poder de decisión que, en ciertos contextos, podría operar en detrimento de otros actores legítimamente interesados, como terceros innovadores o incluso el propio proveedor, cuando este actúa de buena fe o con fines técnicos justificables.

Desde una perspectiva crítica, autores como Duch-Brown, Martens y Mueller-Langer (2017) advierten que el control excesivamente concentrado en un único actor puede replicar, bajo otro esquema, los mismos problemas que intenta resolver: restricciones a la reutilización de datos, limitación de flujos informacionales y fricción en la innovación. En sectores industriales complejos, como el minero, un modelo centrado exclusivamente en la voluntad del usuario podría generar bloqueos contractuales o estratégicos al uso compartido de datos que son técnicamente generados en entornos interdependientes.

Asimismo, Diker Vanberg & Ünver han advertido que, aún en el caso de protección de datos personales, si bien el empoderamiento del usuario es deseable, la excesiva dependencia de su consentimiento individual puede limitar la fluidez de los ecosistemas de datos**,** (citado en Drexl, 2018, p. 54) especialmente en entornos donde los usuarios carecen de incentivos o capacidad técnica para gestionar adecuadamente el acceso o definir los términos de uso. Esta posición cobra fuerza en contextos B2B con estructuras técnicas complejas, donde la función de coordinación y gobernanza de datos no puede delegarse completamente en decisiones individuales sin riesgo de fragmentación.

En ese sentido, a pesar que la solución del *Data Act* pretenda corregir la asimetría existente a favor del fabricante, esta centralización en el usuario no debería entenderse como un punto de llegada, sino como un punto de partida para explorar modelos más balanceados, como los *data stewardship models* (modelos fiduciarios), *data commons (*gobernanza colectiva de los datos) o *data trusts (*en donde un tercero administrador fiduciario gestiona los datos en nombre de un grupo de beneficiario) que distribuyen los derechos de uso de manera proporcional entre

actores, atendiendo a sus roles, aportes y riesgos (Mills, 2019). Así, se podría evitar que la reconfiguración de poder sobre la información derive simplemente en una "asignación de mayor fuerza a los usuarios", en lugar de habilitar mecanismos verdaderamente cooperativs y orientados al beneficio sectorial o social.

A propósito del "*data stewardship*" o la idea de un fideicomiso de datos, son entidades que gestionan los datos en nombre de los contribuyentes de datos y otros beneficiarios para facilitar el acceso justo y no discriminatorio y, al mismo tiempo, protegen los intereses de los actores que contribuyen a generarlos, lo cual es una alternativa de solución innovadora para gestionar estos derechos de uso y acceso (Eckardt y Kerber, 2024). Los autores también sugieren abiertamente esta propuesta como una herramienta efectiva para aliviar las limitaciones de los derechos de acceso y uso individual que ha implementado el *Data Act* y, al mismo tiempo, pueden abordar cuestiones de monopolios y distribuir beneficios.

En la aplicación del sector minero, el fideicomiso podría ser un comité de representantes de empresas mineras, proveedores y otras partes interesadas, incluyendo la participación del Estado. Las decisiones sobre acceso de ciertos datos se tomarían de manera conjunta y también modos de resolución de conflictos. Las empresas mineras acceden a sus datos para buscar sostenibilidad o mejorar sus operaciones, los proveedores o fabricantes pueden utilizar los datos para mejorar sus dispositivos AIoT o crear nuevos productos y, terceros como investigadores u otras empresas de análisis de datos podrían acceder bajo condiciones específicas. De este modo se fomenta la colaboración entre agentes económicos y la creación de datos abiertos, confiables y reales.

Abordando este derecho desde una perspectiva económica, la implementación busca equilibrar intereses de los múltiples actores intervinientes en la cadena de valor de los datos. Por un lado, los usuarios, requieren acceder y utilizar los datos para mejorar la eficiencia operativa, optimizar procesos extractivos, reducir costos o fortalecer la seguridad. Por otro, los proveedores tecnológicos cuentan con un legítimo interés en recuperar la inversión realizada en el desarrollo de dispositivos inteligentes y modelos de IA, y aspiran a obtener retornos mediante la explotación de los datos generados por sus tecnologías (Eckardt & Kerber, 2024). La normativa evita reconocer automáticamente un derecho de uso inherente al control técnico, y obliga a direccionar dicho uso a través de la negociación contractual, lo que promueve una asignación más justa de los beneficios derivados del uso de los datos.

La delimitación del derecho de uso requiere establecer condiciones claras, tanto desde el diseño contractual como desde la política pública. Es fundamental definir los fines legítimos y específicos para los cuales los datos pueden ser usados, evitar ambigüedades legales que permitan usos indeseados y asegurar que no se restrinja injustificadamente la reutilización de datos por otros actores autorizados.

Particularmente en el sector minero, donde múltiples proveedores ofrecen soluciones a una misma unidad operativa, la disputa entre intereses de los actores puede generar tensiones alrededor del uso de datos. Es importante que se puedan abordar los legítimos intereses de las partes que intervienen. Por un lado, los usuarios de las minas, quienes requieren acceso a los datos para optimizar operaciones, garantizar seguridad y buscar eficiencia y, por otro lado, es posible que busquen acceso y uso sin restricción alguna por parte de los fabricantes. Esto los legitima a compartir los datos a terceros proveedores competidores, sin embargo, se pueden establecer límites para evitar prácticas anticompetitivas.

Los proveedores tecnológicos buscan recuperar los costos en los que han incurrido en el desarrollo del dispositivo inteligente y buscan el retorno económico mediante la explotación de los datos que se generan en el AIoT, ofreciendo soluciones sólidas, eficientes y que les permita obtener ganancias. En ocasiones, con el fin de beneficiarse de manera absoluta, son quienes mantienen un interés por limitar a nivel técnico el uso de los datos no personales por terceros, a fin de proteger su posición en el mercado.

Frente a ello, es necesario fomentar marcos de gobernanza que respeten tanto la autonomía del usuario como el interés económico legítimo de los proveedores, permitiendo compartir datos con terceros bajo condiciones de equilibrio competitivo. Esto exige mecanismos contractuales bien definidos, pero también estándares sectoriales que eviten la fragmentación normativa y promuevan prácticas equitativas.

Además, la normativa especializada debe definir fines específicos y fines legítimos, de tal modo que permitan equilibrar los intereses entre las partes, pero limitar las prácticas de beneficio unilateral o la competencia desleal. Incluso con la intervención del Estado, quien puede intervenir no solo para aprovechar también de los datos a partir de un interés público (para salvaguardar cuestiones sobre el medio ambiente o la protección de bienes públicos, la prestación de un servicio público, etc), sino también con regulación que garantice prevención del abuso de poder,

fomento de la competencia o incentivos de colaboración como *data trust* que gestionan accesos a datos sectoriales.

El Estado cumple un rol clave en la regulación del derecho de uso, tanto desde su dimensión garantista como desde su función promotora del interés público. En primer lugar, debe establecer límites normativos frente al uso dominante o unilateral de los datos que afecten la competencia, la privacidad o el acceso equitativo a la innovación. Y, en segundo lugar, puede facilitar modelos de gobernanza colaborativa mediante instrumentos como los *data trust*, entidades fiduciarias que gestionan el acceso y uso de datos en sectores estratégicos, promoviendo esquemas de cooperación entre actores públicos y privados (Mills, 2019).

En conclusión, el derecho de uso constituye una herramienta estratégica para equilibrar el valor informacional generado por tecnologías AIoT en sectores productivos como el minero. Su ejercicio exige acuerdos claros, estándares técnicos y mecanismos de gobernanza que permitan compatibilizar los intereses de los usuarios, los proveedores tecnológicos y la sociedad en su conjunto. Frente a la complejidad de las relaciones B2B y la sensibilidad económica del uso de datos, resulta un factor clave para adoptar un enfoque regulatorio que combine distribución justa a través de la negociación y marcos institucionales flexibles, a fin de evitar desequilibrios y garantizar un uso ético y productivo de los datos no personales.

5.3. Derechos de Compartición

El derecho de compartición previsto en el artículo 5 del *Data Act* también es una extensión espontánea del derecho de acceso, en tanto faculta al usuario del producto o servicio conectado acceder y utilizar los datos generados, además de autorizar a terceros para que accedan y los utilicen bajo condiciones previamente definidas. Este derecho refleja una transformación estructural en la gobernanza de los datos no personales, ya que desplaza la facultad de decidir con quién se comparte la información desde el fabricante o proveedor tecnológico hacia el usuario operativo del dispositivo (Eckardt & Kerber, 2024).

El derecho de compartición responde al propósito de fomentar la competencia, la innovación y la interoperabilidad, habilitando que empresas distintas al proveedor original, como servicios de mantenimiento, proveedores complementarios, aseguradoras o analistas de datos, puedan acceder directamente a los datos generados, siempre que cuenten con autorización expresa del usuario y respeten los fines autorizados.

A nivel práctico, el ámbito del derecho de compartición permite que el usuario minero *autorice a un tercero* acceder directamente a los datos generados por el AIoT. Este derecho de compartición permite, por ejemplo, que las empresas de mantenimiento, analítica de datos, o aseguradoras accedan a los datos con autorización del usuario, que el tercero pueda usar los datos únicamente para la finalidad autorizada o que esté sujeto a obligaciones de confidencialidad, seguridad y uso adecuado.

Desde una perspectiva jurídica, el derecho de compartición implica reconocer al usuario una posición céntrica en la toma de decisiones sobre la circulación de datos, permitiéndole ejercer una función de *gatekeeper* respecto al acceso de terceros. Esta capacidad se encuentra sujeta a ciertos límites, como la obligación de que el tercero solo utilice los datos con fines determinados, y que garantice estándares adecuados de confidencialidad, ciberseguridad y protección de información sensible (art. 5.4 del *Data Act*).

Desde la perspectiva comercial, este derecho tiene un profundo impacto en la estructura competitiva del ecosistema de datos. Permitir que los usuarios compartan datos con terceros genera un entorno más abierto, en el que se reducen los efectos de *lock-in* y se habilita la participación de nuevos actores en la cadena de valor informacional (Duch-Brown, Martens & Mueller-Langer, 2017). Además, promueve la innovación en servicios digitales, al permitir que empresas distintas al proveedor original desarrollen soluciones especializadas a partir de los mismos datos base.

Sin embargo, una excesiva concentración del poder de decisión en el usuario puede perpetuar la fragmentación del acceso a los datos, la falta de estandarización técnica y en general, limita nuevamente el derecho al acceso a los datos en general. En contextos B2B como el sector minero, donde múltiples proveedores interactúan sobre una misma infraestructura, es ideal que el fomento de la innovación a partir del acceso y compartición de los datos se pueda distribuir de manera equitativa y diversificar, sin que el poder de ejercicio de este derecho recaiga sobre un solo actor.

El derecho de compartición adquiere una relevancia particular en el contexto industrial minero, porque al haber múltiples proveedores que ofrecen soluciones tecnológicas, de análisis o soporte adecuadas a los procesos mineros y desplegados en una misma operación, diversificar el control produciría mayores beneficios y crecimiento colectivo.

En estos escenarios, garantizar que los datos puedan ser compartidos de manera ordenada y bajo criterios de equidad permite fomentar la innovación en servicios digitales complementarios, reducir los riesgos de monopolios a partir del proveedor tecnológico inicial, promueve la interoperabilidad entre operaciones e incentiva la competencia entre actores con igualdad de oportunidades. Sin embargo, esta compartición debe estructurarse con criterios técnicos y jurídicos estandarizados. Como ha señalado Mills (2019), es necesario establecer reglas claras que resulten suficientes para gestionar el volumen, sensibilidad y complejidad de los datos en sectores como el industrial extractivo.

El derecho de compartición se configura como un pilar esencial para una economía de datos abierta, interoperable y equitativa. Si bien otorga al usuario un rol central en la decisión sobre el destino de los datos generados, su eficacia depende de la existencia de condiciones técnicas, contractuales e institucionales que estructuran el acceso por parte de terceros de forma segura, trazable y competitiva. Es crucial que se prevean condiciones o mecanismos de gobernanza colaborativa, regulación sectorial y estructuras neutrales que garanticen una distribución justa, evitando cuellos de botella o formas encubiertas de exclusión.

6. Desafíos de la propiedad de los datos no personales

6.1. Monopolización de los datos

Uno de los principales riesgos que derivan de las relaciones B2B en el uso de dispositivos AIoT, es la consolidación de estructuras de control técnico exclusivo por parte de los fabricantes del producto conectado. Estos proveedores diseñan sistemas cerrados por defecto, lo cual les permiten generar un acceso exclusivo a los datos generados por estos dispositivos, lo que en la práctica configura monopolios de facto, en el uso y explotación de información. Esta situación se produce principalmente por la ausencia de límites y controles específicos sobre los usuarios u otros actores intervinientes, permitiendo que dichas prácticas se mantengan vigentes en el mercado de los datos y el entorno digital.

En este contexto, uno de los ejes centrales alrededor de la construcción de una regulación, es el fomento de sistemas de gestión de datos abiertos, que permitan un acceso más equitativo a la información generada y que prevengan concentraciones informacionales injustificadas. Tal como se ha discutido a lo largo del presente capítulo, las distintas posiciones sobre la atribución de derechos exclusivos derivan en escenarios de apropiación técnica, amparados bajo argumentos de confidencialidad, acuerdos previos contractuales o de propiedad intelectual.

Frente a ello, es indispensable incorporar una ponderación de derechos, especialmente cuando colisionan, como el derecho constitucional a la información o el principio de libre competencia. En este sentido, cualquier excepción o restricción que limite el acceso legítimo a los datos deberá superar un examen de proporcionalidad**,** asegurando que los intereses protegidos no se impongan de manera desproporcionada sobre derechos igualmente relevantes.

Esta necesidad de ponderar intereses en conflicto encuentra cierta justificación en la doctrina de las facilidades esenciales, desarrollada en el ámbito del derecho de la competencia. Dicha teoría establece que, cuando una empresa dominante controla un recurso o infraestructura indispensable para que otros actores compitan en el mercado, puede imponerse la obligación de otorgar acceso a ese recurso bajo condiciones objetivas, razonables y no discriminatorias (Kresalja & Quintana, 2015, pp.59-60).

Esta doctrina se diseña para contextos de infraestructura de red o monopolios naturales (redes eléctricas, espectro radioeléctrico) y aplica a los casos donde los recursos son rivales, cuando no son replicables económicamente por otro agente. En otras palabras, se aplica cuando sin el acceso abierto a dicho “recurso” otros nuevos operadores no podrían siquiera competir porque no tienen acceso a ello y, por ende, la competencia sería imposible.

Aplicado al contexto AIoT, los datos generados por dispositivos inteligentes, *prima facie,* son considerados un insumo esencial para la innovación y la prestación de servicios tecnológicos. Sin embargo, los datos no personales al ser no rivales y replicables de diferentes maneras, su uso por un actor no impide que otro lo utilice, y sobre el acceso, es posible que pueda ser obtenido en diferentes formas bajo una misma infraestructura pero con la posibilidad de comprometer la calidad o una inversión adicional.

Evitar que los dispositivos AIoT se conviertan en mecanismos de concentración informacional requiere no solo reglas claras sobre derechos de acceso, uso y compartición, sino también una vigilancia activa sobre prácticas que puedan reproducir monopolios bajo nuevas formas tecnológicas. Una regulación basada en principios de proporcionalidad, transparencia y apertura funcional será clave para garantizar un entorno competitivo y justo en la economía de datos del sector minero.

Si bien la doctrina de las facilidades esenciales (DFE) ha sido tradicionalmente aplicada a recursos cuya duplicación resulta inviable por razones técnicas, legales o económicas, como

redes de telecomunicaciones o infraestructuras de monopolio natural, su aplicación al ámbito de los datos no personales generados por dispositivos AIoT merece una consideración particular. Aunque los datos no son, en principio, recursos físicamente indivisibles o técnicamente irreproducibles, en la práctica, su generación, acumulación y procesamiento sí puede estar concentrado en ciertos actores que han alcanzado posiciones dominantes en el mercado, ya sea por su capacidad de inversión, trayectoria o integración vertical de soluciones tecnológicas.

En ese sentido, la teoría de las facilidades esenciales (DFE) ofrece un marco conceptual útil para abordar los desafíos de acceso y uso de los datos no personales generados por AIoT o dispositivos conectados en contextos B2B. Según Diez Canseco (2012) la DFE determinaría que son una facilidad esencial si:

a) Constituye en un activo esencial para que una empresa desarrolle una actividad en un determinado mercado.
b) Es un activo que no puede ser duplicado o replicado por la competencia y con efectos exclusorios en el mercado en el que se solicita
c) Debe ser susceptible de uso compartido. (pp. 80-85)

De manera preliminar, señalamos que la DFE no es suficiente para abordar el problema puesto que no necesariamente cumple con los 3 requisitos exigidos. Los datos no personales son imprescindibles para competir o aplicarlos en servicios complementarios, es necesario de datos para poder generar productos tecnológicos, procesarlos y crear resultados significativos para una industria. La falta de acceso y la constante denegatoria por argumentos estratégicos contractuales o bajo esquemas de secretos industriales pueden impedir la entrada a estos datos no personales y en consecuencia, afectar la competitividad del sector. Sin embargo, no es cierto que este activo no pueda ser duplicado. Si bien el acceso a los datos es más fácil partiendo de los datos previamente recopilados por otro proveedor, no significa que no puedan ser obtenidos por cuenta propia.

A modo de ejemplo, los sensores instalados en equipos mineros generan datos industriales críticos sobre el rendimiento de las máquinas y el entorno operativo. Estos sensores recogen datos esenciales sobre el rendimiento del equipo y las condiciones del entorno operativo. Si el fabricante del vehículo conectado retiene el control exclusivo de dichos datos y deniega el acceso a un proveedor externo que desarrolla soluciones compatibles o complementarias, se imposibilita

la innovación en servicios, y la mina, como usuario final, ve limitada su capacidad para optimizar su operación e inversión tecnológica.

En tal caso, la aplicación de la DFE podría justificar una obligación de compartir los datos en términos justos, razonables y no discriminatorios, equilibrando así los intereses de ambas partes y fomentando un ecosistema más competitivo e interoperable. Sin embargo, esta doctrina ofrece ciertos mecanismos en los que se encuentran oportunidades que llevan a la idea de que, si bien la DFE puede ser un modelo de inspiración para fomentar la libre competencia en mercados particulares como el estudiado, no se puede aplicar en sentido estricto debido que la naturaleza de los datos no personales no encaja en la categoría de una facilidad esencial.

Al igual que un puerto o una red de telecomunicaciones, ciertos datos no personales generados en contextos de AIoT para minas pueden ser insumos indispensables para competir (por ejemplo los datos de la flota minera, sensores de seguridad u otros que son necesarios para los servicios de mantenimiento predictivo), también no son replicables por un tercero porque depende de un acceso exclusivo a sensores instalados en los fabricantes de las maquinarias (OEM) y cuando este último se niega a compartir sus datos, limita la competencia en mercados relacionados.

Sin embargo, siguiendo como referencia el ejemplo de la red de postes eléctricos, los datos no se agotan ni se deterioran por un uso simultáneo, lo que debilita la premisa de escasez física que justifica la calificación de “esencial” para la prestación de un servicio. No todos los datos son necesarios, pueden existir diferentes fuentes alternativas, que comprometen su calidad o eficiencia, pero que se pueden inferir de otras fuentes o mediante una inversión adicional.

Finalmente, si obligamos a que todo datos sea compartidos mediante la DFE, los fabricantes podrían perder incentivos para invertir en tecnologías de sensorización, porque la ventaja competitiva prevalece sobre sus datos y por ende, se crearían nuevas formas para mantener un control perpetuo sobre estos.

Saraf y Katare (2023) sostienen que no todos los datos constituyen una facilidad esencial. Por su naturaleza no competitiva, la monopolización de datos por parte de un actor con posición dominante no impide que otros competidores obtengan datos equivalentes de otras fuentes, tal como sucedió en los casos de Telefónica UK/Vodafone UK/Everywhere/KC. En este caso se sostuvo que aun cuando las empresas conjuntas pueden procesar más datos de consumidores, ello no limita la capacidad de los competidores de recopilar información equivalente. Esto

demuestra que los datos son duplicables, son no rivales y existen sustitutos parciales que permiten a los competidores mejorar sus servicios, los cual evidencia que quedan fuera del ámbito de la DFE.

