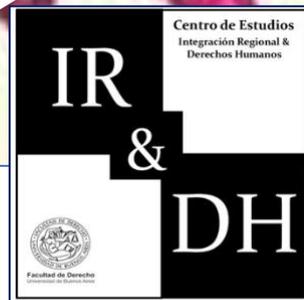


# Integración Regional & Derechos Humanos / Revista Regional Integration & Human Rights / Review

Año XIII – N° 1 – 1° semestre 2025



# Integración Regional & Derechos Humanos /Revista Regional Integration & Human Rights /Review

Revista del Centro de Estudios  
Integración Regional & Derechos Humanos  
Facultad de Derecho  
Universidad de Buenos Aires – Argentina

Año XIII – N°1 – Primer Semestre 2025

**ISSN: 2346-9196**

Av. Figueroa Alcorta 2263 (C1425CKB)  
Buenos Aires - Argentina  
revistairydh@derecho.uba.ar

Se permite la copia o redistribución parcial de la presente obra exclusivamente haciendo referencia a la revista, con indicación del nombre, número, año de publicación, nombre del autor o autora y nombre del artículo original, indicando asimismo la fuente con un hipervínculo operativo que conduzca al sitio web oficial de la revista. Asimismo, debe dejarse constancia de cualquier cambio que se haya introducido al contenido. Fuera de este supuesto, la revista se reserva todos los derechos. Por consultas dirigir la correspondencia epistolar o digital a las direcciones indicadas.

## **DIRECTOR**

CALOGERO PIZZOLO

Catedrático *Jean Monnet* (Universidad de Buenos Aires, Argentina)

## **CONSEJO ACADÉMICO**

PAOLA ACOSTA (Universidad del Externado de Colombia, Colombia)

JOSÉ MARÍA SERNA (Universidad Nacional Autónoma de México, México)

JAVIER PALUMMO (Universidad de la República, Uruguay)

CARLOS FRANCISCO MOLINA DEL POZO (Universidad de Alcalá de Henares,  
España)

MARCELLO DI FILIPPO (Universidad de Pisa, Italia)

ROBERTO CIPPITANI (Universidad de Perugia, Italia)

JAVIER GARCÍA ROCA (Universidad Complutense de Madrid, España)

LAURENCE BURGORGUE LARSEN (Universidad de París I, Francia)

LAURA MONTANARI (Universidad de Udine, Italia)

VALENTINA COLCELLI (Consiglio Nazionale delle Ricerche, Italia)

FABRIZIO FIGORILLI (Universidad de Perugia, Italia)

PABLO PODADERA RIVERA (Universidad de Málaga, España)

JOSÉ MARÍA PORRAS RAMÍREZ (Universidad de Granada, España)

ALFREDO SOTO (Universidad de Buenos Aires, Argentina)

SANDRA NEGRO (Universidad de Buenos Aires, Argentina)

## **CONSEJO EDITORIAL**

ANDREA MENSA GONZÁLEZ (Universidad de Buenos Aires, Argentina)

MIGUEL ÁNGEL SEVILLA DURO (Universidad de Castilla-La Mancha, Albacete,  
España)

## **COORDINACIÓN**

NATALÍ PAVIONI

## **EDICIÓN**

GUILLERMO ALVAREZ SENDON

# Índice

## **Estudios / Debates**

*Mentiras digitales y “contaminación” del debate público en procesos electorales. Inteligencia Artificial (IA), libertad de expresión y sociedad democrática desde un enfoque europeo* 5  
CALOGERO PIZZOLO

## **Sección Especial “Derecho, IA y nuevas tecnologías” /**

*Algunos Problemas Jurídicos Del Uso De Los Datos En La Economía Digital* 55  
ROBERTO CIPPITANI & MARÍA ISABEL CORNEJO PLAZA

*Entre Tecnofilia y Tecnofobia: la prudencia del jurista* 88  
IAN HENRÍQUEZ HERRERA

*De la formación clásica al contrato digital: evolución histórica-jurídica de la oscuridad contractual* 102  
EDUARDO RIVERA CARRASCO, EDUARDO RODRÍGUEZ ÁLVAREZ & VÍCTOR JAURE CATALDO

*Introducción al legal TECH: algunas notas preliminares para su estudio* 126  
RUBÉN MÉNDEZ REÁTEGUI & EDUARDO BERNARDO MORALES BARRA

*¿Puede una IA ser su Señoría Ilustrísima? un estudio exploratorio sobre el rol que le cabe a las nuevas tecnologías en la función jurisdiccional* 143  
VALERIA GAJARDO GONZÁLEZ, LUISA QUIMBAYO OCAMPO & DAVID DOMÍNGUEZ HUENCHO

*El derecho humano a la ciberseguridad en la Unión Europea: desafíos de implementación e interrelaciones con los derechos fundamentales* 168  
JULIANA ESTÉVEZ

*La IA como un nuevo territorio de disputa: omisiones y sesgos en clave de género y desigualdad* 186  
AGOSTINA A. LÓPEZ & IRALA GONZÁLEZ OLIVIA R.