Los autores señalan que incluso en el contexto indio, no existe jurisprudencia consolidada. En el caso *National Restaurant Association versus Zomato*, la Asociación apeló que plataformas de reparto como *Swiggy* y *Zomato* incurrían en conductas anticompetitivas al ocultar datos de consumidores (*data masking*), lo que privaba a los restaurantes que eran asociados a acceder a información valiosa para su negocio y generaban problemas de transparencia. No obstante, la Comisión de Competencia India no emitió decisión respecto al enmascaramiento de datos, dejando abierta la cuestión sobre si podía aplicarse del DFE en este caso.

En otras palabras, la aplicación de la DFE a los datos no personales del AIoT plantea desafíos normativos que deben abordarse cuidadosamente. Uno de los principales consiste en definir con precisión de qué datos puede considerarse “esenciales”, evitando generalizaciones que puedan desincentivar la inversión de los fabricantes o afectar la protección de activos intangibles. En esa línea, es necesario establecer criterios normativos que permitan identificar cuándo un conjunto de datos es efectivamente insustituible para la competencia y no meramente conveniente, lo que puede ser una limitación técnica, cuando la tendencia de hoy es maximizar el uso de datos posible.

Es indispensable equilibrar el derecho de los fabricantes a proteger sus secretos comerciales con los intereses legítimos de los usuarios y terceros innovadores. En este contexto, la solución podría encontrarse en la implementación de accesos pero con límites de mecanismos de compensación proporcional y razonables, que reconozcan los costos asumidos por los fabricantes en la generación, almacenamiento y puesta a disposición de los datos, dependiendo del tipo de procesamiento que se les haya aplicado y los esfuerzos adicionales en materia de interoperabilidad, las condiciones de seguridad y la infraestructura técnica asociada.

Los datos no personales utilizados en contextos de AIoT no deben calificarse directamente como facilidades esenciales porque su naturaleza no rival y reproducible los distingue de las infraestructuras físicas. Sin embargo, su lógica puede inspirar un marco de gobernanza sectorial, cuando la negativa de acceso a ciertos datos impide efectivamente la competencia e innovación.

Aunque la DFE constituye en una herramienta útil para promover marcos jurídicos innovadores que protejan el concepto de los bienes digitales comunes, promover el acceso equitativo, prevenir abusos de posición dominante y dinamizar los mercados complementarios, su eficacia dependerá de la capacidad de los reguladores para establecer criterios objetivos, mecanismos de compensación justos y garantías de protección técnica e informativa, que equilibren el derecho a la competencia con el fomento legítimo de la innovación tecnológica.

6.2. Desincentivos a la innovación tecnológica

Establecer regímenes de exclusividad en la explotación de los datos generados por dispositivos AIoT puede producir efectos adversos importantes sobre la innovación tecnológica. Cuando el acceso a los datos no está garantizado, o está sujeto a barreras técnicas, económicas o contractuales impuestas por quienes detentan el control de facto y dominante sobre estos –generalmente los fabricantes o desarrolladores de las soluciones tecnológicas–, se genera un entorno de incertidumbre que desincentiva a nuevos actores a invertir en el desarrollo de productos o servicios que dependen de dichos datos.

Tal como advierten Eckardt y Kerber (2024), el control exclusivo de facto que ejercen los fabricantes sobre los datos no personales, sumado a decisiones técnicas como el diseño de sistemas cerrados o la falta de interoperabilidad, les permite establecer precios monopólicos sobre el acceso a datos, restringiendo su volumen de circulación y provocando una sub-utilización sistemática de información crítica. Esta situación genera pérdidas de bienestar *(deadweight losses)* y restringe el potencial innovador en mercados secundarios como el mantenimiento predictivo o los servicios analíticos especializados.

Este riesgo es particularmente relevante para *startups*, micro y pequeñas empresas (MYPEs) en el sector minero, cuyos modelos de negocio suelen basarse en soluciones altamente especializadas, muchas de las cuales requieren datos operativos para ser diseñadas, entrenadas o validadas. En ausencia de acceso abierto o regulado a este tipo de datos, los actores se enfrentarían a barreras de entrada, reduciendo su participación en el mercado e impidiendo la diversificación de la innovación tecnológica dentro del ecosistema industrial.

Adicionalmente, existe un riesgo conexo que debe subrayarse: la infrautilización de los datos**.** Cuando los datos generados por dispositivos inteligentes no se comparten, reutilizan ni activan en procesos de análisis, predicción o desarrollo de soluciones complementarias, se convierten

en activos estáticos que no generan valor más allá del uso restringido que les da el titular del control técnico. Como señala la Cámara de Comercio Internacional (ICC), las restricciones innecesarias al flujo o compartición de datos no personales pueden impedir que estos se transformen en insumos útiles para soluciones sociales, económicas o industriales, elevando los costos y reduciendo la eficiencia de los ecosistemas digitales, especialmente para negocios emergentes (2023).

Asimismo, la desigualdad de condiciones entre grandes empresas y actores emergentes se ve reflejada en la dificultad que enfrentan las MYPEs para acceder a datos en igualdad de condiciones. En América Latina, por ejemplo, las pequeñas empresas que prestan servicios o son proveedores del sector minero desde el ámbito tecnológico enfrentan limitaciones estructurales para integrar tecnologías de análisis de datos debido a la falta de acceso, recursos técnicos y marcos jurídicos habilitantes (CEPAL, 2013)

Este escenario, además, genera un impacto negativo acumulativo. A medida que se consolidan estructuras cerradas de explotación informacional, se reduce el incentivo para que otros actores apuesten por el desarrollo de soluciones interoperables o innovadoras, generando un círculo vicioso de dependencia, estancamiento y concentración de mercado. Este efecto no solo afecta la dinámica competitiva, sino que también limita el avance de tecnologías emergentes como la inteligencia artificial aplicada a la minería, la eficiencia energética o la gestión predictiva de activos críticos.

Frente a ello, la apertura de datos bajo marcos contractuales justos, condiciones técnicas interoperables y estructuras de gobernanza colaborativa se presenta como una condición necesaria para activar la innovación tecnológica en entornos AIoT, especialmente en sectores estratégicos como el minero, donde el potencial transformador de los datos aún está lejos de ser plenamente aprovechado.

6.3. Creación de barreras de entrada

Como se ha analizado hasta ahora, las distintas teorías sobre la atribución de titularidad respecto de los datos no personales reflejan tensiones en torno a la concentración del control informacional. La consolidación de derechos exclusivos sobre datos generados por tecnologías AIoT puede traducirse en obstáculos para la participación de pequeñas y medianas empresas (MYPEs) y *startups*, las cuales generalmente carecen de los recursos financieros, capacidades

técnicas o poder de negociación necesaria para acceder, licenciar o explotar esos datos en condiciones competitivas.

Este fenómeno no solo produce un entorno de exclusión, sino que consolida asimetrías que limitan el dinamismo del ecosistema digital. Como advierten Duch-Brown, Martens y Mueller-Langer (2017), los regímenes de acceso restringido generan efectos de monopolización sobre los datos, transformándolos en barreras de entrada que restringen el desarrollo de nuevos productos o servicios derivados. A esto se suma el riesgo de ineficiencia económica, ya que la exclusividad en el control de datos tiende a inhibir su circulación, reduciendo su aprovechamiento colectivo y generando pérdidas de bienestar (*deadweight losses*) en mercados complementarios.

Por otra parte, la titularidad compartida sobre los datos, si bien aparece como una alternativa al modelo de apropiación exclusiva, presenta desafíos jurídicos relevantes**.** En particular, la falta de mecanismos claros para regular la forma en que los cotitulares pueden usar, explotar o autorizar el acceso a los datos puede derivar en disputas contractuales, incertidumbre jurídica o bloqueos estratégicos. Como señala la Cámara de Comercio Internacional (ICC, 2023)**,** cuando no existen reglas claras sobre la interoperabilidad, gobernanza y licenciamiento, el riesgo de conflicto entre intereses divergentes se incrementa, especialmente en sectores con múltiples actores operando simultáneamente sobre los mismos datos.

Frente a este escenario, se han identificado enfoques regulatorios alternativos para mitigar la creación de barreras de entrada y fomentar una economía de datos inclusiva. En primer lugar, la promoción de modelos de datos abiertos (*open data*) constituye una herramienta clave para democratizar el acceso. Esto incluye no solo la disponibilidad de datos en formatos estructurados, legibles y reutilizables, sino también el fomento de licencias abiertas, que permitan a las MYPEs utilizar la información sin incurrir en altos costos de transacción. En efecto, como sostiene Tarkowski y Vogelezang (2021)**,** los derechos exclusivos sobre datos deben ser limitados cuando generan obstáculos a la competencia y a la reutilización eficiente, proponiendo modelos de gobernanza basados en bienes comunes informacionales (*data commons*) como alternativa equilibrada.

En segundo lugar, en los casos de cotitularidad de datos, resulta crucial establecer mecanismos que permitan una distribución funcional de los derechos. La regulación debe evitar que alguno de los titulares impida el uso compartido mediante prácticas anticompetitivas o estrategias de

bloqueo, garantizando que todas las partes puedan beneficiarse equitativamente de la explotación tecnológica de los datos. El diseño de acuerdos tipo, cláusulas de resolución de disputas y estructuras neutrales de gobernanza puede aportar claridad en este sentido.

Finalmente, una estrategia cada vez más explorada por los reguladores es la implementación de *sandbox* regulatorios**,** que permiten crear entornos de prueba para innovaciones emergentes sin que estas estén sujetas de forma inmediata a marcos regulatorios restrictivos o desproporcionadamente onerosos. Como destaca la literatura en gobernanza tecnológica, los *sandbox* regulatorios permiten un equilibrio flexible entre la necesidad de proteger derechos adquiridos y la urgencia de promover la innovación, constituyéndose en un instrumento adaptativo para explorar nuevos modelos de acceso, licenciamiento y compartición de datos.

En conclusión, reducir las barreras de entrada en el uso de datos no personales generados por el AIoT exige un enfoque regulatorio orientado a la apertura controlada, la interoperabilidad funcional y la equidad entre actores**.** El acceso justo y competitivo a los datos no solo es un prerrequisito para el desarrollo de tecnologías inclusivas, sino también un factor indispensable para dinamizar la competencia, reducir la dependencia en el sector y fortalecer el ecosistema de innovación digital dentro de la minería.

6.4. Ausencia de Interoperabilidad

A la fecha, en el Perú, persisten los problemas de fragmentación de datos abiertos que se han puesto a disposición a través de la Plataforma Nacional de Datos Abiertos (PNDA). Un esfuerzo implementado mediante políticas estatales sectoriales promovidas por la Secretaría de Gobierno y Transformación Digital, adscrita a la Presidencia de Consejo de Ministros (PCM), y que a partir de la Ley de Gobierno Digital aprobado por Decreto Legislativo No. 1412 dispone un marco normativo para impulsar la transformación digital del Estado peruano con una gestión eficiente, interoperable y segura a nivel nacional, regional y local.

Esta ley cubre muchos aspectos claves alrededor de la interoperabilidad en términos de accesibilidad a los servicios públicos de forma eficiente y equitativa. Esto implica que, en el marco de acceso a la información pública, se contemple la publicación de los datos que manejan las entidades públicas con el objetivo de promover espacios que aporten a la innovación digital y gobierno de datos (Gobierno del Perú, s/f).

Disponer de datos abiertos significa que los datos pueden presentarse en estructuras diversas y, muchas veces, no representan un estándar único para visualizarlos o utilizarlos. Nicon Consortium, en el marco del Centro de Cooperación Digital Gubernamental de Perú y Corea, también analiza la situación actual de los datos abiertos y el marco normativo, evidenciando la existencia de algunos problemas respecto de la plataforma, como la falta de datos estandarizados, la falta de APIs y de información sobre acceso a datos, que impide que los desarrolladores e investigadores utilicen plenamente los datos, su integración y análisis de datos de múltiples fuentes (Nicon Consortium, 2024). Con ello, al considerarse una publicación voluntaria por parte de los privados, la fragmentación a nivel técnico se mantiene en términos de legibilidad, accesibilidad y seguridad entre sistemas.

De ese modo, se dificulta el acceso a estos desde fuentes de datos abiertos, al no adoptar un enfoque pleno de la interoperabilidad, dado que es una solución cercana a los problemas creación de barreras de "bloqueo de datos" (*lock-in data*) entre los diferentes actores del mercado.

En setiembre del 2025, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, ha elaborado la "*Estrategia Nacional de Gobierno de Datos 2026-2030*" aún sujeto a consulta. Este documento constituye un lineamiento clave para impulsar la interoperabilidad en las entidades públicas, fomentar la innovación en el aprovechamiento de datos personales y no personales generados por las entidades públicas, a partir de instrumentos de gestión de los datos y creación de repositorios centralizados con datos de calidad e interoperables.

A pesar que está centrado en el ámbito gubernamental, su orientación es relevante para analizar cómo los contextos actuales exigen panoramas de gobernanza de datos basados en condiciones de interoperabilidad e innovación tecnológica. Su consideración en el marco de las relaciones B2B en sector privado permite observar como los principios de interoperabilidad y gobernanza pueden ser trasladados a espacios privados y en contextos industriales, promoviendo la creación de ecosistemas digitales más abiertos y competitivos que puedan aportar en mejorar los servicios públicos y garantizar la disponibilidad de los datos para el público en general.

Can Atik (2022), desde su perspectiva en la agroindustria y en base a conceptos de *data governance*, considera que los problemas técnicos relacionados con barreras de interoperabilidad o estándares tecnológicos pueden resolverse mediante la provisión de

derechos de acceso en lugar de derechos exclusivos sobre los datos, mitigando así, los riesgos de aislamiento de los datos fragmentados. No obstante, aunque esta propuesta podría resolver algunos problemas, sigue siendo necesario crear espacios estructurados para compartir datos con un enfoque en la interoperabilidad.

Asimismo, este autor señala que la interoperabilidad técnica requiere que los proveedores de tecnología adopten estándares que permitan el intercambio de datos entre dispositivos y plataformas (Atik, 2022). De ese modo, hace útil el concepto de open data, en tanto hace disponibles diversas fuentes de datos, pero los estándares deberían manejarse por consensos de manera sectorial o uniforme.

Además, podría lograrse mediante el diseño de derechos de acceso, exigencias de estándares mínimos en el acceso, incluso con una definición amplia del derecho de acceso *per se*, ya sea que se pueda adaptar a temas de legibilidad en diferentes tecnologías, o en términos de disponibilidad, cuando abarca un uso en tiempo real, con el fin de que se genera una coexistencia de servicios de múltiples proveedores dentro de una misma operación.

No obstante, dado que la principal motivación para el uso de los datos es la monetización exclusiva de los datos, en la actualidad se excluye del aprovechamiento a través de condiciones de apropiación de facto (ya sea por la arquitectura o diseño por *default* de los dispositivos o sistemas que recopilan datos), como la predominancia de quien realiza el tratamiento de los datos en las relaciones comerciales. Esto además, se debe a que al tener mejor posición a nivel técnico hace el acceso mucho más fácil y la custodia es un hecho.

Esta situación crea una especie de barrera de acceso libre por parte de diferentes actores que no dispongan de facultad de negociación y derechos que otorguen acceder a tal información. En estos casos, si quien recopila los datos se atribuye la posesión y control total sobre los datos, podría rechazar solicitudes de acceso bajo diversos argumentos, limitando así la competencia y el desarrollo tecnológico.

Asimismo, *ICC Policy Primer on Non-Personal Data* (2023) define la interoperabilidad como la capacidad de diferentes sistemas, dispositivos o aplicaciones de interactuar, intercambiar y utilizar datos entre sí de manera efectiva, independientemente de sus características técnicas propias. Ello es importante en el contexto de los datos no personales porque al permitir conexión

y legibilidad de los mismos, se fomenta su uso, reutilización y transferencia en diversos contextos y sectores.

La ausencia de un estándar que permita la comunicación diversificada o la lectura de los datos entre diferentes sistemas podrían generar ciertas barreras. Incluso los derechos de propiedad intelectual son ejercidos sobre ciertos sistemas, limitando la posibilidad de que puedan ser compartidos o tener acceso directo, mucho menos en tiempo real de los datos. Dicha fragmentación y restricción reduce la eficacia de sistemas como de IA para ser entrenados y el potencial uso de estos se acapara.

Además, se argumenta que la falta de interoperabilidad también responde a preocupaciones sobre la seguridad en el intercambio de datos entre sistemas, lo que podría comprometer la privacidad y facilitar el uso inadecuado de los datos o inclusive, de los accesos que se podrían facilitar a nivel de *hardware* o estructura física. Por ello, es crucial adoptar estándares no solo para garantizar la legibilidad de los datos, sino también para exigir la adopción de mecanismos con altos niveles de seguridad y privacidad en su acceso e intercambio.

Un desafío adicional radica en los costos asociados con la implementación de sistemas interoperables. Adaptar sistemas ya operativos para permitir su conexión con otros implica costos significativos, incluyendo recursos financieros y horas de trabajo para adquirir un lenguaje compatible y formato correspondiente. Estos costos pueden ser particularmente difíciles de asumir para pequeñas y medianas empresas.

Finalmente, los enfoques de Data Driven, Data Trust y Open Data son enfoques complementarios y estratégicos para la gestión, uso y regulación de datos no personales. En el contexto del AIoT y las relaciones B2B, estos principios pueden ser fundamentales para diseñar un marco regulatorio equilibrado y efectivo.

La integración de estos enfoques proporciona un marco sólido para regular los datos no personales en el uso de AIoT en relaciones B2B. Mientras que el *data trust* facilita la gestión justa de datos, el *open data* amplifica su impacto social, y el enfoque *data-driven* asegura que estos datos se utilicen de manera eficiente y estratégica. Juntos, estos principios pueden guiar una regulación equilibrada que fomente la innovación, la competencia y el desarrollo sostenible.

Aproximándonos a las conclusiones de este segundo capítulo, la atribución de titularidad de los datos no personales plantea desafíos complejos y multifacéticos que tienen implicaciones

directas en la innovación, la competitividad y la equidad en el acceso y uso de los datos. Aunque los datos no personales no están protegidos bajo las mismas reglas que los datos personales, su creciente importancia en la economía digital y su capacidad para impulsar la innovación tecnológica exigen un enfoque regulatorio que garantice un equilibrio entre los derechos de acceso, la interoperabilidad y la seguridad.

En este sentido, es evidente que el control exclusivo o la apropiación de facto de los datos no personales por parte de quienes los recopilan puede generar barreras de acceso, fragmentación del mercado y una limitación en la interoperabilidad, afectando no solo a competidores, sino también a terceros interesados en utilizar los datos para desarrollar soluciones innovadoras. Por ello, es necesario un marco regulatorio que promueva principios como la transparencia, la equidad en el acceso, la interoperabilidad técnica y la protección de la seguridad y confidencialidad de los datos a través de la atribución compartida de titularidad.

El concepto de "*Data Trust*" emerge como una herramienta prometedora para garantizar la gestión equitativa y segura de los datos no personales, permitiendo a todas las partes interesadas participar en el aprovechamiento de estos recursos bajo términos claros y equilibrados. Asimismo, la implementación de derechos de portabilidad y acceso, en lugar de derechos exclusivos de propiedad, podría contrarrestar los efectos de "bloqueo de datos" y fomentar la colaboración en sectores clave como la minería y otras industrias dependientes de tecnologías AIoT.

Finalmente, aunque las soluciones como el *open data* y los enfoques *data-driven* ofrecen vías para maximizar el valor de los datos no personales, su efectividad depende de la adopción de estándares técnicos que garanticen la interoperabilidad y el cumplimiento de altos niveles de seguridad. Solo a través de un equilibrio entre flexibilidad regulatoria, estándares técnicos comunes y mecanismos de resolución de conflictos, será posible superar los retos asociados a la titularidad y el control de los datos no personales, impulsando su uso como un recurso estratégico que promueva la innovación, la sostenibilidad y el desarrollo equitativo en el ecosistema digital.

CAPÍTULO III: ENFOQUES REGULATORIOS COMPARADOS SOBRE LOS DATOS NO PERSONALES

En el presente capítulo, se abordan los contextos regulatorios en el uso de los datos no personales desde una perspectiva global y comparada, lo que permite definir el contexto teórico de los datos no personales y su aplicación en las industrias. A partir de este enfoque, se ofrece una referencia sobre los cuestionamientos más interesantes alrededor del valor de los datos y si otras jurisdicciones han considerado pertinente el tratamiento de los datos no personales, así como qué retos existen en la regulación comparada respecto la innovación y acceso a los datos.

Dado que, en el Perú no se cuenta con una regulación específica o especializada respecto al tratamiento de los datos no personales en el contexto de la industria minera o tecnológica, el presente capítulo nos permite comparar los modelos normativos de países que han asumido este reto a la vanguardia como la Unión Europea con el *Data Act* o China con su regulación respecto de los datos industriales.

Esto nos permite evaluar y comparar diferencias y similitudes respecto de las legislaciones implementadas, o de alternativas que prevean mecanismos de incentivos o permitan la accesibilidad, reutilización y generar interoperabilidad al momento de compartir los datos no personales, especialmente en los sectores industriales. A partir de ello, se busca identificar qué aspectos son necesarios a considerar en la implementación de eventual marco regulatorio a nivel nacional que apunte hacia una un sistema más abierto, equitativo e interoperable, que permita explotar los beneficios para el desarrollo de la innovación.

1. Perspectiva europea de la regulación de datos no personales

La Unión Europea ha contribuido considerablemente en el desarrollo de una regulación comunitaria en materia de privacidad y protección de datos, pero también crea las bases de un sistema que hace prevalecer un enfoque económico al momento de regular los espacios digitales evolutivos y de constante innovación. Pero además de la regulación en materia de protección de datos personales, la UE también se ha preocupado por otras cuestiones alrededor de la era de nuevas tecnologías y la transformación tecnológica, centrándose en la regulación de tecnologías emergentes a partir del uso de sistemas de inteligencia artificial y del uso de los datos en contextos de Big Data.

Desde RGPD hasta el Reglamento de Inteligencia Artificial, el cual tuvo entrada en vigencia en el 2025, junto con otros paquetes normativos como el *Service Data Acta* (SDA) o *Markets Data Act* (MDA), y otros reglamentos como el Data Act o Reglamentos de Datos y leyes de Gobierno de Datos, se lidera el catálogo normativo en materia de transformación digital, economía digital y promoción del uso de nuevas tecnologías de manera consciente y con un enfoque garantista.

A partir de este enfoque, se evidencia la relevancia que adquieren los datos en los espacios digitales, especialmente aquellos utilizados en ámbitos industriales. Dichos datos requieren una protección adecuada y tutela frente al ejercicio de otros derechos, debido a que constituyen fuente esencial de alimentación para los sistemas de inteligencia artificial y/o tecnologías emergentes. Se debe considerar además que, el uso de los datos no personales no constituyen un riesgo inminente para las personas como lo es en el caso de los datos personales, pero además, es un activo indispensable que fomenta la innovación en las industrias, en la mejora de productos o servicios y, en general, aporta a la innovación tecnológica sin incidir negativamente en la esfera íntima de las personas o en la afectación de otros derechos personales.

En definitiva, la perspectiva europea reconoce que los datos no personales, además de ser fundamentales para el impulso tecnológico, poseen un valor económico estratégico que debe ser gestionado cuidadosamente. Bajo esta óptica, se busca no solo proteger su libre circulación, sino también fomentar su explotación conjunta y simultánea entre diversos agentes del mercado. Así, la regulación europea apuesta por un equilibrio entre incentivar el aprovechamiento de los datos como recurso de innovación y salvaguardar un mercado dinámico y plural, donde los beneficios del uso de los datos no personales puedan ser compartidos de manera más equitativa y sostenible entre todos los participantes del ecosistema digital. A continuación desarrollaremos a detalle algunos de los instrumentos normativos que la UE ha incorporado como regulación de la transformación digital en materia de datos no personales y su gobernanza.

1.1. Data Act (Reglamento (UE) 2023/2854)

El Data Act es un instrumento legal comunitario que se adopta en diciembre del 2023 con rango de reglamento, entra en vigor el 11 de enero del 2024 pero es aplicable desde el 12 de septiembre del 2025 y por tanto, de aplicación directa en los Estados Miembros. Su objetivo es determinar reglas, en base a un método de normas armonizadas, sobre el adecuado acceso a los datos que se generarán a partir de los dispositivos conectados, como el Internet de las Cosas (IoT) o servicios complementarios (como el mantenimiento).

Este reglamento busca además “democratizar” el acceso a los datos para que tanto los usuarios, terceros e incluso el Estado, puedan aprovechar los beneficios de la información que se genera, sin depender de los fabricantes o proveedores tecnológicos del IoT. Para Robles (2025), señala que este dispositivo normativo establece un régimen normativo complejos que empieza por la determinación de su ámbito de aplicación subjetiva y material, puesto que parte de la idea del reconocer explícitamente que la generación de los datos es el resultado de las acciones de dos o más agentes en un contexto donde no siempre existe equidad (p. 214).

No obstante, el Data Act ha sido objeto de intensos debates. Mientras algunos sectores lo consideran una oportunidad para democratizar y y permitir que un mayor número de instituciones públicas y privadas independientemente de su tamaño puedan beneficiarse de ello; para otros, como los grandes tecnológicos, han manifestado cierta preocupación. Entre estas destacan el posible impacto negativo sobre las ventaja competitivas, los costos adicionales asociados a la creación de sistemas de datos abiertos y el riesgo que representaría para la protección de los secretos comerciales y la obligación de compartir información considerada sensible a terceros.

El principal propósito del *Data Act* es crear reglas que establecen quién puede acceder y usar los datos generado en la UE en diferentes sectores económicos y ante la diversidad de agentes, con el objetivo de asegurar el justo equilibro en la distribución del valor de los datos y eliminar obstáculos que incidan en el correcto funcionamiento del mercado de los datos. Ello se logra no solo con la creación de condiciones de acceso sino también garantizando que los titulares de datos pongan a disposición en condiciones justas, razonables y no discriminatorias y de manera transparente.

Con ello, se busca estimular la competitividad del mercado, que abra las oportunidades a la innovación basado en *data driven* y que se haga a los datos más accesibles a los usuarios. Cabe resaltar que esta ley se enfoca principalmente en el sector industrial y establece límites cuando se tratan datos personales, por su especial contribución en la economía, es un requisito establecer medidas de protección alrededor de su importancia.

1.1.1 Objetivo y ámbito de aplicación

Kerber (2023) comenta el memorándum del Data Act, evidenciando que existen principalmente 4 objetivos que permiten identificar el propósito de la ley:

a) Empoderar a los consumidores y negocios para mantener un mayor control sobre el uso de los datos del IoT para beneficiarse de mejores productos o servicios o más económicos en el mercado secundario (a través de mayor competencia en el mercado).
b) Hacer los datos más accesibles a los negocios, especialmente para mayor innovación (desbloqueando los beneficios de los datos existentes).
c) Equidad en la asignación de valor de los datos entre los actores de la economía.
d) Preservar las iniciativas de inversión en nuevas formas de generar valor desde los datos.

Estos objetivos buscan equilibrar las diferencias que surgen en el ejercicio del poder sobre los datos, especialmente en función de la posición de mercado de quienes los controlan. De este modo, se pretende que los beneficios derivados del uso de los datos puedan ser aprovechados sin que ello represente un riesgo para otros actores del mercado ni limite los usos legítimos que puedan asignarse a dicha información.

El Data Act se aplica específicamente a determinados agentes involucrados en la generación de datos no personales, estableciendo reglas particulares en los entornos de relaciones *Business to Business* (B2B) y *Business to Consumer* (B2C) incluso Business to Government (B2G), dentro de un ámbito de aplicación delimitado y con características específicas. Los principales sujetos comprendidos en su alcance son los fabricantes de productos conectados, es decir, aquellos dispositivos que se encuentran vinculados a una red de internet, los proveedores de servicios complementarios establecidos en la Unión Europea, y los usuarios de dichos dispositivos conectados.

En este contexto, los denominados “titulares de datos” (*data holders*) son aquellos que ponen a disposición de los usuarios los datos generados en la Unión Europea. El reglamento busca empoderar tanto a consumidores como a empresas para que ejerzan un mayor control sobre los datos derivados del uso de sus dispositivos, tanto en relaciones B2B como B2C. Esta lógica parte del reconocimiento de que los datos representan la digitalización de las acciones o comportamientos de los usuarios; en consecuencia, se establece que estos deben tener acceso efectivo a los datos que contribuyen a generar, garantizando así un uso más justo y equilibrado de los recursos digitales.

El Data Act persigue el objetivo de impulsar el desarrollo de la economía digital europea mediante la maximización del uso de los datos generados en entornos industriales, particularmente orientado a la optimización de procesos productivos. A través de esta iniciativa, se busca fomentar la interoperabilidad entre los distintos actores y competidores del mercado, con el fin de fortalecer la competitividad sectorial y promover un ecosistema digital más dinámico e inclusivo.

La regulación del acceso y el intercambio de datos no se limitan únicamente a las relaciones entre agentes privados, sino que también contempla la posibilidad de compartir datos con entidades del sector público. Esta transferencia estará justificada en aquellos casos en que los datos resulten necesarios para el diseño y ejecución de políticas públicas o para la atención de situaciones de emergencia que involucren un interés público relevante.

Es importante destacar que, a pesar que regula tanto datos personales como no personales, en ningún caso busca alterar las reglas relativas a los datos personales, ni atribuye derechos de acceso o tratamiento sobre estos últimos más allá de lo dispuesto en la normativa aplicable del RGDP. El ámbito de aplicación de este reglamento, respecto de los datos no personales generados, se aplican a los datos “que no se modifican sustancialmente, es decir, los datos brutos, llamados también datos fuente o primarios” (Data Act, fundamento 15), estos incluyen los metadatos, lo que permite interpretar, utilizar y, eventualmente, hacer interoperables los datos no personales entre distintos productos y servicios.

1.1.2. Alcance de los datos no personales que se regulan

El reglamento se centra en los datos que se generan por el uso de dispositivos de Internet de las cosas o *Internet of Things* (en adelante “IoT”) que pueden ser, electrodomésticos, automóviles conectados, maquinaria industrial, dispositivos médicos, entre otros y los distingue en diferentes categorías que se desarrollan a continuación.

Los datos que se generan por el usuario son aquellos recopilados por los sensores o por un grupo de sensores integrados en los dispositivos IoT o los que tengan interacción a través de una interfaz, incluyendo aquellos que se generan cuando el dispositivo está en reposo o apagado, en su condición de venta, arrendamiento o cualquier otra modalidad contractual en la que se haya dispuesto el dispositivo al usuario y que este recopile sus datos en el uso. Para

dicha norma los datos que se recopilan a partir de un producto conectado están dentro del alcance, pero también aquellos generados durante la prestación de un servicio relacionado, por parte del mismo proveedor o de un tercero.

Así también, respecto del tipo de dato que incluye el reglamento, son exclusivamente respecto de los datos en bruto, a los que refiere como a puntos de datos que se generan de manera automática sin haber ejercido un nivel de procesamiento o tratamiento posterior. Pero también, como lo señala el Memorándum del Data Act, aplican a aquellos datos previo a tratamiento, por ejemplo, los datos recogidos para casos de uso más amplios y que podrían determinar una característica física o cualidad, tales como la temperatura, la presión, el nivel de líquido, posición, velocidad, etc.

Sobre este último punto, el Comité que elabora el memorándum, ha realizado una precisión sobre el término “datos pretratados” el cual no implica que para llevar a cabo la limpieza, filtración y la legibilidad de los datos que, al ser relacionados con otros, pueden dar información aún valiosa, implique una obligación necesaria para los fabricantes o proveedores de realizar una inversión altamente onerosa para generar este tipo de datos.

En consecuencia, se encuentran excluidos del ámbito de aplicación datos derivados o inferidos. Es decir, no se regulan los datos procesados a partir de los modelos que haya implementado el fabricante, en tanto la mayoría de estos son protegidos por derechos de propiedad intelectual o secretos industriales. Asimismo, en la medida que es tipo de información se deriva del resultado de una inversión adicional que permite generar valor y conocimiento sobre los datos, los algoritmos que se les aplica son de propiedad exclusiva y, por ende, no podrían serle aplicables las disposiciones de la ley.

Finalmente, las consideraciones que se adoptan al momento de determinar el alcance de la aplicación de la ley son importantes en tanto los productos conectados han sabido monetizar con los datos obtenidos de sus usuarios, pero siempre han tenido un extremo control sobre estos a pesar de que no haya existido atribución legal de derechos sobre ellos y aún usarlos y explotarlos, y esto se debe a que se han adoptado medidas técnicas o diseños que no permiten a los usuarios a acceder a estos, bien porque no son accesibles o legibles o porque no se ha tomado importancia hasta la fecha, la importancia del dato.

Ahora bien, para evitar que se ejerzan efectos de bloqueo no solo por el diseño que tienen los productos conectados o servicios relacionados, la UE considera conveniente la regulación del flujo de los datos y a su vez, considera necesaria el establecimiento de un marco regulatorio que otorgue derechos que puedan permitir el uso y el acceso a los datos no personales de manera equilibrada, persiguiendo los fines ya establecidos en el punto de los objetivos del reglamento.

1.1.3. Derechos otorgados

El mecanismo que ha sido adoptado por el mencionado reglamento a fin de alcanzar los objetivos es el establecimiento de derechos de acceso y compartir datos generados por sus dispositivos IoT que no sean renunciables, tal como se establece en los artículos 4 y 5 del Reglamento UE 2023/2854. Estos derechos se le otorgan tanto a los usuarios, como a los terceros intervinientes e interesados en el acceso a los datos generados por los dispositivos conectados.

Para ello se ha determinado qué actores tienen derechos específicos, por ejemplo, en el caso de los usuarios finales, en el marco de las relaciones B2B (también aplican para B2C y B2G pero dichas relaciones exceden el objeto de estudio del presente trabajo).

1.1.3.1. Derecho de acceso

El Data Act establece un derecho de acceso a los datos generados por dispositivos y servicios conectados, otorgado a diversos actores con el objetivo de evitar la concentración del control y posibles abusos por parte de los fabricantes de productos conectados y los proveedores de servicios relacionados.

De acuerdo con los artículos 3 a 5 del Reglamento (UE) 2023/2854, los usuarios finales, ya sean personas naturales o jurídicas, en contextos tanto B2C como B2B, tienen derecho a acceder, de forma gratuita, a los datos brutos generados por los dispositivos que utilizan, incluidos los metadatos necesarios para interpretar las condiciones bajo las cuales se han recopilado los datos. Esta previsión normativa amplía, en cierta medida, el principio de autodeterminación informativa, en tanto permite a los usuarios utilizar dichos datos para los fines que estimen convenientes.

"***Artículo 6: Obligaciones de terceros que reciben datos a petición del usuario***

> *"Un tercero **tratará los datos que se pongan a su disposición** con arreglo al artículo 5 únicamente para la finalidad y en las condiciones **acordados con el usuario y respetando el Derecho de la Unión y nacional en materia de protección de datos personales**, incluidos los derechos del interesado en lo que respecta a los datos personales. El tercero suprimirá los datos cuando ya no sean necesarios para la finalidad acordada, a menos que acuerde otra cosa con el usuario en relación con los datos no personales."* (énfasis agregado).

El límite de los "datos en bruto" es importante, estos refieren a aquellos datos que se generan a partir de los usos de un producto o servicio conectado, sin que hayan sido sometidos a procesos de tratamiento o análisis, tal como señala la misma ley:

> "*El ámbito de aplicación del presente Reglamento incluye los datos que no se modifican sustancialmente, es decir, los datos brutos, también conocidos como datos fuente o datos primarios, que se refieren a puntos de datos que se generan automáticamente sin ninguna forma de tratamiento posterior, así como los datos que, previamente a su tratamiento y análisis, han sido objeto de un tratamiento destinado a hacerlos comprensibles y que puedan ser utilizados. Tales datos incluyen los datos recogidos a partir de un único sensor o de un grupo conectado de sensores con el fin de hacer comprensibles los datos recogidos para casos de uso más amplios, determinando una cantidad o una calidad física o la modificación de una cantidad física, como la temperatura, la presión, el caudal, el audio, el valor del pH, el nivel líquido, la posición, la aceleración o la velocidad*"

El reglamento también reconoce el derecho de los usuarios a designar terceros para acceder a los datos en su nombre. Esta facultad es especialmente relevante cuando los usuarios desean contratar servicios adicionales que no provienen del proveedor inicial del producto o servicio complementario. En estos casos, el acceso de terceros debe garantizarse en condiciones de equidad, siguiendo el principio de "FRAND", con el fin de evitar prácticas discriminatorias o abusivas en el acceso y reutilización de los datos.

El principio FRAND, acrónimo de *Fair, Reasonable and Non-Discriminatory* (justo, razonable y no discriminatorio) constituye un estándar ampliamente reconocido en el derecho de la competencia y también aplicable a la regulación de tecnologías, especialmente en contextos de licenciamiento de patentes esenciales para estándares técnicos. Su finalidad es asegurar que

los titulares de derechos sobre tecnologías o recursos indispensables no abusen de su posición de poder para restringir el acceso de otros actores, facilitando así un entorno de mercado más equitativo y competitivo.

Respecto a las obligaciones de los fabricantes, vendedores, arrendadores o proveedores de productos conectados, el artículo 3.2 y 3.3 del reglamento establece que estos deben informar de manera transparente a los usuarios acerca de la recopilación de datos, ya sea directa o indirectamente, a través de los dispositivos. Esta obligación se inscribe en el principio de transparencia que rige el tratamiento de los datos, garantizando que los usuarios sean plenamente conscientes del flujo de información generada por el uso de los productos.

El acceso a los datos puede configurarse de dos maneras:

- Acceso directo: Los usuarios pueden acceder de manera inmediata a los datos mediante interfaces técnicas habilitadas, en *streaming* o a través de versiones descargables, sin necesidad de presentar solicitudes previas. Algunos ejemplos incluyen la creación de plataformas o cuentas de usuario donde se otorgan opciones para visualizar o descargar los datos generados por los dispositivos conectados.
- Acceso indirecto: En ciertos casos, el acceso a los datos requiere una solicitud previa y la aprobación de parte del titular de los datos o del proveedor del servicio. Esta modalidad se da cuando los datos están almacenados en ubicaciones específicas que no permiten el acceso inmediato y automático, por lo que es necesario pasar por un flujo de autorizaciones administrativas.

Ahora bien, bajo este contexto, algunos autores han realizado algunas apreciaciones sobre el ejercicio de este derecho. Para Kerber y Schweitzer (citado en Kerber, 2023), aunque se promueve el acceso, se prioriza la capacidad de los fabricantes para explotar o monetizar con los datos que recopilan en sus sistemas y, en consecuencia, prevalece la posición competitiva de algunos bajo el reconocimiento del control de facto de los datos respecto de los fabricantes de dispositivos AIoT.

De otro lado, Scweitzer señala que se debe tener un especial cuidado y monitoreo sobre los efectos positivos y negativos de los costos de generar datos porque los estos pueden generarse tanto de manera automática como no automática y, en consecuencia, generar un efecto adverso

a la promoción de la compartición de los datos entre los diferentes actores (citado en Kerber, 2023).

Finalmente, Rubinfeld (2024) indica que las limitaciones que se han impuesto en el reglamento respecto del uso de datos para fines que generen algún tipo de competencia entre los actores podrían eventualmente reducir el impacto positivo de la apertura de los datos y de algún modo frenar la innovación, es decir que la capacidad de monetizar también podría estar asociada a generar barreras de entrada si los datos son controlados por unos pocos actores que tienen una posición prevalente y, por otro lado, si no hay un marco adecuado de compensación por la estructuración y procesamiento de los datos, entonces se puede reducir los incentivos.

Adicionalmente, el Data Act contempla un acceso especial para las entidades públicas en situaciones excepcionales. En casos como emergencias sanitarias, desastres naturales o eventos de interés público significativo, las autoridades podrán solicitar el acceso a datos no personales en poder de actores privados. Esta facultad busca priorizar el interés público frente a situaciones de urgencia, aunque su ejercicio está sujeto a condiciones estrictas y limitaciones específicas.

Desde el plano doctrinal, autores como Martens (citado en Kerber, 2023) consideran que el derecho de acceso regulado en el Data Act constituye un mecanismo que incentiva la competencia en los mercados digitales, permitiendo la entrada de nuevas empresas innovadoras que puedan desarrollar servicios basados en los datos previamente recopilados por los fabricantes de productos AIoT. No obstante, en la práctica, los fabricantes han manifestado preocupaciones recurrentes, argumentando que el acceso generalizado podría poner en riesgo sus secretos comerciales y comprometer la seguridad de sus sistemas.

Aunque el Data Act introduce mecanismos para proteger los secretos comerciales en el marco del acceso a los datos, persisten desafíos relevantes en la práctica.
El reglamento establece que el acceso a los datos no debe comprometer la confidencialidad de la información sensible ni poner en riesgo la seguridad de los sistemas; sin embargo, la distinción entre datos brutos y datos derivados o estratégicos no siempre es clara y no se han establecido disposiciones que especifiquen la materia, sobre todo en entornos tecnológicos complejos como el AIoT, donde incluso los datos pueden revelar patrones de comportamiento críticos de los dispositivos.