*La inteligencia Artificial y el derecho humano a la Buena Administración* 210  
ANDREA MENSA GONZÁLEZ

## **Doctrina /**

*El derecho a la vivienda adecuada en el Derecho Internacional de los Derechos Humanos* 238  
CAMILA F. SCAGNETTI

*Núcleo e Identidad Constitucional a la luz de los principios y valores constitucionales básicos, su protección a través de las limitantes a las reformas constitucionales en sede internacional* 265  
SILVERIO RODRÍGUEZ CARRILLO

*Reflexiones acerca de la criminalización de la migración en el Cono Sur. Cuerpos racializados, género y tensiones con la integración regional* 294  
ÁNGELES BELÉN FREZZA

*Integración regulatoria sanitaria como estrategia de autonomía periférica: el caso de la investigación clínica en América Latina* 316

MARÍA AZUL MARTÍNEZ GONZÁLEZ

### **Recensión de libros /**

*Las relaciones entre las integraciones económicas y sus estados parte un estudio desde la teoría federal, recensión del libro de Sevilla Duro, M. Á. (2025). Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza* 336

CARLOS MARIANO LISZCZYNSKI

*La Carta de Derechos Fundamentales de la Unión Europea. Quince años de jurisprudencia, recensión del libro de López Castillo, A. (Dir.), & Martínez Alarcón, M. L. (Coord.). (2025). (2.ª ed.). Tirant lo Blanch, Valencia.* 341

NATALÍ PAVIONI

### **Jurisprudencia /**

#### **Corte Interamericana de Derechos Humanos:**

*Reseña de jurisprudencia primer semestre 2025*

JONATHAN FERRARI, LAURA BARROS BARRIENTOS, EMMA SOSA LIUT, AGUSTINA CABRERA & ULISES FURUKAWA AKIZAWA 355

#### **Tribunal de Justicia de la Unión Europea:**

*Reseña de jurisprudencia primer semestre 2025*

SOFIA TONELLI 413

**Sección Especial /**  
*“Derecho, IA y nuevas  
tecnologías”*

Fecha de recepción: 30 de junio de 2025<sup>4</sup>

Fecha de aceptación: 10 de julio de 2025

## Resumen

El presente artículo examina los desafíos jurídicos que plantea la economía digital en relación con la definición, clasificación y regulación de los datos, tanto personales como no personales, a los que se hace referencia como el «oro» o el «petróleo» del siglo XXI. En un contexto en el que los datos tienen una creciente relevancia económica y social, la Unión Europea, los países latinoamericanos y organizaciones internacionales como la OCDE, la OMS y la UNESCO han adoptado fuentes jurídicas que ponen de manifiesto la existencia de vacíos normativos y dificultades conceptuales, como la indefinición jurídica del término «dato», la ambigüedad entre datos personales y no personales, y la insuficiencia de las normas actuales (como el RGPD) para hacer frente a fenómenos como la inteligencia artificial o las neuro tecnologías. Además, se cuestiona la aplicabilidad del régimen tradicional de propiedad civil sobre los datos y se propone un enfoque alternativo en el que se privilegia la gobernanza colaborativa, el acceso abierto y el interés colectivo. El artículo concluye proponiendo la construcción de un nuevo estatuto jurídico para

---

<sup>1</sup> El presente trabajo se enmarca dentro de las actividades del Módulo Jean Monnet “e-Ride” (*Ethics and Research Integrity in the Digital Age*)(2024-2027), financiado por la UE, Programa Erasmus+, Grant Agreement no. 101175756 y del Laboratorio de Innovación, Tecnologías y Fronteras de las Ciencias Jurídicas del Doctorado de la Universidad Autónoma de Chile, Proyecto ANID código 8622004.