Además, existe el riesgo de que las obligaciones de acceso impuestas bajo principios de equidad puedan ser explotadas estratégicamente por competidores para obtener información técnica valiosa, afectando así la ventaja competitiva de los fabricantes o proveedores originales. En consecuencia, si bien el Data Act introduce salvaguardias importantes, su eficacia dependerá en gran medida de cómo se interpreten y apliquen en la práctica conceptos como el secreto comercial, la proporcionalidad en el acceso, y los mecanismos de resolución de conflictos entre las partes involucradas.

Ahora bien, para autores como Martens (citado en Kerber, 2023), ambos coinciden en que el derecho al acceso que se concede en el reglamento son un incentivo para la competencia en los mercados digitales, dando lugar a que nuevas empresas innovadoras, puedan desarrollar servicios basados en los datos que han sido recopilado previamente por los fabricantes de AIoT. No obstante, se ha determinado en la práctica que los fabricantes constantemente argumentan que sus secretos comerciales se exponen a diferentes riesgos y también la seguridad de los sistemas.

1.1.3.2. Derecho de uso

El derecho de uso hace referencia a la facultad de procesar los datos no personales generados por productos o servicios conectados, con la finalidad de destinarlos a propósitos específicos como análisis, entrenamiento de algoritmos, optimización operativa, o desarrollo de nuevos productos. A diferencia del derecho de acceso, que hace posible la obtención técnica de los datos, el derecho de uso se orienta hacia su explotación funcional, siendo esta el motivo por el cual justifica el interés por acceder a los datos en primer lugar.

En el marco del Data Act (UE) 2023/2854, este derecho no se configura como una prerrogativa absoluta, sino que está supeditado a acuerdos contractuales entre las partes involucradas, especialmente entre el usuario del dispositivo y el proveedor tecnológico (*data holder*). En ese sentido, el proveedor o fabricante del dispositivo solo puede hacer uso de los datos si existe una base contractual habilitante suscrita con el usuario (art. 4.13), quien se reconoce como actor central en la generación de valor a través del uso legítimo de la tecnología.

Jurídicamente el derecho de uso puede concebirse como una extensión del derecho de acceso habilitada mediante contrato entre las partes. Asimismo, se instaura como una respuesta

normativa para corregir la situación de control exclusivo de facto que ostentan los fabricantes de dispositivos IoT sobre los datos no personales generados.

Como explica Specht-Riemenschneider (2022), este control no proviene de un derecho legal formal, sino de la arquitectura técnica del dispositivo, que permite a los fabricantes excluir a otros, incluidos los propios usuarios, del acceso, uso y monetización de los datos. No obstante, el Data Act plantea un cambio al establecer, en sus artículos 4(13) y 4(14), que los *data holders* ya no pueden utilizar, compartir o extraer valor de los datos sin el consentimiento del usuario.

Este giro normativo implica una reasignación del conjunto de facultades para empoderar a los usuarios legítimos de los dispositivos, quienes pasan a ocupar el centro del enfoque de la gobernanza de datos no personales. En ese sentido, el derecho de uso reconocido en el Data Act deja de estar condicionado por la posición técnica de control y pasa a depender de la voluntad y legitimación del usuario, reforzando una idea de una redistribución estructural del poder informacional en entornos industriales conectados.

El reconocimiento de un derecho de uso condicionado permite fomentar un modelo de gobernanza de los datos que promueva la eficiencia sin comprometer la competencia ni el reparto justo del valor generado. En entornos como el sector minero, esta regulación garantiza que los proveedores tecnológicos puedan seguir desarrollando soluciones avanzadas a partir de los datos operativos, pero sin apropiarse unilateralmente de la información ni impedir que los usuarios o terceros autorizados también la utilicen.

Como han destacado Specht-Riemenschneider (2023) y Graef y Husovec (2022), este enfoque funcionalista genera un entorno más equilibrado donde los datos pueden circular, reutilizarse y potenciarse en distintos niveles, respetando siempre la voluntad y el interés de quienes los generan. De este modo, el derecho de uso se articula como una herramienta de gobernanza técnica y económica, y no como una manifestación de propiedad exclusiva.

Aunque el *Data Act* representa un avance significativo en el reequilibrio del control sobre los datos no personales generados por dispositivos inteligentes, la solución normativa que se propone al pretender centralizar la titularidad funcional del acceso, uso y compartición en el usuario del dispositivo, no está exenta de tensiones. Si bien esta redistribución busca corregir el control de facto ejercido por los fabricantes, puede generar un nuevo desequilibrio al otorgar al

usuario un poder de decisión que podría usarse en detrimento de otros actores legítimamente interesados.

Desde una perspectiva crítica, autores como Duch-Brown, Martens y Mueller-Langer (2017) advierten que el control excesivamente concentrado en un único actor puede replicar, bajo otro esquema, los mismos problemas que intenta resolver: restricciones a la reutilización de datos, limitación de flujos informacionales y fricción en la innovación. En sectores industriales complejos, como el minero, un modelo centrado exclusivamente en la voluntad del usuario podría generar bloqueos contractuales o estratégicos al uso compartido de datos que son técnicamente generados en entornos interdependientes.

Asimismo, Diker Vanberg and Ünver han advertido que, aún en el caso de protección de datos personales, si bien el empoderamiento del usuario es deseable, la excesiva dependencia de su consentimiento individual puede limitar la fluidez de los ecosistemas de datos**,** (citado en Drexl, 2018, p. 54) especialmente en entornos donde los usuarios carecen de incentivos o capacidad técnica para gestionar adecuadamente el acceso o definir los términos de uso. Esta posición cobra fuerza en contextos B2B con estructuras técnicas complejas, donde la función de coordinación y gobernanza de datos no puede delegarse completamente en decisiones individuales sin riesgo de fragmentación.

En ese sentido, a pesar que la solución del *Data Act* pretenda corregir la asimetría existente a favor del fabricante, esta centralización en el usuario no debería entenderse como un punto de llegada, sino como un punto de partida para explorar modelos más balanceados, como los *data stewardship models* (modelos fiduciarios), *data commons (*gobernanza colectiva de los datos) o *data trusts (*en donde un tercero administrador fiduciario gestiona los datos en nombre de un grupo de beneficiario) que distribuyen los derechos de uso de manera proporcional entre actores, atendiendo a sus roles, aportes y riesgos (Mills, 2019). Así, se podría evitar que la reconfiguración de poder sobre la información derive simplemente en una "asignación de mayor fuerza a los usuarios", en lugar de habilitar mecanismos verdaderamente cooperativps y orientados al beneficio sectorial o social.

A propósito del “*data stewardship*” o la idea de un fideicomiso de datos, son entidades que gestionan los datos en nombre de los contribuyentes de datos y otros beneficiarios para facilitar el acceso justo y no discriminatorio y, al mismo tiempo, protegen los intereses de los actores que contribuyen a generarlos, lo cual es una alternativa de solución innovadora para gestionar estos

derechos de uso y acceso (Eckardt y Kerber, 2024). Los autores también sugieren abiertamente esta propuesta como una herramienta efectiva para aliviar las limitaciones de los derechos de acceso y uso individual que ha implementado el *Data Act* y, al mismo tiempo, pueden abordar cuestiones de monopolios y distribuir beneficios.

En la aplicación del sector minero, el fideicomiso podría ser un comité de representantes de empresas mineras, proveedores y otras partes interesadas, incluyendo la participación del Estado. Las decisiones sobre acceso de ciertos datos se tomarían de manera conjunta y también modos de resolución de conflictos. Las empresas mineras acceden a sus datos para buscar sostenibilidad o mejorar sus operaciones, los proveedores o fabricantes pueden utilizar los datos para mejorar sus dispositivos AIoT o crear nuevos productos y, terceros como investigadores u otras empresas de análisis de datos podrían acceder bajo condiciones específicas. De este modo se fomenta la colaboración entre agentes económicos y la creación de datos abiertos, confiables y reales.

Abordando este derecho desde una perspectiva económica, la implementación busca equilibrar intereses de los múltiples actores intervinientes en la cadena de valor de los datos. Por un lado, los usuarios, requieren acceder y utilizar los datos para mejorar la eficiencia operativa, optimizar procesos extractivos, reducir costos o fortalecer la seguridad. Por otro, los proveedores tecnológicos cuentan con un legítimo interés en recuperar la inversión realizada en el desarrollo de dispositivos inteligentes y modelos de IA, y aspiran a obtener retornos mediante la explotación de los datos generados por sus tecnologías (Eckardt & Kerber, 2024). La normativa evita reconocer automáticamente un derecho de uso inherente al control técnico, y obliga a direccionar dicho uso a través de la negociación contractual, lo que promueve una asignación más justa de los beneficios derivados del uso de los datos.

La delimitación del derecho de uso requiere establecer condiciones claras, tanto desde el diseño contractual como desde la política pública. Es fundamental definir los fines legítimos y específicos para los cuales los datos pueden ser usados, evitar ambigüedades legales que permitan usos indeseados y asegurar que no se restrinja injustificadamente la reutilización de datos por otros actores autorizados.

Particularmente en el sector minero, donde múltiples proveedores ofrecen soluciones a una misma unidad operativa, la disputa entre intereses de los actores puede generar tensiones alrededor del uso de datos. Es importante que se puedan abordar los legítimos intereses de las

partes que intervienen. Por un lado, los usuarios de las minas, quienes requieren acceso a los datos para optimizar operaciones, garantizar seguridad y buscar eficiencia y, por otro lado, es posible que busquen acceso y uso sin restricción alguna por parte de los fabricantes. Esto los legitima a compartir los datos a terceros proveedores competidores, sin embargo, se pueden establecer límites para evitar prácticas anticompetitivas.

Los proveedores tecnológicos buscan recuperar los costos en los que han incurrido en el desarrollo del dispositivo inteligente y buscan el retorno económico mediante la explotación de los datos que se generan en el AIoT, ofreciendo soluciones sólidas, eficientes y que les permita obtener ganancias. En ocasiones, con el fin de beneficiarse de manera absoluta, son quienes mantienen un interés por limitar a nivel técnico el uso de los datos no personales por terceros, a fin de proteger su posición en el mercado.

Frente a ello, es necesario fomentar marcos de gobernanza que respeten tanto la autonomía del usuario como el interés económico legítimo de los proveedores, permitiendo compartir datos con terceros bajo condiciones de equilibrio competitivo. Esto exige mecanismos contractuales bien definidos, pero también estándares sectoriales que eviten la fragmentación normativa y promuevan prácticas equitativas.

Además, la normativa especializada debe definir fines específicos y fines legítimos, de tal modo que permitan equilibrar los intereses entre las partes, pero limitar las prácticas de beneficio unilateral o la competencia desleal. Incluso con la intervención del Estado, quien puede intervenir no solo para aprovechar también de los datos a partir de un interés público (para salvaguardar cuestiones sobre el medio ambiente o la protección de bienes públicos, la prestación de un servicio público, etc), sino también con regulación que garantice prevención del abuso de poder, fomento de la competencia, incentivos de colaboración como *data trust* que gestionan accesos a datos sectoriales.

El Estado cumple un rol clave en la regulación del derecho de uso, tanto desde su dimensión garantista como desde su función promotora del interés público. En primer lugar, debe establecer límites normativos frente al uso abusivo o unilateral de los datos que afecten la competencia, la privacidad o el acceso equitativo a la innovación. En segundo lugar, puede facilitar modelos de gobernanza colaborativa mediante instrumentos como los *data trusts*, entidades fiduciarias que gestionan el acceso y uso de datos en sectores estratégicos, promoviendo esquemas de cooperación entre actores públicos y privados (Mills, 2019).

En conclusión, el derecho de uso constituye una herramienta estratégica para equilibrar el valor informacional generado por tecnologías AIoT en sectores productivos como el minero. Su ejercicio exige acuerdos claros, estándares técnicos y mecanismos de gobernanza que permitan compatibilizar los intereses de los usuarios, los proveedores tecnológicos y la sociedad en su conjunto. Frente a la complejidad de las relaciones B2B y la sensibilidad económica del uso de datos, resulta un factor clave para adoptar un enfoque regulatorio que combine distribución justa a través de la negociación y marcos institucionales flexibles, a fin de evitar desequilibrios, promover la innovación y garantizar un uso ético y productivo de los datos no personales.

1.1.3.3. Derecho del usuario a compartir con terceros

Este es un derecho que proporciona un grado de importancia sobre el esfuerzo de la UE por regular este tipo de datos, puesto que su principal objetivo se centra en el compartir y hacer más accesibles los datos. Esta norma, al ser diseñada para facilitar el intercambio de datos entre diferentes proveedores y actores, se requiere la adopción de disposiciones que permitan la interoperabilidad y reduzca la dependencia existente con los usuarios de un solo proveedor.

Por ello, el reglamento confiere a los usuarios la capacidad de transferir sus datos a terceros en base a ciertas condiciones de integridad y disponibilidad de estos, tal como se desarrolla en el artículo 9 del citado reglamento. Los proveedores de servicios en la nube, sea de almacenamiento o procesamiento, tendrán que facilitar la portabilidad de los datos, respetando la preferencia del usuario, evitando la imposición de cualquier barrera contractual o técnica para que el usuario cambie de proveedor, tal como lo establece el artículo 23 del Data Act:

> *"Los proveedores de servicios de tratamiento de datos adoptarán las medidas previstas en los artículos 25, 26, 27, 29 y 30* ***para permitir a los clientes cambiar a un servicio de tratamiento de datos que cubra el mismo tipo de servicio****, que sea prestado por un* ***proveedor diferente*** *de servicios de tratamiento de datos o a una infraestructura de TIC local o, cuando proceda, usar varios proveedores de servicios de tratamiento de datos simultáneamente. […] los proveedores de servicios de tratamiento de datos* ***eliminaran y no pondrán obstáculos pre comercial, comercial, técnico, contractual y organizativo*** *que disuada a los clientes:*
>
> *(…)*
>
> *d) de conformidad con el artículo 24,* ***alcanzar la equivalencia funcional en el uso del nuevo servicio de tratamiento de datos en el entorno de las TIC*** *de un*

> *proveedor o proveedores diferentes de servicios de tratamiento de datos que incluyan el mismo tipo de servicio;*
> *e)* ***la desagregación, cuando sea técnicamente viable****, de los servicios de tratamiento de datos a que se refiere el artículo 30, apartado 1, de otros servicios de tratamiento de datos prestados por el proveedor de servicios de tratamiento de datos.* (Énfasis añadido)

Ahora bien, un aspecto relevante en el análisis del Reglamento de Datos es comprender si cabe preguntarse si el derecho de los usuarios a compartir datos no personales con terceros replica las disposiciones del derecho a la portabilidad de datos personales, o si responde a una lógica distinta. Aunque ambos derechos comparten ciertos fundamentos, como el empoderamiento del usuario, el Reglamento de Datos no concibe el derecho de compartición como una mera extensión o réplica del derecho de portabilidad regulado en el Reglamento General de Protección de Datos (RGPD). En su lugar, adapta ciertos matices, partiendo de la premisa de que los datos no personales poseen una naturaleza diferente, especialmente en contextos donde son generados a través de dispositivos conectados.

La portabilidad es una facultad de los usuarios que no es exclusiva de los sistemas de AIoT o en relación al uso de los datos no personales en el sector tecnológico. Es una facultad que ha sido conferida a los usuarios por el reglamento para poder adquirir mejores condiciones ofrecidas por otro proveedor en base a la ejecución de un servicio y que son necesarios para el despliegue del servicio mismo (Díaz, 2023). Esta facultad ha sido implementada tanto en el sector bancario como en telecomunicaciones, y ha sido de cierta forma una imposición que se ha generado por las entidades estatales en la búsqueda por crear mejores condiciones entre competidores.

En efecto, el artículo 5 del Data Act establece que los usuarios pueden permitir a terceros acceder a los datos co-generados por sus dispositivos, reforzando así la apertura de mercados y reduciendo riesgos de concentración de datos. La portabilidad, en este marco, se limita a asegurar que los datos puedan ser transmitidos en un formato estructurado, de uso común y lectura mecánica, evitando que existan barreras técnicas que impidan su transferencia (Eckardt & Kerber, 2024). En consecuencia, mientras la portabilidad busca permitir la migración de los datos y prevenir los efectos *lock-in*, el derecho de compartición trasciende a la promoción de ecosistemas de competencia abierta, donde múltiples actores intervienen y ofrecen servicios sobre los mismos datos.

Por ejemplo, si los datos pueden ser almacenados tanto por servidores en la nube como en servidores locales. En el caso de los servidores en la nube que constituyen como tal un servicio, la portabilidad permite que los usuarios, cuenten con la posibilidad de contratar entre diferentes opciones de almacenamiento en la nube y por ende, para hacerlo efectivo, es necesario que se hagan portables los datos sin tener que perder su información. Sin embargo, el deber de compartir los datos garantiza que los usuarios puedan permitir que otras empresas accedan a los datos de sus dispositivos de AIoT sin depender del fabricante o de los servicios que este provea. De este modo no se ven perjudicados por la imposición de barreras, contractuales o técnicas, para contar con otros proveedores con nuevos o mejores productos.

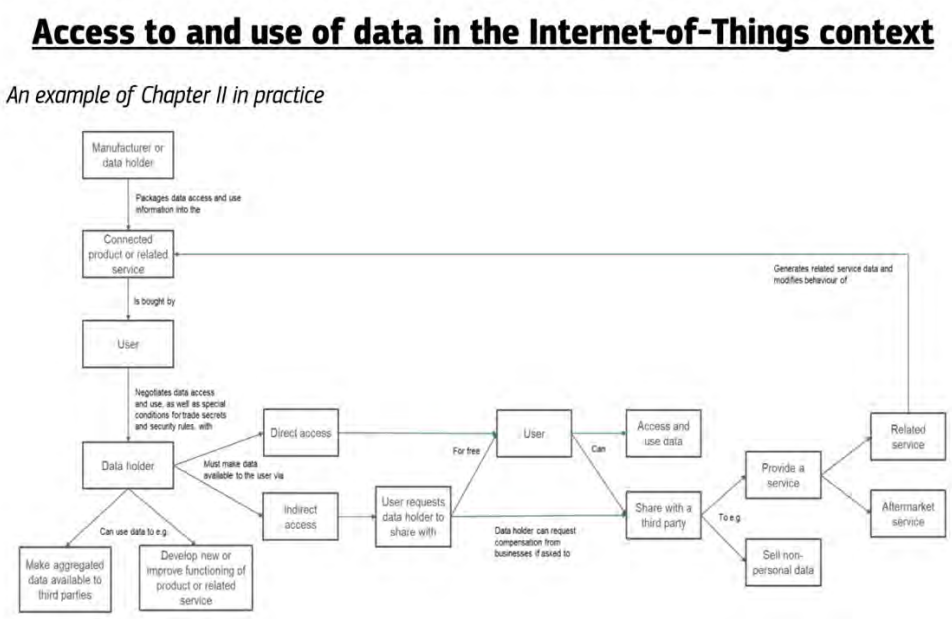
En consecuencia, si bien ambos conceptos buscan dar mayor poder a los usuarios sobre ciertos datos que poseen y se generan, el enfoque y su alcance no es el mismo. Los datos sobre los cuales se ejerce la portabilidad refieren únicamente a los datos propios de empresa y, por su parte, el derecho de compartir los datos con terceros comprende, por el contrario, los datos que son generados por los dispositivos de AIoT y compartidos con terceros a solicitud del usuario.

Desde esta perspectiva, estimo que la portabilidad no debe configurarse como un derecho autónomo en el tratamiento de datos no personales, en tanto el valor económico y jurídico de estos difiere sustancialmente del atribuido a los datos personales. Antes bien, debe entenderse como una prerrogativa instrumental del usuario, orientada a garantizar que, al ejercer su derecho de compartir datos con terceros, se implementen las condiciones técnicas necesarias que faciliten la transferencia efectiva, evitando que surjan barreras técnicas que obstaculicen la interoperabilidad entre distintos proveedores o restrinjan la competencia en el mercado.

Ahora bien, el concepto de portabilidad ha sido introducido como un derecho en el Reglamento General de Protección de Datos el cual otorga la potestad al titular de datos de recibir los datos que le concierne y que el responsable del tratamiento pueda facilitarle un formato estructurado, de uso común y lectura mecánica (art. 20 de la RGPD), dicho en otros términos, refiere a un formato legible y posible de transmitir a otro responsable de tratamiento.

En el ámbito de los datos no personales, el Data Act ha incorporado el concepto de portabilidad tomando como referencia las definiciones establecidas en el Reglamento General de Protección de Datos (RGPD). Sin embargo, no lo configura como un derecho autónomo, sino como un requisito funcional destinado a garantizar la efectividad del derecho de compartición y a favorecer

la interoperabilidad entre servicios. Esta incorporación también forma parte de un esfuerzo por mantener coherencia con las disposiciones aplicables a los datos personales y con la noción de que tanto las personas naturales como las jurídicas, en calidad de usuarios, detentan un cierto grado de poder sobre los datos que generan o controlan.



Nota. Adaptado de *Access to and use of data in the Internet-of-Things context*, de Comisión Europea, 2024, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act.

Este diagrama es útil para mostrar cuál es el flujo de relaciones entre los distintos actores involucrados en el ecosistema de datos generados por productos conectados. Muestra cómo el usuario adquiere un rol activo al obtener acceso gratuito a los datos y al tener la facultad de compartirlos con terceros. Asimismo, se visualizan las obligaciones del titular de los datos (fabricante o proveedor), así como los posibles usos posteriores de la información, tanto por parte del usuario como del titular, conforme a lo previsto en el Data Act.

1.1.4. Críticas

Rubinfeld menciona que el enfoque regulador europeo tiende a imponer reglas sobre el acceso a datos, pero no siempre garantiza que estas reglas se apliquen de manera efectiva para fomentar la competencia. En este sentido, advierte sobre el riesgo de que los datos se mantienen en "silos" dentro de las empresas que los generan, sin ser compartidos de manera significativa para generar valor en el ecosistema digital (2024). Es decir, el autor refiere a una práctica común en el entorno digital e industrial en la que las empresas que generan datos (por ejemplo, a través

de dispositivos conectados o servicios digitales) los almacenan y gestionan internamente sin compartirlos con otros actores del ecosistema, como usuarios, proveedores de servicios o terceros innovadores.

Si bien el Data Act es una norma que concede a los datos un nivel de disponibilidad casi inmediata, y dicha disponibilidad está sujeta a una prohibición de uso por una posible afectación a la seguridad del producto, violación de confidencialidad o desarrollar de productos directamente competitivos con los fabricantes originales, de algún modo, los efectos prácticos para favorecer la competencia, en la práctica, se vuelve un imposible.

Por un lado, se han formulado críticas en torno al poder residual que conservarían los fabricantes bajo el Data Act, dado que la regulación se centra primordialmente en fortalecer los derechos de los usuarios. Aunque la norma impone la obligación de compartir los datos generados, los fabricantes mantienen cierto control sobre los mecanismos de monetización, lo que, según algunos, podría seguir constituyendo una barrera para la entrada de nuevos actores en el mercado.

Sin embargo, discrepo de esta visión. Considero que el esquema previsto no solo busca equilibrar el valor potencial de los datos al facilitar su acceso y reutilización por parte de terceros, sino también reconocer un legítimo retorno propio de los fabricantes en razón de las inversiones realizadas en el desarrollo (tiempo, capital e intelecto) y despliegue de dispositivos conectados en un inicio (entrada en el mercado bajo un modelo de negocio). La posibilidad de obtener ingresos derivados del uso posterior de los datos no debe verse como un privilegio exclusivo, sino como un incentivo necesario para estimular la innovación tecnológica y la expansión del ecosistema digital.

Por otro lado, se ha manifestado que los costos de implementación, sobre todo para las pequeñas y medianas empresas, enfrentan constantes dificultades técnicas y económicas para cumplir este tipo de regulación. Y, finalmente, la falta de interoperabilidad efectiva no se evidencia porque, si bien se exige portabilidad de los datos, no se han establecido estándares que garanticen uniformidad al momento de la transferencia.

El Data Act también enfrenta dificultades para definir los datos personales y los no personales que sean útil en la medida que técnicamente lo sea también. En muchos casos, se puede dar

que los datos contienen información que indirectamente identifica a las personas o datos no personales que, con un uso sistematizado, es posible identificar a una persona en específico y su diferenciación, una vez generado el resultado, no siempre es clara, lo que genera un vacío regulatorio. Y, de otro lado, aunque el reglamento prohíbe cláusulas abusivas, no se han definido mecanismo que pueda monitorear y buscar la aplicación efectiva de la norma.

Un artículo de Kerber (2024), apunta a realizar una crítica a la aplicación real del reglamento, identificando ciertos obstáculos o conflictos que se podrían generar. En primer lugar, se podrían crear barreras y costos a causa de reglas específicas en el uso de los derechos de los usuarios como la obligación de disponer los datos sin dilación y bajo condiciones específicas que se hayan sido negociadas previamente en el contrato de licencia. Los márgenes de negociación podrían verse limitados o extralimitarse ante la ausencia de acuerdos específicos técnicos o de definición de alcances.

Por otro lado, al momento de determinar los modelos estandarizados para generar interoperabilidad y, en consecuencia, hacer in situ el derecho de acceso, se pueden ver involucrados problemas respecto a la protección de los secretos comerciales, puesto que no se pueden determinar los riesgos de manera ex ante y porque no se puede determinar del todo, qué tipo de información contiene secretos comerciales (Kerber, 2024). En contextos como los tecnológicos donde los datos representan un insumo crucial, el recelo de los competidores con su información se convierte en un comportamiento habitual y una cultura que el Reglamento de Datos pretende disuadir.

Leistner y Antoine dedican el capítulo II a precisar el equilibrio entre derechos de acceso y protección de la propiedad intelectual y los secretos empresariales. Señalan que el Data Act ya incorpora salvaguardias generales para los secretos comerciales (art. 4.3 y 5.8), pero proponen afinar esta técnica distinguiendo dos categorías:

- Información sensible de mercado, que abarca datos estratégicos sobre parámetros de competencia;
- Know-how genérico, que incluye simples conocimientos técnicos o creativos. (p. 342)

Esta distinción permitiría calibrar con mayor precisión sobre qué datos exigir en un régimen FRAND y qué compensaciones corresponden, sin desincentivar la innovación. Además, recomiendan que los contratos tipo de intercambio de datos incluyan cláusulas no obligatorias

para licencias de secretos, de modo tal que las partes cuenten con plantillas claras y equilibradas que reduzcan la incertidumbre jurídica en las redes de cooperación de datos (2022).

Dada esta amplitud y la introducción de conceptos jurídicos novedosos, los autores advierten que cualquier esfuerzo de concreción normativa que defina criterios de proporcionalidad, parámetros de compensación sobre los datos no personales se dará inevitablemente en base a la práctica jurisprudencial y no de reglamentos secundarios o líneas directrices dispares. Por ello, defiende la tesis de confiar prioritariamente en la litigación privada, donde los tribunales de derecho civil irán precisando, caso a caso, el alcance y los límites de los derechos y obligaciones previstos en el Data Act.

Incluso proponen un mecanismo que surge por la crítica de una posible intervención superpuesta de autoridades estatales como de agencias de Competencia, autoridades de Protección de Datos u órganos nacionales de Supervisión del Data Act, que podrían dictar resoluciones contradictorias y generar inseguridad jurídica, por lo cual, consideran que la intervención pública sea opcional y simplificada: un mecanismo de “ventanilla única europea” o incluso una meta-autoridad centralizada que coordine los recursos sancionadores y las consultas, garantizando homogeneidad y evitando duplicidades

La regulación de los datos no personales debe promover su disponibilidad, accesibilidad y libre circulación a nivel transfronterizo, porque representa un bajo riesgo para los derechos fundamentales y posee un potencial valor para impulsar el crecimiento económico, la innovación tecnológica y la solución de desafíos globales (International Chamber of Commerce - ICC, 2023).

Según la ICC (2023), toda restricción sobre estos datos debe ser excepcional, fundada en una evaluación de riesgos concreta y basada en evidencia técnica, evitando enfoques genéricos que puedan limitar el desarrollo de nuevas tecnologías o incrementar los costos de cumplimiento para las organizaciones. Además, es necesario adoptar una aproximación diferenciada que reconozca la diversidad de los datos no personales y rechace su tratamiento como una categoría homogénea, a fin de no restringir injustificadamente su aprovechamiento social y económico.

La misma, señala que es necesario priorizar la interoperabilidad y el establecimiento de estándares comunes en torno a la estructura, calidad y gestión de los datos, como medidas esenciales para evitar la fragmentación normativa. También se debe velar por incentivar el intercambio voluntario de datos no personales, protegiendo secretos comerciales y garantizando

libertad contractual, sin imponer obligaciones desproporcionadas o imprecisas. Para ello, la cooperación internacional en base a normas con estándares de interoperabilidad es fundamental para maximizar los beneficios de los datos no personales, en favor del desarrollo de la innovación y la equidad digital (ICC, 2023).

Consideramos que el Data Act es un instrumento que da un marco sólido para iniciar un proceso de regulación al acceso justo y uso equilibrado de los datos en una economía digital, aprovechando sus múltiples beneficios comunes sociales. A pesar de los desafíos, aún se busca fomentar la innovación y la consolidación de mercados más competitivos a través de la atribución de un equilibrio efectivo entre acceso a los datos y la protección de otros derechos empresariales especialmente en las dinámicas B2B. Es cierto que el reglamento aún no entra en vigor sino hasta septiembre del 2025, pero se espera que los resultados sean tanto buenos para el reconocimiento del uso de los datos no personales como activo clave con potencial para generar un bienestar común e impulse la innovación tecnológica.

1.1.5. Aplicación en el sector minero

En el sector minero, aún persiste una marcada resistencia a compartir datos generados a través de tecnologías como el Internet de las cosas Industrial (IIot) o el AIoT. Tal como refiere Lester Villar, gerente de Investigación y Desarrollo de una empresa tecnológica vinculada al sector en el Perú, esta resistencia se debe, en gran medida, a la generación de datos de alta calidad, que son necesarios para perfeccionar los modelos predictivos o de operación. Los datos, al ser necesarios para la ejecución de los algoritmos, es necesario realizar prueba en los equipos en condiciones reales, lo que implica riesgos operativos y posibles pérdidas económicas cada vez que se realizan pruebas.

Actualmente, la gobernanza de los datos no personales en minería se estructura predominantemente a través de acuerdos contractuales, que establecen condiciones específicas y no necesariamente ventajosas para los diferentes agentes intervinientes. Los datos se incorporan de forma limitada y su acceso suele estar condicionado a términos especiales, como descuentos comerciales o tarifas diferenciadas. Sin embargo, no existe en la actualidad una legislación que obligue de manera general a abrir o compartir estos datos de forma estructurada, estandarizada y accesible (Duch-Brown, Martens, & Mueller-Langer, 2017).

La entrada en vigor del Data Act de la Unión Europea (Reglamento (UE) 2023/2854) introduce una transformación significativa en este escenario. De acuerdo con esta normativa, los usuarios finales de dispositivos IoT industriales, como los equipos de perforación minera, tendrán derecho a acceder a los datos generados por los dispositivos que utilizan, en tiempo real y bajo un formato estructurado, sin imponer costes adicionales injustificados (artículos 4 y 5 del Data Act). Además, podrán autorizar a terceros (como proveedores de servicios analíticos) a acceder a esos datos, siempre que se respeten los requisitos de calidad y formato previstos.

Un ejemplo de ello es el caso en el cual una empresa minera desea compartir con un proveedor desarrollador de software de análisis geotécnico los datos generados por su sistema de perforación inteligente. Bajo el Data Act, el fabricante del equipo de perforación deberá proporcionar estos datos a solicitud del usuario, garantizando su calidad y accesibilidad, salvo que pueda acreditar de manera justificada una excepción legítima.

Sin embargo, la aplicación del Data Act en minería aún es limitada. El reglamento se centra únicamente en datos en bruto o preprocesados (datos fuente o datos primarios), que se generan en el funcionamiento normal de los dispositivos y excluyendo los procesados (inferidos o derivados), como los resultados de las fases experimentales o los pilotos de pruebas (Reglamento (UE) 2023/2854, Considerando 15). Lo cual implica que aquellos datos que se generen a partir de las pruebas de sensores para la identificación de un fin determinado o la realización de hallazgos no estarían automáticamente disponibles, salvo acuerdo de las partes. Este último punto, en la práctica, suele ser atribuida la propiedad a las minas.

En segundo lugar, se observa el riesgo de que algunos fabricantes intentan invocar la protección de secretos industriales o de propiedad intelectual como justificación para negar o restringir el acceso a los datos, lo que podría obstaculizar los objetivos de apertura y reutilización de la normativa (Rens, 2019). Este fenómeno de "captura de datos" ya había sido advertido como un problema estructural en el ecosistema IoT industrial (Eckardt & Kerber, 2024).

Es evidente que la situación podría derivar en que, el acceso otorgado por el fabricante como una obligación, pueda derivarse de una imposición de tarifas poco razonables a cambio de compartir los datos. También es posible dilatar la entrega de datos para favorecer su propio análisis de datos bajo argumentos de dificultad técnica, esfuerzos desproporcionados, incluso

argumentar que tales datos se encuentran protegidos por secretos industriales y otros derechos de propiedad que estarían legitimando su negación a lo dispuesto en el reglamento.

En consecuencia, si bien el Data Act pretende democratizar el acceso a datos industriales en sectores como el minero, su implementación exigirá una supervisión estricta y mecanismos complementarios que aseguren su efectividad frente a posibles prácticas restrictivas y considerando las relaciones particulares en el sector. Asimismo, será fundamental promover acuerdos contractuales claros y en regular el equilibrio entre estos respecto de los datos generados en fases de experimentación tecnológica, para no dejar zonas grises que perpetúen mayores restricciones al flujo de información y la innovación.

La eficacia del Data Act o una normativa similar, en entornos mineros dependerá de las condiciones y el corte de la normativa a implementar, pero también su implementación práctica. Existen riesgos de que los titulares de datos impongan obstáculos indirectos mediante cláusulas contractuales restrictivas, demoras en la entrega de datos o interpretaciones amplias de los secretos industriales. Como señala Atik (2022), la regulación de los datos debe ir más allá de la mera atribución de derechos de acceso, incorporando garantías estructurales que prevengan el uso estratégico de la exclusividad para bloquear la competencia.

Finalmente es necesario considerar el Data Act como un referente, pero no como una solución final y basta. Es necesario que se complemente con políticas de fomento de interoperabilidad, establecimiento de incentivos para la creación de espacios de datos industriales compartido, acompañado de un plan de *enforcement* que prevea mecanismos de resolución rápida y eficiente de disputas sobre el acceso y en general, del ejercicio de derechos que se otorguen bajo los principios necesarios para garantizar el acceso y disfrute de los datos no personales.

1.2. Libre Circulación de Datos no personales de la Unión Europea

El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, adoptado en noviembre de 2018, establece un marco jurídico para garantizar la libre circulación de datos no personales dentro de la Unión Europea. Su objetivo principal es eliminar las restricciones injustificadas basadas en la localización de los datos, permitiendo así que empresas y entidades públicas puedan almacenar y procesar datos no personales en cualquier Estado miembro, sin obligación de establecer infraestructuras locales.

Este reglamento constituye un pilar esencial para el fortalecimiento de la economía digital europea, al facilitar el acceso y la movilidad de grandes volúmenes de datos industriales y de otro tipo, siempre que no estén relacionados con datos personales, los cuales permanecen regulados por el Reglamento General de Protección de Datos (RGPD).

La Comisión Europea ha destacado que la libre circulación de datos no personales es clave para el desarrollo de tecnologías emergentes como el Internet de las Cosas (IoT) y la Inteligencia Artificial (IA), donde el tratamiento de datos masivos resulta fundamental para la innovación. En el sector industrial, en particular, se reconoce que la integración de IoT e IA permite la recopilación y análisis de enormes cantidades de datos operativos. Al no estar vinculados a personas físicas, estos datos adquieren la categoría de datos no personales, y su libre flujo resulta crucial para la optimización de procesos, la mejora de la eficiencia y el impulso competitivo a través de la innovación.

Sin embargo, persisten debates respecto al establecimiento de derechos de propiedad sobre los datos no personales. Algunos sostienen que la atribución de derechos de propiedad podría incentivar la inversión y proporcionar mayor seguridad jurídica sobre los datos generados. Otros, en cambio, advierten que tal enfoque podría generar monopolios de datos, restringir el acceso y frenar la innovación. Por ello, en lugar de optar por regímenes de propiedad, diversas propuestas como la de Tarkowski y Vogelezang (2021) apuestan por el fortalecimiento de derechos de acceso y por la promoción de entornos de intercambio de datos más equitativos en los ecosistemas digitales.

En conclusión, aunque el Reglamento (UE) 2018/1807 no aborda la cuestión de establecer un sistema de derechos de propiedad sobre los datos no personales, tema que sigue siendo objeto de evolución y debate, sí constituye un instrumento fundamental para garantizar su libre circulación en la Unión Europea. De esta manera, actúa como un motor adicional para el desarrollo tecnológico, especialmente en sectores como el industrial, donde la innovación basada en datos es cada vez más estratégica.

1.3. Ley de Gobernanza de Datos (Data Governance Act o GDA)

La Unión Europea ha definido la Ley de Gobernanza de Datos como uno de los principales instrumentos para reutilizar los datos públicos o protegidos impulsando el intercambio y a la posición de datos de manera altruista, con el objetivo de beneficiar a la sociedad y afrontar

problemas sociales que pueden ser abordados a partir del análisis de datos, por ejemplo en el sector salud, para curar enfermedades para personalizar tratamientos de cuidado, en el sector trabajo para impulsar nuevos trabajados y ser un apoyo para los emprendimientos.

Ahora bien, consideramos que esta ley es clave para facilitar el acceso, compartición y en general, la reutilización de los datos no personales, y fortalece dicha interacción en las relaciones B2B, puesto que su implementación proporciona un marco legal que permite resolver las disputas sobre la titularidad de los datos y fija reglas claras para disuadir las prácticas anticompetitivas.

Si bien en los mercados digitales y en el uso de AIoT, las empresas se entrenan a problemas como la poca claridad sobre quién posee derechos para utilizar y acceder a los datos que se generan por los dispositivos conectados o a partir de los datos industriales que se recopilan en estos contextos, este marco regulatorio permite aclarar ciertos términos en relación de quienes son los “intermediarios” de datos neutrales que son quienes facilitan el compartir de los datos disuadiendo los controles absolutos o concentración en una sola empresa.

Por otro lado, ofrece mecanismo para acceder a los datos en tanto establece cómo se deben compartir los datos sin afectar la competencia y, por otro lado, facilita la interoperabilidad en la medida que sus mecanismos reducen el riesgo de bloqueo por parte una empresa que ha creado un ecosistema que está diseñado para excluir a otros de forma naturalmente técnica.

Por ejemplo, en el marco minero, un fabricante de sensores al recopilar los datos de rendimiento de una maquinaria, una empresa de software podría usar esos datos para investigar los factores que contribuyen a gestionar de manera sostenible el consumo de energía de la mina. De no contar con un marco que promueva el acceso, permitiría al fabricante bloquear el acceso a los datos, haciendo más oneroso la recolección de datos por otras empresas innovadoras y, en el caso de compartirse, no serían bajo términos equilibrados o justos que permita incentivar la innovación.

Por su parte, esta regulación genera que las empresas y usuarios cuenten con mecanismos de acceso sin depender de la voluntad y entera discreción de los fabricantes, disuadiendo los efectos *lock-in* de los datos y reduciendo la fragmentación en el acceso a los datos industriales. No obstante, aún quedan desafíos pendientes.

A diferencia de China, por ejemplo, los datos no personales pueden ser considerados propiedad de la empresa que los procesa, en tanto la UE establece derechos de acceso en vez de derecho de propiedad exclusivo. No obstante, aún quedan desafíos pendientes en relación con el límite para reclamar la titularidad de los datos que se generan a partir de su infraestructura y cuáles son los estándares técnicos para compartir los datos en términos de interoperabilidad.

Aunque pareciera que esta ley redunda en lo ya expuesto en el Reglamento de Datos, existen diferencias en relación con los objetivos, ámbitos de aplicación y datos que regula. A diferencia del DGA, el cual fomenta la participación voluntaria de los agentes en el mercado para que compartan los datos, estableciendo mecanismos que generen confianza para realizarlo, el Data Act impone obligaciones sobre los datos no personales de manera que restablece el equilibrio entre las partes y aporta condiciones de balance en el mercado.

Por otro lado, los tipos de datos en el DGA aplican a datos públicos, los anonimizados, datos no personales y los voluntariamente compartidos lo cual se sumerge dentro del marco de los datos abiertos, a diferencia del Reglamento de datos que trata de regular las situaciones B2B y B2C en un marco privado y en el uso de dispositivos IoT enfocado en los datos no personales. En suma, si el primer instrumento normativo se centra en datos previamente existentes que no están siendo correctamente utilizados o aprovechados por otros agentes de diferentes acciones y, en el segundo se regulan el acceso y el uso de los datos en mercados digitales en espacios de relaciones de consumidor o industriales.