<sup>2</sup>Co-Director de la Cátedra ISAAC (Individual Rights in Scientific Research and Cooperation) de la Universidad Nacional de Educación a Distancia (Madrid); Profesor titular del Instituto Nacional de Estudios Superiores en Ciencias penales (México) y de la Escuela Judicial del Poder Judicial del Estado de Oaxaca (México)

<sup>3</sup> Coordinadora académica del Módulo Jean Monnet e-Ride (*Ethics and Research Integrity in the Digital Age*); Directora de los grupos de IA y D y de Neurometa, Grupo de Investigación en Neuroderechos, Inteligencia Artificial y Metaverso y Directora del Laboratorio de Innovación, Tecnologías y Fronteras de las ciencias jurídicas de la Universidad Autónoma de Chile.

<sup>4</sup> Ponencia presentada en las “I Jornadas Internacionales sobre Derecho y Nuevas Tecnologías” que tuvieron lugar en la Facultad de Derecho de la Universidad de Buenos Aires los días 7 y 8 de mayo pasado.

los datos, adecuado a su función en la economía digital y coherente con los valores fundamentales.

*Palabras clave: Inteligencia artificial, neurotecnologías,*

**Title:** SOME LEGAL ISSUES REGARDING THE USE OF DATA IN THE DIGITAL ECONOMY

**Abstract**

The article examines the legal challenges posed by the digital economy in relation to the definition, classification and regulation of data, both personal and non-personal, referred to as the “gold” or “oil” of the 21st century. In a context where data is becoming increasingly important economically and socially, the European Union, Latin American countries and international organisations such as the OECD, WHO and UNESCO have adopted legal sources that highlight the existence of regulatory gaps and conceptual difficulties, such as the legal vagueness of the term “data”, the ambiguity between personal and non-personal data, and the inadequacy of current rules (such as the GDPR) to deal with phenomena such as artificial intelligence and neurotechnologies. In addition, the applicability of the traditional civil property regime to data is questioned and an alternative approach is proposed that privileges collaborative governance, open access and the collective interest. The article concludes by proposing the construction of a new legal status for data, appropriate to its role in the digital economy and consistent with fundamental values.

*Keywords: Artificial Intelligence, Neurotechnologies*

**Sumario:** I. Contexto. II. Fuentes de las Organizaciones internacionales sobre la circulación de datos. III. Disciplinas jurídicas sobre los datos personales y no personales. IV. Libertad de circulación de los datos y sus límites. V. Problemas jurídicos de la disciplina jurídica de los datos. V.i. Definición e clasificación de los datos. V.ii. Indiferencia de los contenidos y neutralidad tecnológica. V.iii. Insuficiencia de las disciplinas sobre los datos personales para proteger todos los otros derechos e intereses fundamentales. VI. Cuestiones sobre los derechos y las relaciones jurídicas concernientes los datos. VI.i. Sujetos y obligaciones. VI.ii. Datos

y bienes. VI.iii. Datos y contratos. VII. Relevancia jurídica de los datos: necesidad de garantizar la calidad de los datos. VIII. Intereses colectivos y bienes comunes. IX. Gobernanza de la economía digital. X. Bibliografía.

## I. Contexto

Según el informe “Estudio sobre el mercado europeo de datos 2024-2026” de la COMISIÓN EUROPEA (2024), la “economía de datos” se puede definir como el impacto global del mercado de datos en la economía en su conjunto, que incluye la generación, recopilación, almacenamiento, procesamiento, distribución, análisis, elaboración, entrega y explotación de datos brindados por las tecnologías digitales (LÓPEZ SABATER: 2017, p. 23). Ella sola valió UE+UK 814,544 billones de euro en el 2024, mientras que en el 2030 se espera que la economía de datos (siempre en Europa) supere el valor de 1100 billones de euros.

Solo el valor del mercado de los datos ha sido de 90,036 billones millones de euros en el 2024 y se prevé que alcance los 100 billones en el 2025. En EE. UU. dicho mercado es cuatro veces los de la EU.

El sitio web “Statista” estima que la esfera de datos global crecerá hasta los 51 zettabytes para 2025<sup>5</sup>. Se prevé que la economía “ecodigital global” (la combinación de ecología y digitalización) duplique su tamaño, pasando de 16,6 billones de dólares en 2023 a casi 32,9 billones de dólares en 2028, un crecimiento superior al 98% (CONSULTANCY.EU: 2024).

Dada la importancia de la economía digital, se habla de los datos como el “nuevo petróleo” o el “nuevo oro” y se utilizan expresiones como “fiebre del oro contemporánea” para indicar la relevancia geopolítica de controlar la producción y el uso de los datos.

Pero los datos son cruciales no solo desde el punto de vista económico, sino también debido a su relevancia social y su impacto en actividades como cultura, salud, educación, justicia, laboral, seguridad, investigación entre otros.