El gran reto consiste en que toda regulación logre equilibrar adecuadamente obligaciones e incentivos, de modo que promueva la innovación tecnológica mediante beneficios claros y se garantice el acceso equitativo y el aprovechamiento colectivo de los datos. Asimismo, resulta fundamental definir qué autoridad sería competente para resolver los eventuales conflictos, tanto de índole legal como técnica, y establecer los mecanismos adecuados para su gestión. Además, debe considerarse el impacto económico que implica la creación de estándares de interoperabilidad, asegurando al mismo tiempo la protección de los derechos de propiedad intelectual de las empresas.

2. Perspectiva china de la Regulación de los datos no personales

Un reporte de la BBC ha destacado que la posición de China frente al desarrollo tecnológico para obtener la primacía comercial en el mundo como parte de su agenda política y económica del 2025. Pekín busca aumentar la producción en el sector y el aumento de sus exportaciones y con el establecimiento de estándares tecnológicos para incentivar la competencia (BBC News Mundo, 2024).

Asimismo, China está transformando su enfoque de la economía digital a partir de la integración compleja entre la IA y los datos en su economía. Con la inauguración de la Administración Nacional de Datos (NDA) en el 2023 se confirma el compromiso para el desarrollo económico basado en datos a partir del concepto “Data X”.

Esta política pública tiene como objetivo ampliar la visión sobre el valor estratégico de los datos, promoviendo la uniformización de estándares en las industrias para considerarlos como un activo fundamental. Busca maximizar el valor de los datos mediante su tratamiento y análisis, impulsando la innovación a través de la combinación de tecnologías como la inteligencia artificial (IA) y el Big Data, tanto para optimizar procesos de toma de decisiones como para utilizar los datos como catalizadores que permitan extraer información significativa. Además, promueve la circulación eficiente de los datos entre sectores, gobiernos y empresas privadas, fomentando la eliminación de barreras mediante la interoperabilidad de los sistemas (Foro Económico Mundial, 2024)

La articulación normativa de China en torno a la evolución de la economía digital ha contemplado la regulación de los datos no personales como activos jurídicos y económicos estratégicos. A través de su nuevo Sistema de Derechos de Propiedad de Datos, China establece derechos específicos de tenencia, uso y gestión sobre productos de datos, sin otorgar un derecho exclusivo de propiedad sobre los datos brutos. De este modo, se promueve la coexistencia de derechos funcionales que buscan estimular la comercialización y el uso compartido de los datos, favoreciendo la innovación tecnológica (Huang, 2024).

Esta coexistencia de derechos sobre un mismo conjunto de datos, como se ha señalado en el apartado 3.4. del capítulo II de este trabajo, coincide con las posiciones doctrinales que sostienen que la atribución compartida de derechos sobre datos puede fomentar el ecosistema de innovación y maximizar el valor de la información.

No obstante, como desarrolla Huang (2024), los tradicionales derechos de propiedad, como la titularidad exclusiva o el usufructo, no se adaptan a las características de los datos, dado que estos pueden ser duplicados y utilizados simultáneamente por múltiples procesadores. Por ello, la regulación china supera estos límites tradicionales mediante la asignación de derechos diferenciados que permiten la coexistencia de múltiples agentes económicos sobre los datos procesados.

En cuanto al control de la circulación internacional de datos, el régimen estatista chino, influenciado por consideraciones de seguridad nacional, ha establecido mecanismos como una "lista negra" o "*black list*" para restringir la transferencia de datos considerados sensibles, y "canales verdes" para facilitar el flujo de datos no sensibles en sectores estratégicos.

Finalmente, en 2022, en China se implementó un marco que reconoce derechos patrimoniales sobre *big data*, datos derivados del procesamiento de datos personales o no personales, garantizando un retorno económico razonable a los individuos o entidades que hayan contribuido a su creación (Huang, 2024). En ese marco, en comparación con la UE, ambos rechazan el modelo de propiedad exclusiva pero ambos reconocen que la estructura que permite explotar el valor económico de los datos es a través de derechos de acceso y uso.

En particular, China posee 3 mecanismos amplios en relación a los datos. Por un lado, la Regulación de Seguridad de Datos en Redes, que aplica a todo procesamiento de datos, incluyendo los datos no personales de los negocios, finanzas o datos industriales. En segundo lugar, la Ley de Seguridad de datos que se aplica de manera transversal a toda categoría de datos, incluyendo los datos no personales y, finalmente, la Ley de Protección de Información Personal (PIPL) muy similar a los objetivos que persigue el RGPD, el cual es proteger la información personal pero no se limita a esta.

Un informe de DLA Piper, desarrolla además que China posee regulación que afecta los datos no personales, cuyas disposiciones están contenidas en la Ley de Seguridad de Datos y en la Regulación de Seguridad de Datos en Redes que rigen el procesamiento de los datos que se genera en dispositivos de IoT y establecen disposiciones para su transferencia tanto interna como de manera externa.

El propósito de estas leyes es resguardar los derechos de los ciudadanos y entidades, a través de la seguridad de la información online y priorizando el reguardo de la seguridad pública y el

interés público. También tiene un alcance público y privado y es extraterritorial, puesto que se aplica a toda la actividad de procesamiento dentro o fuera de China y aquellos que se encuentran en el extranjero tendrían ciertas obligaciones. Además, se ha resaltado la importancia de proteger "datos importantes" y "datos centrales" que podrían ser parte del alcance de los datos generados por infraestructuras como el del IoT en las industrias. Para ello, al aplicarse tanto a datos personales como a los no personales, obliga a las empresas a clasificar y proteger los datos a partir del nivel de sensibilidad.

A su vez, la Regulación de Seguridad de Datos en Redes tiene un alcance bastante amplio porque aplica a los datos procesados en las redes, obligando a que los proveedores que generen en dispositivos conectados sean procesados dentro de China y, si son exportados, deberán pasar una evaluación de seguridad por la entidad encargada, la Administración del Ciberespacio de China (CAC).

Una clara distinción sobre la regulación expuesta en el Data Act, es que China introduce una serie de regulaciones respecto de los datos, la seguridad y el flujo de estos. El enfoque es predominantemente sobre el control estatal y en la aplicación de restricciones en las transferencias internacionales. Por el caso de "datos importantes" como categoría de datos, China ha establecido que estos deberán ser almacenados únicamente China y las restricciones para su transferencia son altamente severas y deben ser revisadas previamente por el CAC.

A diferencia de la Unión Europea con el Data Act, este promueve la compartición y acceso equitativo a los datos que se generan por el IoT en igual condiciones. Asimismo, los usuarios y terceros pueden acceder a los datos de dispositivos IoT bajo términos FRAND y, por último, respecto al flujo transfronterizo existe una flexibilización de los requisitos de seguridad, que si bien se deben adaptar, en la medida que sea subsanables, el flujo se promueve abiertamente.

Por su parte, los datos no personales en relación a la propiedad intelectual, China establece medidas para protegerlos a través de las bases de datos, siempre que estas cumplan con los criterios específicos de legalidad, que sean procesados por algoritmos y contener un valor comercial. Los derechos de propiedad intelectual sobre las bases de datos les permite ser transferibles e incluso ser usados como parte de garantía financiera puesto que representan un valor monetario y permiten a las empresas explotar su valor monetario.

China promueve el acceso y la compartición de datos aun cuando estos no tengan un propietario único. Sin embargo, a diferencia de los sistemas basados en principios de *open data*, como el impulsado por la Unión Europea, su enfoque se caracteriza por un acceso controlado o "parcial". En este modelo, los procesadores de datos pueden obtener derechos funcionales exclusivos sobre el uso y comercialización de los productos de datos, aunque no sobre los datos fuente, fomentando así la explotación económica bajo estricta supervisión estatal (Huang, 2024).

Asimismo, mientras la UE fomenta la libre circulación de datos no personales mediante estándares comunes y protección de la privacidad, China implementa listas negativas que restringen la transferencia internacional de ciertos datos considerados estratégicos, acompañadas de canales verdes para facilitar flujos en sectores autorizados.

Un rasgo distintivo del sistema chino es su apertura a reconocer derechos patrimoniales sobre productos de datos, con la intención de fortalecer la innovación tecnológica doméstica. Esto contrasta con el enfoque del Data Act europeo, que busca evitar la concentración de datos en manos de grandes corporaciones, promoviendo un acceso equitativo y competitivo.

Si bien China avanza en la compatibilización de su régimen con acuerdos como el Asociación Económica Integral Regional[4] (RCEP), restringiendo la localización de datos solo cuando sea estrictamente necesario por razones de seguridad nacional, persisten desafíos en materia de interoperabilidad, seguridad jurídica y acceso igualitario para empresas extranjeras. Además, subsisten incertidumbres en la distinción práctica entre datos personales y no personales y en la asignación efectiva de derechos y beneficios sobre estos, particularmente en entornos AIoT.

A la fecha este modelo también ha recibido ciertas críticas y asume retos conforme avanzan la aplicación de las disposiciones en la distinción entre datos personales y no personales sigue siendo difícil de implementar, lo que genera incertidumbre en la regulación de flujos de datos transfronterizos. Y por otro lado, se necesitan clarificaciones adicionales sobre la interacción de los diversos derechos asignados a los procesadores y sobre cómo garantizar una distribución justa de beneficios para los sujetos de datos.

[4] Es un acuerdo de libre comercio entre 10 estados miembros de la Asociación de Naciones del Sudeste Asiático (ASEAN) y 5 estados de Asia y Oceanía (Australia, Nueva Zelanda China, Corea del Sur, Japón).

China está desarrollando un marco regulatorio innovador que busca equilibrar la seguridad nacional, los derechos de los procesadores y el acceso a los datos para fomentar un ecosistema de datos eficiente y competitivo. Sin embargo, enfrenta desafíos relacionados con la interoperabilidad internacional y la implementación de derechos claros y justos.

Una apreciación interesante que desarrolla Huang en su análisis de las diferencias entre los derechos de propiedad reconocidos en China de aquellos establecidos por la UE es que los procesadores de datos en China son predominantemente domésticos, a diferentes de los procesadores de la UE que son comúnmente de procedencia de Estados Unidos y sus políticas han sido dirigidas principalmente para exigir a los procesadores americanos a compartir los datos con los entes en territorio europeo.

Tal es el motivo por el cual, muchos de los países a nivel internacional deberían estar impulsados a estandarizar o uniformizar las disposiciones en materia de circulación y reutilización de los datos no personales, no solo porque permite la colaboración internacional en el flujo de datos con el fin de desarrollar sectores específicos a partir de la creación s e innovación con tecnología de vanguardia, sino además, permite modificar los comportamientos de los agentes en el mercado en relación a la adopción de medidas técnicas más seguras para evitar exponer vulnerabilidad y poner en riesgo sus sistemas y los datos en general.

Los desafíos en materia de regulación de datos aún se mantienen pendientes. El primer paso es reconocer que, al menos en el sector industrial, los datos no personales son cruciales para desarrollar y mejorar las condiciones en el desarrollo de actividades productivas, incluso ciertas aplicaciones en relación con la seguridad en el trabajo y los colaboradores, y lo que se mantiene en discusión latente es cómo deberían ser distribuidos los datos, cómo deben ser utilizados, quien los posee o es titular.

A pesar de esta situación que la regulación en China está centrada en el uso de los datos para fines de innovación, el factor de interés público es predominante y ello, deja en incertidumbre o en una zona gris, a las empresas extranjeras, quienes aún podrían tener dificultad para acceder en las mismas condiciones que las empresas nacionales chinas a los datos no personales. Esta situación implica burocracia y falta de incentivos por parte de las empresas nacionales chinas a compartir los datos.

En suma, China está construyendo un marco innovador que, aunque impulsa la innovación tecnológica nacional, plantea interrogantes para la cooperación digital internacional y el comercio transfronterizo de datos, aspectos donde el modelo europeo ofrece un enfoque más abierto y competitivo.

2.1. Objetivos y ámbito de aplicación

China adopta un modelo de regulación de datos que reconoce derechos funcionales específicos a los procesadores de datos, quienes transforman datos en productos valiosos, asignándoles facultades de posesión, uso y comercialización de los productos derivados, sin reconocer una propiedad exclusiva sobre los datos brutos. Paralelamente, establece derechos de acceso limitados a los titulares de los datos, principalmente respecto de los datos en estado bruto.

El Sistema de Derechos de Propiedad de Datos de China, tal como analiza Huang (2024), persigue tres objetivos principales: reforzar el control estatal y la seguridad nacional; incentivar la monetización de los datos no personales a través de los procesadores; y prevenir la formación de monopolios privados que puedan concentrar información estratégica.

En primer lugar, del análisis del texto de Huang y el reporte de DLA Piper, se desprende que el control estatal y la seguridad nacional ha sido siempre una prioridad de la República Popular, y el control de los datos, que funciona como un activo que proporciona poder y fuente de conocimiento a partir la información inferida, ha llevado a su regulación control el acceso y uso de los datos que se generan por infraestructuras críticas o a partir del internet de las cosas, lo cual busca restringir su transferencia al extranjero por el tipo de información que posee con el uso de listas negras de tipos de datos que no deben ser compartidos y estableciendo canales verdes para la transferencia de datos al extranjero, asegurando además su almacenamiento dentro del territorio chino.

Por otro lado, en cuanto a la monetización, el sistema otorga a los procesadores de datos derechos exclusivos sobre productos de datos a través de una estructura tripartita: derechos de posesión de datos, derechos de procesamiento y derechos de gestión comercial. Esta lógica busca incentivar el desarrollo de servicios de datos y fortalecer la economía digital nacional.

Sin embargo, a diferencia del Data Act de la UE, el sistema chino no impone un deber general de compartición de datos inferidos. Si bien fomenta el acceso a ciertos datos en bruto, la

comercialización de datos procesados permanece mayormente bajo control del procesador, reflejando una política de innovación dirigida hacia el fortalecimiento de actores nacionales

El Comité Central del Partido Comunista Chino y el Consejo de Estado han señalado que la consolidación de un sistema de propiedad de datos busca establecer una infraestructura jurídica sólida para regular el uso, la transferencia y la apertura controlada de los datos en favor del desarrollo económico y la soberanía digital.

En este contexto, China ha manifestado su interés en adherirse al *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP). Sin embargo, para cumplir con los estándares de dicho tratado, deberá realizar ajustes significativos en su régimen de protección de datos personales, en los requisitos de localización de datos, y en las disposiciones de ciberseguridad, a fin de facilitar la libre circulación internacional de datos conforme a las exigencias del comercio digital global.

Este acuerdo es considerado uno de los proyectos más grandes que actualmente tiene con Japón, Australia, Canadá y México en la libertad de flujo de datos, pero para que China entre a dicho acuerdo tendría que modificar no solo su legislación en tema de protección de datos personales sino también en los estándares de ciberseguridad que tienen establecidos a nivel internacional a fin de cumplir con los requisitos del tratado.

De lo comentado podemos concluir que, si bien tanto el Data Act europeo como el Sistema de Derechos de Propiedad sobre Datos de China persiguen incentivar el aprovechamiento económico de los datos, sus enfoques y objetivos divergen significativamente. Mientras la Unión Europea prioriza la democratización del acceso y la equidad en el ecosistema de datos, China privilegia el control estatal, la seguridad nacional y la monetización estratégica a favor de procesadores locales. Esta diferencia estructural refleja modelos de gobernanza digital antagónicos, cuyas tensiones se proyectan tanto en el comercio internacional como en la construcción futura de marcos regulatorios globales para los datos no personales.

2.2. Oportunidades

El sistema chino de derechos de propiedad sobre datos enfrenta aún numerosos desafíos, no solo en términos de fragmentación normativa, sino también respecto al acceso efectivo a los datos industriales y a la consolidación de un ecosistema de datos dinámico y competitivo.

Por un lado, persisten importantes barreras para las empresas extranjeras en el acceso a datos industriales estratégicos. La combinación de estrictos controles regulatorios, procesos burocráticos complejos y exigencias de localización de datos crea condiciones poco favorables para el intercambio transfronterizo de información, afectando negativamente el desarrollo de iniciativas de innovación internacional.

Por otro lado, la falta de incentivos claros para que las empresas nacionales compartan datos con terceros limita la apertura del mercado digital y restringe el surgimiento de nuevos negocios o servicios ofrecidos desde otros países. Esta situación también impide que los datos locales sean utilizados en estudios globales que requieran diversidad demográfica, cultural o socioeconómica, reduciendo así el potencial de los datos chinos para alimentar tecnologías inclusivas y adaptadas a estándares internacionales.

Para consolidar un sistema de datos competitivo y globalmente integrado, será necesario que China avance hacia una mayor armonización normativa, garantice reglas de acceso equitativas, y adopte políticas que favorezcan el flujo seguro de datos a nivel internacional, equilibrando los intereses de innovación económica a nivel global con las legítimas preocupaciones de seguridad nacional.

Considero que a fin de fortalecer el ecosistema de datos y potenciar su entrada en el mercado global sin constituir una amenaza o una fuente de datos inestable y poco transparente como actualmente se percibe a China, se deberá considerar medidas que apunten a mejorar la transparencia regulatoria, reducir las cargas burocráticas en la transferencia de datos y fomentar mecanismos de interoperabilidad internacional.

Establecer estándares claros de acceso equitativo, reconocer derechos balanceados entre procesadores y usuarios, y favorecer prácticas de gobernanza de datos en concordancia con los avances en marcos internacionales facilita el desarrollo tecnológico interno y su participación más activa y confiable de China en los mercados digitales globales.

2.3. Críticas

China aún se enfrenta a problemas para aplicar este modelo “tradicional” de la propiedad y el uso de los datos. Este sistema, que permite incluso, las formas de usufructo tradicionales no se adaptan a la naturaleza de los datos, que como ya hemos visto, es no rival, no se agota en su uso y puede duplicarse y compartirse de forma simultánea. No obstante, al mismo tiempo no

existe exclusividad, lo que resulta contraproducente aplicar reglas que funcionan para bienes que son pasibles de ser tratados como exclusivos, cuando en el caso de los datos, dificulta definir claramente los derechos de los usuarios y de quienes los procesan.

En consecuencia, a pesar que se cuenta con un sistema de reconocimiento de derechos que aborda también la multiplicidad de actores que intervienen dentro del procesamiento de los datos no personales en contextos como Big Data en general o AIoT, aún queda como un reto los posibles de conflictos de distribución equitativa de los beneficios porque aún no se dejan claras las reglas sobre si los usuarios pueden acceder o no a la data inferida o si es posible la previsión de una retribución por el compartir los datos, además que no se establecen cuestiones de privacidad y podría generar un conflicto en la competencia.

Finalmente, China ha generado un marco normativo que evita compartir datos que ellos mismos generan a otras jurisdicciones y, si bien tienen tendencias sobre los datos abiertos dentro de China, aún se evidencian algunas restricciones para la internacionalización de los datos y esto conlleva a consolidar su posición en los derechos de propiedad que se les atribuye a los datos, porque de esa forma generan un control sobre los datos legitimando su intervención estatista para el uso de estos.

Por un lado, promueven la compartición nacional de los datos, así como pretenden fomentar la competitividad al prever formas de compartición de datos y el establecimiento de medidas de seguridad para dicha transferencia, pero por otro, aún se imponen estrictos controles sobre la transferencia y acceso a los datos, especialmente en sectores como el IoT, finanzas y telecomunicaciones que son estratégicos al establecer restricciones de almacenamiento local y aprobaciones previas por el gobierno para compartir los datos fuera del país.

A continuación, un cuadro comparativo didáctico para comprender algunas diferencias a tomar en cuenta de las regulaciones de China y la UE, basados en la investigación de Huang y de lo analizado sobre el Data Act:

Criterio	Data Act de la Unión Europea	Sistema de Derechos de propiedad de China
Acceso	Basado en el principio de *open data* para sectores industriales, acceso bajo condiciones FRAND.	Acceso parcialmente abierto, condicionado por finalidades (no lucrativas vs. comerciales) y políticas de seguridad nacional

Derechos sobre los datos	Derechos de acceso, uso y compartición; no derechos de propiedad.	Derechos funcionales (tenencia, uso, gestión) sobre productos de datos, no sobre datos en bruto.
Tratamiento de los datos producidos por el estado	Los datos públicos deben ponerse a disposición en el marco de *Open Data Strategy*.	Los datos gubernamentales se ofrecen gratuitamente solo para fines no comerciales; uso comercial sujeto a tarifas
Restricciones a flujos de datos	Se promueve el flujo libre de datos no personales dentro de la UE y con socios externos, salvo protección de datos personales	Lista negativa para datos sensibles y green channels para facilitar exportaciones de datos no sensibles
Impacto en la competencia	Busca prevenir la concentración de poder en grandes plataformas.	Permite concentración limitada en procesadores nacionales; interés público y seguridad nacional son prioritarios.
Beneficiarios principales	Usuarios industriales, consumidores, PYMES, nuevos entrantes tecnológicos.	Empresas nacionales chinas, controladas por intereses de soberanía digital y seguridad nacional

***Nota**: Cuadro de elaboración propia a partir de las características de la normativa comparada en materia de sistema de protección de datos no personales.*

En ese sentido, las decisiones son centralizadas porque el Estado chino aún mantiene un control significativo sobre la gobernanza de los datos, garantizando que las empresas nacionales y extranjeras cumplan con las regulaciones específicas que imponen, que supervisan constantes y aprueban a través de la entidad fiscalizadora, la Administración del Ciberespacio de China (CAC).

Para finalizar, las oportunidades aún están en constante evolución y análisis a medida que van interactuando los agentes en el mercado digital con nuevas tecnologías, no obstante, a pesar de ello, China equilibra el desarrollo de su economía digital bajo un enfoque de control estatal sobre la compartición de los datos, priorizando la seguridad nacional y refuerza su soberanía en el marco del acceso abierto a los datos.

3. Regulación de los datos en Estados Unidos de América

La regulación de Estados Unidos se ha mantenido al margen y espectadora de los avances regulatorios en materia de protección de datos. Inicialmente respecto de los datos personales que publicó la UE en el 2016 con el RGPD, Estados Unidos no ha considerado relevante crear una ley que regule las formas de tratamiento de los datos y de merecer una tutela efectiva en la

medida que el enfoque de uno de los grandes países tecnológicos ha sido el de dejar al mercado la regulación de los temas en cuestión puesto que prevalece el avance y desarrollo tecnológico.

Respecto a los datos personales, Estados Unidos tiene una regulación compleja y fragmentada a nivel de estados. A nivel federal, existen leyes específicas para ciertos sectores como la *Health Insurance Portability and Accountability Act* (HIPAA) que establece estándares de protección para el uso y divulgación de información protegida sobre la salud (PHI) por parte de entidades sujetas a la norma (*Centers for Disease Control and Prevention*, 2022). Otro es la *Children's Online Privacy Protection Act* (COPPA) que impone obligaciones a los operadores de páginas web para proteger a los menores de 13 años, y la Gramm-Leach-Bliley Act (GLBA) que exige niveles de transparencia respecto de la información que comparten sobre sus clientes y también sobre las garantías de su información sensible en uso de servicios financieros, mientras que a nivel estatal se han promulgado normas heterogéneas.

En consecuencia, hace difícil la adopción de los mecanismos heterogéneos que imponen a nivel de seguridad y dependen del sector aplicable. Tal como señala en un artículo de Mailjet (septiembre 20, 2024) el enfoque político influye decisivamente en esta dinámica normativa, ejemplificado en iniciativas como la propuesta durante la administración Trump para permitir a los proveedores de servicios de internet vender datos de consumidores sin su consentimiento previo, con el argumento de fomentar la competencia en el entorno digital.

En este contexto, podemos evidenciar que hasta ese punto los niveles de protección a los datos de al menos los usuarios que representan personas naturales son mínimamente equilibrados con la expectativa de generar un producto tecnológico viable o de monetizar con ello. Sin embargo, con la adopción de California Consumer Privacy Act en el estado de California, se imponen por primera vez muchas de las disposiciones que se establecen en el RGPD para la protección de los datos y cada vez más estados se sumaron a la tendencia.

En 2024, la fragmentación regulatoria en Estados Unidos se ha profundizado no solo en términos de cantidad de normas estatales, sino también en cuanto a su calidad y orientación temática. Según un informe reciente de la *International Association of Privacy Professionals* (IAPP), las siete nuevas leyes de privacidad estatales promulgadas en 2024 presentan enfoques sustantivamente diferentes en la manera de abordar los daños a la privacidad, reflejando respuestas adaptadas a los desafíos de la innovación tecnológica y nuevas sensibilidades sociales (IAPP, 2024). Esta creciente diversidad legislativa introduce mayores retos de

cumplimiento para las organizaciones, dificultando aún más la consolidación de estándares uniformes a nivel nacional.

Si bien Estados Unidos no cuenta con una ley similar al *Data Act* que prevea un sistema de atribución de derechos sobre los datos no personales para que tanto los usuarios y los proveedores tecnológicos cuenten con mecanismos balanceados para el acceso, uso y explotación de los datos no personales, el *California Consumer Privacy Act* muestra algunos indicios de acceso a los datos que busca equilibrar ciertos poderes en las relaciones usuario-proveedor, otorgando mayor control sobre su información personal que a pesar de aplicarse a datos personales, su impacto ha generado que más empresas replanteen sus prácticas sobre el uso de los datos a nivel general (Mailjet, 2024).

Respecto a los datos no personales y la economía del Internet de las Cosas (IoT), Estados Unidos carece actualmente de una regulación federal integral comparable al Data Act europeo, que establezca derechos específicos para usuarios o procesadores sobre los datos industriales. Sin embargo, existen esfuerzos parciales. La *Internet of Things Cybersecurity Improvement Act* (Ley de mejora de ciberseguridad para el Internet de las Cosas) de 2020 exige al Instituto Nacional de Estándares y Tecnología (NIST) definir estándares mínimos de ciberseguridad para dispositivos IoT adquiridos por el gobierno federal, evidenciando una preocupación creciente por la protección de datos, sean personales o no personales.

En un artículo de Global Sing, Illing (2024) señala que, en relación con los dispositivos IoT en edificios inteligentes, miles de sensores están siendo instalados en 80 edificios gubernamentales en los estados americanos, los cuales buscan para rastrear, localizar y controlar la emisión de más de 200.000 vehículos para garantizar el cumplimiento de los mandatos gubernamentales en la disminución de gases de efecto invernadero. De este modo, asegurar la calidad y la confianza en el uso de dispositivos IoT no solo a nivel estatal sino nacional, es un reto que debe ser asumido al margen de la posibilidad de interconectar a los proveedores para la compartición de datos, que, dicho sea de paso, será una condición fundamental en la previsión de una eventual regulación de los datos personales por los Estados Unidos.

En conclusión, si bien en Estados Unidos existen regulaciones importantes en materia de protección de datos personales y estándares mínimos de ciberseguridad para dispositivos IoT, aún no se ha desarrollado una legislación federal específica que regule la gestión, el acceso o la

reutilización de datos no personales. Dada la importancia estratégica de estos datos para el desarrollo tecnológico, la internacionalización de las empresas y la competitividad digital, la creación de un marco jurídico que equilibre los intereses de usuarios y proveedores podría constituir un paso crucial hacia un ecosistema de datos más seguro, interoperable e innovador.

CONCLUSIONES

A partir de lo analizado a lo largo del presente trabajo, se concluye lo siguiente:

- El uso de sistemas AIoT en entornos industriales complejos, generan datos personales y no personales en el despliegue de los sistemas. Específicamente en el sector minero, en el marco de las relaciones B2B, se evidencian una serie de relaciones complejas respecto al uso de estos datos no personales en el uso de estas tecnologías, siendo la generación y procesamiento de los datos no personales un componente de gran valor para el crecimiento y desarrollo de la industria. Estos intereses versan sobre los beneficios económicos potenciales del procesamiento de los datos no personales y la búsqueda por su apropiación y control exclusivo es inminente. Estos datos no personales no poseen regulación, por lo que no se puede determinar quiénes están legitimados a ejercer exclusión sobre estos, lo cual evidencia la importancia de determinar una regulación a que permita la gestión adecuada a fin de promover un crecimiento equitativo y sostenible del sector tecnológico y de la innovación. En ese sentido, es necesario abordar la naturaleza jurídica de los datos no personales, considerando que en la práctica ya tienen un valor económico, con la finalidad de determinar qué categoría jurídica se le debe asignar para regular una adecuada gestión y disponibilidad de estos en sectores donde intervienen múltiples agentes como el uso de AIoT en las relaciones B2B del sector minero.
- La determinación de la categoría jurídica de los datos no personales empieza por determinar cuál es la naturaleza jurídica de estos, y para ello es importante destacar que poseen características económicas que los hacen pasibles de tutela. En primer lugar, se caracterizan por ser bienes no rivales, parcialmente excluibles y pueden ser reproducidos de manera ilimitada, es decir no son escasos y con ello, su aprovechamiento. Estas características demuestran que sus atributos económicos y estructurales no encajan con categorías jurídicas tradicionales y por tanto, requieren ser abordados bajo un régimen de gobernanza común como el de los comunes digitales. Este esquema se alinea con las características intrínsecas de los datos no personales y, al reconocer su potencial valor en el proceso de digitalización, responde como un modelo alternativo, que determina la titularidad de forma no exclusiva. Los datos no personales como *digital commons* buscan ser administrados colectivamente por la comunidad sin ser necesariamente de propiedad exclusiva de privados o pública. lo que permite que sean gestionados en común,

promoviendo libertades de acceso y uso bajo condiciones limitadas y reguladas, evitando los efectos de monopolización y barreras para la entrada de nuevos competidores.

- Los modelos jurídicos tradicionales de atribución de propiedad, desde la concepción de exclusividad, como los derechos reales, la propiedad intelectual o la protección de datos personales, resultan inadecuados para regular los datos no personales. En los derechos reales, el control exclusivo, absoluto y oponible a terceros es incompatible con la reproducibilidad y naturaleza compartida de los datos. En la propiedad intelectual, la exigencia de originalidad y creatividad colisiona con la característica de los datos en bruto como representaciones fragmentadas de la realidad. En el ámbito de la protección de datos personales, el elemento subjetivo vinculado a la persona natural se encuentra ausente, por lo que no estaría dentro del ámbito de aplicación. Evaluar categorías tradicionales e insistir en la réplica de estos modelos para la regulación de los datos no personales, supone forzar categorías jurídicas que desconocen una realidad técnica y que generaría situaciones adversas a los objetivos de gestión colectiva como la tendencia del ejercicio de exclusividad "de facto" sobre los datos no personales, trabas en el fomento del aprovechamiento de los datos y trabas a la innovación en condiciones equitativas.
- A partir del análisis dogmático-sistemático de las categorías jurídicas tradicionales privadas y públicas posiblemente aplicables, resultan insuficientes para abordar los desafíos que plantea un ecosistema de datos en el mercado digital, por lo que la atribución de "propiedad" sobre los datos no personales, deviene en contraproducente a los objetivos de promover la innovación, competencias e interoperabilidad. Por el contrario, resulta pertinente asignar una titularidad funcional y no los conceptos de propiedad, pues esta última refiere a exclusividad respecto la cosa y, la titularidad, parte sobre la base de asignar derechos que permitan ser portados por ciertos agentes sobre un título de un derecho. Estos derechos deben promover la circulación de los datos no personales desde una perspectiva funcional. Esta funcionalidad está basada en la asignación de conjunto de facultades como el acceso, uso y compartición, así como garantías técnicas y jurídicas respecto a límites y transparencia. A su vez, es importante determinar costos razonables, mecanismos de auditoría y reglas FRAND (*fair, reasonable and non-discriminatory*) que constituyen una solución eficiente y funcional, porque permite maximiza el valor social del dato sin desincentivar la innovación privada ni erosionar la protección legítima de la propiedad intelectual.

- La normativa comparada los califica como insumos valiosos y, entonces introduce el Data Act, un referente normativo que prioriza el acceso equitativo y compartición de datos como mecanismos para corregir las asimetrías de poder entre fabricantes, usuarios y terceros. Este modelo promueve un ecosistema basado en la interoperabilidad y la innovación colaborativa, garantizando a su vez la seguridad de los datos industriales. A diferencia del modelo chino cuyo enfoque se centra en la monetización y control estatal de los datos priorizando objetivos de seguridad nacional y restringiendo el flujo transfronterizo. Este contraste evidencia que el diseño regulatorio no es neutral, por el contrario responde a objetivos de seguridad nacional confirme las prioridades políticas y económicas. En el Perú, como parte de la región de América Latina, resulta más cercano un esquema que busque fomentar la innovación y equilibrar accesos entre los agentes industriales y evitar los riesgos de control excesivo que desincentive el desarrollo nacional de tecnología como internacional.

- Existe una necesidad que la regulación específica para la atribución de derechos sobre los datos no personales contemple disponibilidad de los datos en término de acceso, sin que predomine un enfoque restrictivo o en la apropiación exclusiva de los datos. Es importante, además, que el desarrollo de una regulación especial realice una reflexión sobre los eventuales riesgos con otros objetivos de interés público, como la promoción de la innovación tecnológica, la interoperabilidad y la equidad en el acceso al conocimiento. Con un modelo equilibrado, los datos no personales, especialmente aplicable a los datos en bruto, se utilizarían en el mercado bajo parámetros de disponibilidad por derechos de acceso y estándares de interoperabilidad, permitiendo que los usuarios y fabricantes del AIoT u otros agentes intervinientes estén facultados a compartir datos con terceros (privados o públicos), independientemente de la relación de competencia. Con la asignación equilibrada de titularidad y tomando en consideración los intereses de los diversos actores intervinientes, se puede generar una situación de bienestar compartido en el mercado digital y sobre todo en el fomento de la innovación y competitividad en igualdad de condiciones.

- La Unión Europea ha realizado avances regulatorios en la materia a fin de promover el intercambio voluntario de datos. El Data Act busca que puedan ser compartidos en condiciones equitativas, sin cargas monetarias excesivas o desproporcionadas. Es un reto para otras regulaciones que no solo se persiga esta finalidad sino que también avancen los estándares de interoperabilidad como un requisito principal para evitar barreras en el ejercicio de los derechos respecto al flujo de los datos no personales en contextos industriales. Sin embargo, en el ámbito peruano, persisten significativos retos en la aplicación de las normas preestablecidas, que pueden intervenir de manera a posteriori. Por ende, de la revisión de la normativa existente en esquemas tradicionales, se replantea el tipo de situación jurídica que requiere la gestión de los datos no personales y dicho esquema debe responder a ciertos riesgos como la monopolización de los datos no personales, desincentivos a la innovación tecnológica, creación de nuevas barreras de entrada y la ausencia de interoperabilidad.

- Sobre el uso de herramientas para promover la libre competencia, como la doctrina de las facilidades esenciales debe reservarse como última ratio, puesto que su intervención ex post, los exigentes estándares de esencialidad, la exigencia de calificar como bien insustituible y el riesgo de constituir una barrera para el desarrollo tecnológico, convierten a este instrumento jurídico como un remedio reactivo y poco escalable en mercados dinámicos y orientados a la interoperabilidad como los datos no personales. En contextos AIoT, conviene implementar una normativa con un diseño *ex ante* de acceso, disponibilidad e interoperabilidad por diseño. Con este esquema se busca reducir asimetrías de poder en la cadena de valor tecnológica aplicada a industrias, y que articule límites claros por privacidad y la propiedad intelectual.

- La aplicación contextualizada de la DFE en el ámbito de los datos no personales del AIoT puede constituir una herramienta útil de inspiración para promover marcos jurídicos innovadores que protejan el concepto de los bienes digitales comunes y promover el acceso equitativo, prevenir abusos de posición dominante y dinamizar los mercados complementarios. Sin embargo, su eficacia dependerá de la capacidad de los reguladores para establecer criterios objetivos, mecanismos de compensación justa y garantías de protección técnica e informativa, que equilibren el derecho a la competencia con el fomento legítimo de la innovación tecnológica.

- El desarrollo de un régimen jurídico para los datos no personales en el Perú debe ser gradual, integral y funcional. Debe ser gradual porque requiere de maduración tecnológica pero también institucional en el país. Integral, porque se deben coordinar políticas actuales sobre la innovación y prepararse para los problemas a los que nos enfrentamos en caso de desbalances o incumplimientos, por lo que la competencia de las instituciones públicas y privadas debe estar preparada. Finalmente, funcional o pragmática porque debe ofrecer soluciones adaptadas a la realidad de la industria minera y otros actores estratégicos. Este régimen debe reconocer expresamente derechos de acceso y uso, fomentar estándares abiertos de interoperabilidad, establecer incentivos claros para compartir datos de manera segura y fortalecer las capacidades institucionales del Estado para regular de forma eficiente. Solo bajo un enfoque de innovación, equidad y eficiencia institucional será posible transformar los datos no personales en activos estratégicos de real impulso a la innovación tecnológica del país y, en consecuencia, de las industrias.

- El Data Act adopta una posición de titularidad, mediante la asignación de derechos de uso, acceso y compartición de estos, pero la tendencia de este instrumento normativo internacional prevalece sobre la posición del usuario, otorgando mayores facultades para la disposición y acceso a los datos. Esta situación no es ideal, en tanto puede generar nuevas formas de control sobre los datos no personales, provocando efectos que inicialmente se quería combatir. Consideramos que el otorgamiento y ejercicio de estos derechos no debe recaer en un lado más que en el otro, sino que se deben asignar derechos de manera armónica y proporcional, equilibrando la intervención de diferentes actores en el uso del AIoT en contextos industriales.

- China adopta un modelo estatista, creando barreras de compartición bajo criterios de territorialidad y nacionalidad, es decir que no se puede compartir información con terceros que se encuentre fuente del territorio chino o que provengan de empresas extranjeras. Por su parte, Estados Unidos no se ha pronunciado sobre la regulación, pues se entiendo que la negociación contractual es clase para llegar a acuerdos de uso, acceso y compartición, lo cual deja de libre albedrío a las empresas la promoción de los datos no personales en los mercados digitales.

BIBLIOGRAFÍA:

Alessandro Floris, & Luigi Atzori. (2015). *Quality of Experience in the Multimedia Internet of Things: definition and practical use- cases*.

Aldunate, E. (2003). La titularidad de los derechos fundamental. *Estudios Constitucionales 1(1),* 187-201.

Atik, C. (2022). Towards Comprehensive European Agricultural Data Governance: Moving Beyond the "Data Ownership" Debate. *IIC International Review of Intellectual Property and Competition Law*, *53*(5), 701–742. https://doi.org/10.1007/s40319-022-01191-w

Atik, C. (2023). Addressing data access problems in the emerging digital agriculture sector: potential of the refusal to deal case law to complement ex-ante regulation. European Competition Journal, 19(3), 380–409. https://doi.org/10.1080/17441056.2023.2200618

Avendaño Valdez, J., & Avendaño Arana, F. (2017). Derechos reales (Vol. 00001). Fondo Editorial de la Pontificia universidad Católica del Perú.

Awaisi, K. S., Ye, Q., & Sampalli, S. (2024). A Survey of Industrial AIoT: Opportunities, Challenges, and Directions. *IEEE Access*, *12*, 96946–96996. https://doi.org/10.1109/ACCESS.2024.3426279

Barnett, R. E. (1986/2004). Una teoría consensual del contrato [A consent theory of contract] (F. de Cárdenas Romero, Trad.; E. Sotelo Castañeda, Supervisión). *Themis Revista de Derecho*, (49), 269–312. (Trabajo original publicado en 1986 en *Columbia Law Review*, 86, 269).

Berenguer-Contri, G., Gil-Saura, I., Gil, R., Vallejo-Auñón, L., & Juma-Michilena, I.-J. (2021). *ICT and value co-creation in B2B: The new way of loyalty in service*. Journal of Business Research, 129, 839 849. https://doi.org/10.1016/j.jbusres.2020.10.021

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press. Disponible en línea (Creative Commons Noncommercial ShareAlike): https://www.benkler.org/Benkler_Wealth_Of_Networks.pdf

Benkler, Y. (2006). La riqueza de las redes: Cómo la producción social transforma los mercados y la libertad . Yale University Press.

Bernal, M. E. (2006). Breves apuntes sobre la ocupación del dominio público mediante las redes de Telecomunicaciones. *Revista De Derecho Administrativo*, (1), 263–283. Recuperado a partir de https://revistas.pucp.edu.pe/index.php/derechoadministrativo/article/view/16357

Barrios, F. T., & Espinosa, F. M. (2006). El concepto de derechos reales. Revista de Derecho Privado, 36, 115–136.

Barco, C. A. (n.d.). *Autorregulación. Apuntes Conceptuales*. http://www.observatoriofucatel.ci/wp-content/uploads/201

Bertin Martens, B., Kerber, W., Kramer, J., Graef, I., Tombal, T., Zettelmeyer, J., Carugati, C., & in TILEC, participants. (2023). *TILEC Discussion Paper Pro-and anti-competitive provisions in the proposed European Union Data Act*. https://ssrn.com/abstract=2956308https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4387612Electroniccopyavailableat:https://ssrn.com/abstract=4387612

BBC News Mundo. (2024, febrero 22). *Título del artículo exacto en cursiva*. BBC. https://www.bbc.com/mundo/articles/c1d3y7nedv6o

Bercovich, N., Fernández, A., Hofman, A., Jordán, V., Peres, W., Porcile, G., Rojas, F., Stojkovic, G., Stumpo, G., & Sunkel, G. (2013). *The digital economy for structural change and equality*. http://www.cepal.org/socinfo.

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke, D. G., Piccarreta, B., & Scarfone, K. (2021). *Consideraciones para la gesti n de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)*. https://doi.org/10.6028/NIST.IR.8228es

Bühler, M. M., Calzada, I., Cane, I., Jelinek, T., Kapoor, A., Mannan, M., Mehta, S., Mookerje, V., Nübel, K., Pentland, A., Scholz, T., Siddarth, D., Tait, J., Vaitla, B., & Zhu, J. (2023). Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data

Sovereign, Innovative and Equitable Digital Communities. *Digital*, *3*(3), 146-171. https://doi.org/10.3390/digital3030011

Carrière-Swallow, Y., & Haksar, V. (2019). *The Economics and Implications of Data: An Integrated Perspective Strategy, Policy, and Review Department*. www.imfbookstore.org

Castro, A. (2015). Autoría y titularidad en el derecho de autor.» Informática Jurídica: Trabajos. 1 de Enero. http://www.informatica- juridica.com/trabajos/autoria-y-titularidad-en-el-derecho-de-autor/.

Centers for Disease Control and Prevention. (2022, November 3). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. CDC. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

Chui Michael, Collins Mark, & Patel Mark. (2021). *The Internet of Things: Catching up to an accelerating opportunity*.

Corrado, C., Haskel, J., Iommi, M., & Jona-Lasinio, C. (2022). Measuring data as an asset: Framework, methods and preliminary estimates. *OECD Working Papers*. https://doi.org/10.1787/b840fb01-en

Corrado, C., Haskel, J., & Jona-Lasinio, C. (2024). *Data, Intangible Capital, and Productivity**.

Coyle, D., & Diepeveen, S. (2021). Creating and governing social value from data. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3973034

Coyle, D., & Manley1, A. (2022). *What is the Value of Data? A review of empirical methods*.

Cruz, E. (16 de agosto del 2024) Gestión de flota: Sistemas de control y monitoreo para equipos de minería. Revista Rumbo Minero, Consultado en página web: https://www.rumbominero.com/revista/gestion-de-flota-sistemas-de-control-y-monitoreo-para-equipos/

Cajahuaringa, Z. (2024, abril 22). *Tecnología para una minería inteligente*. Rumbo Minero. https://www.rumbominero.com/peru/noticias/mineria/tecnologia-mineria-inteligente/

Cordero, E. (2020). *Estudios sobre propiedad y derecho urbanístico*. Tirant Lo Blanch.

Congreso de la República del Perú. (2011). *Ley N.º 29733, Ley de Protección de Datos Personales*. Diario Oficial El Peruano. https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20Nº%2029733.pdf.pdf?v=1618338779

Deloitte. (2021). *La Minería Inteligente y Operaciones Integradas: Visiones del futuro de la Minería*.

Determann, L. (2019). No One Owns Data. En *Hastings Law Journal* (Vol. 70).

Device Authority. (s/f). *Unpacking IoT Architecture: Symmetric Encryption, Layers and Components Explained - Device Authority*. Recuperado el 23 de septiembre de 2024, de https://deviceauthority.com/unpacking-iot-architecture-layers-and-components-explained/#

De Hert, P., & Gutwirth, S. (2006). *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power*. In *Privacy and the criminal law*.
Weber, R. H. (2013). *Internet of Things – New security and privacy challenges*. *Computer Law & Security Review*, 26(1), 23–30.

Díaz Vera, L. M. (2023). Non-Personal Data Regulation - A Latin American Perspective. *GRUR International*, *72*(1), 37–53. https://doi.org/10.1093/grurint/ikac123

Diez Canseco, L. J. (2012). Teoría del Cuello de Botella: Las Facilidades Esenciales. *Themis*, *61*, 65–93.

Drexl, J. (2018). *Data Access and Control in the Era of Connected Devices*.

Dulong de Rosnay, M., & Stalder, F. (2020). Digital commons. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1530

Eckardt, M., & Kerber, W. (2024). Property rights theory, bundles of rights on IoT data, and the EU Data Act. *European Journal of Law and Economics*. https://doi.org/10.1007/s10657-023-09791-8

Eger, T., & Scheufen, M. (2024). The law and economics of the data economy: introduction to the special issue. *European Journal of Law and Economics*, *57*(1–2), 93–111. https://doi.org/10.1007/s10657-024-09796-x

El-Khoury, M., & Arikan, C. L. (2021). From the internet of things toward the internet of bodies: Ethical and legal considerations. *Strategic Change*, *30*(3), 307–314. https://doi.org/10.1002/jsc.2411

Esposito, M. & Araral, E. (2025, 4 de marzo). *Bienes comunes digitales: cómo aprovechar blockchain para una mejor gobernanza*. Foro Económico Mundial. https://es.weforum.org/stories/2025/03/bienes-comunes-digitales-como-aprovechar-blockchain-para-una-mejor-gobernanza/

European Commision. (n.d.). *Public Consultation on Data Act and amended rules on the legal protection of Databases*.

European Commision (2024). *EU Data Act: Focus Areas Data Act Entities Within Scope Covered Data*.

Foro Económico Mundial. (2024, enero). *China's data and AI approach is changing – here's what that means*. World Economic Forum. https://www.weforum.org/stories/2024/01/chinas-data-and-ai-approach-is-changing-heres-what-that-means/

Federal Trade Commission. (n.d.). *Children's Online Privacy Protection Rule (COPPA)*. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Federal Trade Commission. (n.d.). *Gramm-Leach-Bliley Act*. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Frischmann, B. M., Madison, M. J., & Strandburg, K. J. (Eds.). (2014). *Governing knowledge commons*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199972036.001.0001

García de Enterría, E. (2001). La titularidad de los derechos fundamentales. *Revista Española de Derecho Constitucional*, 21(63), 9-40. https://www.redalyc.org/pdf/820/82010110.pdf

Graux, H. (2024). *What is data ownership, and does it still matter under EU data law?* https://doi.org/10.2830/052185

Graef, I., & Husovec, M. (2022). Seven things to improve in the Data Act. *Journal of European Consumer and Market Law, 11*(5), 201–206.

Haqiq, N., Zaim, M., Bouganssa, I., Salbi, A., & Sbihi, M. (2022). AIoT with I4.0: the effect of Internet of Things and Artificial Intelligence technologies on the industry 4.0. *ITM Web of Conferences*, *46*, 03002. https://doi.org/10.1051/itmconf/20224603002

Hanisch, R., Kaiser, D., Yuan, A., Medina-Smith, A., Carroll, B., & Campo, E. (2024). *NIST Research Data Framework (RDaF)*. https://doi.org/10.6028/NIST.SP.1500-18r2

Herke Kranenborg, O. Lynskey (2016), *The Foundations of EU Data Protection Law*, *International Data Privacy Law*, Volume 6, Issue 4, November 2016, Pages 324–326, https://doi.org/10.1093/idpl/ipw017

Heverly, R. A. (2003). *THE INFORMATION SEMICOMMONS*.

Huang, J. (Jeanne). (2024). The rise of data property rights in China: how does it compare with the EU data act and what does it mean for digital trade with China? *Journal of International Economic Law*. https://doi.org/10.1093/jiel/jgae032

IBM. (s.f.). *Inteligencia artificial*. https://www.ibm.com/mx-es/topics/artificial-intelligence

ICC Policy Primer on Non-Personal Data. (2023). iccwbo.org/news-publications/policies-reports/ICC-policy-primer-on-non-personal-data/

Javaid, M., Haleem, A., Singh, R. P., & Sinha, A. K. (2024). Digital economy to improve the culture of industry 4.0: A study on features, implementation and challenges. *Green Technologies and Sustainability*, *2*(2), 100083. https://doi.org/10.1016/j.grets.2024.100083

Kerber, W. (2016). *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*. https://ssrn.com/abstract=2858171http://www.uni-marburg.de/fb02/makro/forschung/magkspapershttps://ssrn.com/abstract=2858171Electroniccopyavailableat:https://ssrn.com/abstract=2858171

Kerber, W. (2019). *Data-sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars*.

Kerber, W. (2023). Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives. *GRUR International*, *72*(2), 120–135. https://doi.org/10.1093/grurint/ikac107

Kerber, W. (2024). EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation? *Journal of Antitrust Enforcement*, *12*(2), 234–240. https://doi.org/10.1093/jaenfo/jnae011

Kerber, W. (2023). The EU Data Act and the Reconfiguration of the European Data Economy. *European Law Review, 48*(1), 3–24.

Kresalja Rosselló, B., & Quintana Sánchez, E. (n.d.). Prueba 01.

Klippa. (2023). *¿Qué es la anonimización de datos? Protege tus datos*. https://www.klippa.com/es/blog/informativo/anonimizacion-datos/#

Lakhwani, K., Gianey, H., Kofi Wireko, J., & Kant Hiran, K. (2020). *Internet of Things (IoT): Principles, Paradigms and Applications of IoT*. BPB Publications.

La Diega, G. N. (2022). Internet of things and the law: Legal strategies for consumer-centric smart technologies. En *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies*. Taylor and Francis.

Legchekov, S. (2022, agosto). *IoT in Supply Chain Management and Logistics: an Overview*. https://www.scnsoft.com/blog/iot-scm-and-logistics

López, M. M. F. MARGARITA ROBLES CARRILLO, El modelo digital europeo. Tirant lo Blanch, 2025, por Mercedes Fuertes López. *Revista de Derecho Comunitario Europeo*, (81), 379-384

Leistner, M., & Antoine, L. (2022). *Attention, here comes the EU Data Act!* https://www.bmi.bund.de/EN/

Maharana, K., Mondal, S., & Nemade, B. (2022). A review: Data pre-processing and data augmentation techniques. *Global Transitions Proceedings, 3*(1), 91–99. https://doi.org/10.1016/j.gltp.2022.04.020

Mendoza Del Maestro, G. (n.d.). *Apuntes sobre el Derecho de Propiedad a partir de sus Contornos Constitucionales*. www.revistas.uchile.cl/index.php/RCHD/article/viewPDFInterstitial/5138/5022.

Minero, G. (2021). Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 733–756.

Molaei, F., Rahimi, E., Siavoshi, H., Ghaychi Afrouz, S., & Tenorio, V. (2020). A Comprehensive Review on Internet of Things (IoT) and its Implications in the Mining. *Industry. American Journal of Engineering and Applied Sciences*, *2020*(3), 499–515. https://doi.org/10.3844/ajeassp.2020.499.515ï

Mylly, U. M. (2024). Trade Secrets and the Data Act. *IIC International Review of Intellectual Property and Competition Law*, *55*(3), 368–393. https://doi.org/10.1007/s40319-024-01432-0

Nanda, A., & Kapoor, A. (2021). *Understanding Non-Personal Data Sharing A Principle First Approach*.

Nestor Duch-Brown, Bertin Martens, & Frank Mueller-Langer. (2017). The economics of ownership, access and trade in digital data. *European Commission.*

NS Energy. (2022). World Mining Frontiers. *Volume 2*.

OECD, O. for E. C. and Development. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being*. OECD.

Ochoa, H. (2023). *Bienes*. Themis

Organización Mundial de la Propiedad Intelectual. (2016). *Principios básicos del derecho de autor y los derechos conexos* (2.ª ed.). https://doi.org/10.55685/wipo_pub_909_2016

Parlamento Europeo y Consejo de la Unión Europea. (2023). *Reglamento (UE) 2023/2854 sobre normas armonizadas para el acceso y uso de datos*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/eli/reg/2023/2854

Presidencia del Consejo de Ministros. (2024). *Decreto Supremo N.º 009-2024-JUS, que modifica el Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales*. Diario Oficial El Peruano. https://busquedas.elperuano.pe/dispositivo/SE/2349653-1

Presidencia del Consejo de Ministros, Secretaría de Gobierno y Transformación Digital. (2025). *Estrategia Nacional de Gobierno de Datos* 2026-2030 [Documento de trabajo en versión preliminar]. Gobierno del Perú. https://cdn.www.gob.pe/uploads/document/file/8572678/7097112-estrategia-nacional-de-gobierno-de-datos.pdf?v=1756498854

Ravina Sánchez, R. (1998). El Sistema de Clasificación de los Bienes y su Importancia para el Derecho Civil Patrimonial. *Derecho & Sociedad*, (13), 182–194. Recuperado a partir de https://revistas.pucp.edu.pe/index.php/derechoysociedad/article/view/16659

Ryan, M., Atik, C., Rijswijk, K., & otros. (2024). *The future of agricultural data-sharing policy in Europe: Stakeholder insights on the EU Code of Conduct*. *Humanities and Social Sciences Communications, 11*, 1197. https://doi.org/10.1057/s41599-024-03710-1

Rendondo. (2024, 20 de septiembre). Protección de datos en Estados Unidos: ¿Cómo afecta a tu negocio? *Mailjet Blog*. Recuperado de https://www.mailjet.com/es/blog/emailing/proteccion-de-datos-eeuu/

Puyol, F. (2015). *Aproximación jurídica y económica al Big Data (p.335-355)*. Tirant Lo Blanch.

Rubinfeld, D. (2024a). Data portability and interoperability: An E.U.-U.S. comparison. *European Journal of Law and Economics*, *57*(1–2), 163–179. https://doi.org/10.1007/s10657-023-09781-w

Saraf, K., & Katare, J. (2023). *Data as an essential facility: Understanding the flipside*. CBCL Blog. Centro de Estudios en Derecho de la Competencia, National Law University India. Recuperado de https://cbcl.nliu.ac.in/competition-law/data-as-an-essential-facility-understanding-the-flipside/

Selvi, M., & Periasamy, J. K. K. (2020). Analysis of Artificial Intelligence of Things. *International Journal of Electrical Engineering and Technology*, *11*(4), 275–280. http://www.iaeme.com/ijeet/issues.asp?JType=IJEET&VType=11&IType=4http://www.iaeme.com/IJEET/issues.asp?JType=IJEET&VType=11&IType=4

Singh, P. J., & Gurumurthy, A. (2021). *Economic Governance of Data Balancing individualist-property approaches with a community rights framework*.

Smith, S., & Moore John. (2018). *What is OEM (original equipment manufacturer)? | Definition from TechTarget*. https://www.techtarget.com/searchitchannel/definition/OEM

Specht-Riemenschneider, L. (2023). Balancing openness and incentives in the Data Act: The challenge of user empowerment. *Computer Law & Security Review, 50*, 105764.

Supriyadi, D. (2023). The Regulation of Personal and Non-Personal Data in the Context of Big Data. *Journal of Human Rights, Culture and Legal System*, *3*(1), 33–69. https://doi.org/10.53955/jhcls.v3i1.71

Tarkowski, A., & Vogelezang, F. (2021). *The argument against property rights in data. Open Future Policy brief #1*.

Ternera Barrios, F., & Mantilla Espinosa, F. (2006). El concepto de derechos reales. *Revista de Derecho Privado*, (10), 3–37. Universidad del Rosario. https://revistas.urosario.edu.co/index.php/privado/article/view/99

The Open Group. (2014). *The Exploration & Mining Business Capability Reference Map: Concepts and Definitions*. www.opengroup.org/bookstore.

Tiao, S. (2024, marzo 11). *¿Qué es Big Data? | Oracle Perú*. Oracle Website. https://www.oracle.com/pe/big-data/what-is-big-data/

Tribunal Constitucional del Perú. (2021). *Sentencia recaída en el expediente N.° 02140-2020-HD/TC*. https://tc.gob.pe/jurisprudencia/2021/02140-2020-HD.pdf

Tribunal Constitucional del Perú. (2007). *Sentencia Exp. N.° 0003-2007-PC/TC*.

Tribunal Constitucional de España. (2000). *Sentencia 292/2000, de 30 de noviembre*. Recurso de amparo 2372/1993. Boletín Oficial del Estado, (7), 429–439. https://hj.tribunalconstitucional.es/es/Resolucion/Show/4122.

Tribunal Constitucional del Perú. (2022). *Sentencia 02839-2021-HD/TC*. https://tc.gob.pe/jurisprudencia/2022/02839-2021-HD.pdf

Unpacking IoT Architecture: Layers and Components Explained - Device Authority. (s/f). Recuperado el 8 de julio de 2024, de https://deviceauthority.com/unpacking-iot-architecture-layers-and-components-explained/#

Van Asbroeck, B., Debussche, J., & César, J. (2017). *Building the European Data Economy Data Ownership*. http://www.toreador-project.eu/.

Valero, J. (2022). *El régimen jurídico de los datos de alto valor: dificultades y retos para su aplicación práctica.* En R. Martínez & J. Valero, Datos Abiertos y reutilización de la información del sector público (pp.81-102). Editorial Comares

Verma, A., & Gurtoo, A. (2021). *Evaluating global data policies around non-personal data*.

Information Commissioner's Office*. What is personal data?* (2023). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/

Wiebe, A. (2017). Protection of industrial data - A new property right for the digital economy? En *Journal of Intellectual Property Law and Practice* (Vol. 12, Número 1, pp. 62–71). Oxford University Press. https://doi.org/10.1093/jiplp/jpw175

Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. (2016). *The FAIR Guiding Principles for scientific data management and stewardship*. Science Data 3, 160018. https://doi.org/10.1038/sdata.

Xia, L., Baghaie, S., & Mohammad Sajadi, S. (2024). The digital economy: Challenges and opportunities in the new era of technology and electronic communications. *Ain Shams Engineering Journal*, *15*(2). https://doi.org/10.1016/j.asej.2023.102411

Zegarra, D. (2019). La normativa peruana de protección de datos personales frente al reto de pasar de un modelo de gestión de datos al uso responsable de la información. En *La proyección de Derecho Administrativo Peruano. Estudios por el Centenario de la Facultad de Derecho de la PUCP*. (pp. 165 - 210). LIMA. Palestra. Recuperado de: https://palestraeditores.com/producto/la-proyeccion-del-derecho-administrativo-peruano/

Zvarivadza, T., Onifade, M., Dayo-Olupona, O., Said, K. O., Githiria, J. M., Genc, B., & Celik, T. (2024). On the impact of Industrial Internet of Things (IIoT) - mining sector perspectives. *International Journal of Mining, Reclamation and Environment*. https://doi.org/10.1080/17480930.2024.2347131

Perú. Congreso de la República. (2018). *Decreto Legislativo N.º 1412, Ley de Gobierno Digital*. Diario Oficial *El Peruano*, 13 de setiembre de 2018.

Perú. Presidencia del Consejo de Ministros. (2021). *Decreto Supremo N.º 029-2021-PCM, que aprueba el Reglamento de la Ley de Gobierno Digital*. Diario Oficial *El Peruano*, 2 de diciembre de 2021.

Perú. Presidencia del Consejo de Ministros. (2023). *Decreto Supremo N.º 085-2023-PCM, que aprueba la Política Nacional de Transformación Digital al 2030*. Diario Oficial *El Peruano*, 27 de agosto de 2023.

Perú. Presidencia del Consejo de Ministros. (2025). *Documento de trabajo de la Estrategia Nacional de Gobernanza de Datos 2026-2030*. Documento de trabajo. Recuperado de https://www.gob.pe/

Perú. Congreso de la República. (2018). *Decreto Legislativo Nº 1412, Ley de Gobierno Digital*. Diario Oficial *El Peruano*, 13 de setiembre de 2018.

Perú. Congreso de la República. (2011). *Ley Nº 29733, Ley de Protección de Datos Personales*. Diario Oficial *El Peruano*, 3 de julio de 2011.

Perú. Ministerio de Justicia y Derechos Humanos. (2024). *Decreto Supremo Nº 016-2024-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales*. Diario Oficial *El Peruano*, 30 de junio de 2024.

Perú. Presidencia de Consejo de Ministros. (2025). Decreto Supremo Nº115-2025-PCM, que aprueba el Reglamento de la Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país.

Unión Europea. (2018). *Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para el libre flujo de datos no personales en la Unión Europea*.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura - UNESCO (2022). Recomendaciones sobre la ética de la inteligencia artificial. Consultado en: https://unesdoc.unesco.org/ark:/48223/pf0000381137