En la era digital, los datos y la información constituyen el principal activo económico, pero, por otro lado, su recopilación, procesamiento y circulación han

---

<sup>5</sup> Un zettabyte corresponde a 1021 bytes, o 1 000 000 000 000 000 000 000 (un trillón) de bytes

evolucionado a tal magnitud con la ayuda de las tecnologías, especialmente con la irrupción de la Inteligencia Artificial y las neurotecnologías, que han desafiado a la legislación existente en algunos países (por ejemplo, en la Unión Europea y en muchos países latinoamericanos como Chile) que no se ajustan todavía a estos cambios.

## **II. Fuentes de las Organizaciones internacionales sobre la circulación de datos**

Las principales organizaciones internacionales han desarrollado marcos, principios y políticas para regular y facilitar la circulación de datos personales y no personales, buscando equilibrar la protección de derechos fundamentales con la promoción de la innovación, la cooperación internacional y el desarrollo económico.

La OCDE ha sido pionera en establecer directrices internacionales sobre la protección de la privacidad y los flujos transfronterizos de datos personales. Sus “Directrices sobre la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales” (1980, revisadas en 2013) identifican principios como la limitación de la recogida, calidad de los datos, especificación del propósito, limitación del uso, salvaguardias de seguridad, apertura, participación individual y responsabilidad.

La OCDE también promueve el acceso y el intercambio de todo tipo de datos (personales, no personales, abiertos, privados, públicos) para maximizar beneficios sociales y económicos, siempre bajo principios de confianza, interoperabilidad y protección adecuada según el contexto del dato.

Aunque la Organización Mundial de Comercio (OMC) no tenga directrices específicas sobre protección de datos, sus fuentes destacan la importancia de los flujos transfronterizos de datos para el comercio digital. Los debates en la OMC giran en torno a cómo facilitar estos flujos respetando las regulaciones nacionales sobre privacidad y protección de datos, buscando evitar barreras innecesarias al comercio electrónico, pero permitiendo excepciones legítimas por motivos de protección de datos personales.

Por su parte la OMS (Organización Mundial de la Salud) adoptó en 2024 una Política de Protección de Datos Personales que establece principios con el fin de

regular la recolección, análisis, publicación y transferencia de datos personales, especialmente de salud.

UNESCO, como agencia de la ONU, aplica principios específicos para el procesamiento de datos personales: procesamiento justo y legítimo (con consentimiento, interés superior del titular o mandato institucional), especificación de propósito, proporcionalidad y necesidad, transparencia, transferencias seguras y rendición de cuentas. UNESCO puede transferir datos a terceros si garantiza protección adecuada, y mantiene mecanismos internos de supervisión y respuesta ante consultas o incidentes.

### **III. Disciplinas jurídicas sobre los datos personales y no personales**

Desde el punto de vista normativo, los sistemas jurídicos de Europa y Latinoamérica, más que otros continentes, están adoptando, de manera convergente, fuentes jurídicas para disciplinar el uso de los datos (CIPPITANI & CORNEJO-PLAZA, 2025).

En Europa, hace unas décadas, se está elaborando una disciplina jurídica sobre ese tema, sea en el ámbito del Consejo de Europa y, sobre todo, en el Derecho de la Unión Europea. En ese sistema jurídico, la protección de los datos personales como un derecho fundamental (véanse los artículos 2, 6 y 21 del Tratado de la Unión Europea, así como el artículo 8 Carta de los Derechos Fundamentales de la Unión Europea) reglado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante “GDPR” desde el acrónimo en inglés por “General Data Protection Regulation”).

En América Latina, al no existir una integración como la de la UE la situación es obviamente más fragmentada desde el punto de vista normativo. Por ejemplo, en México la Constitución reconoce el derecho al “habeas data” (véase los artículos 6 y 16) y una Ley Federal de Protección de Datos Personales en Posesión de Particulares de 2010 (LFPDPPP) y su Reglamento de 2011 regla la protección de datos personales. La reforma constitucional del 2014 ha establecido un Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

(véase el artículo 6, párr. A, fracción VIII). Otros países de América Latina han adoptado medidas legislativas y organizativas que prevén el “habeas data” para proteger los datos personales, como, por ejemplo: Argentina (véase la Ley de Protección de Datos Personales 25.326 del 2000 y la Agencia de Acceso a la Información Pública, Provisión 60-E/2016), Colombia (véase el artículo 15 de la Constitución Política de Colombia y la Ley 1581 de 2012; la Superintendencia de Industria y Comercio (SIC) está facultada para ejercer la vigilancia); Brasil (Ley 13.709 del 2018 o LGPD; se ha establecido una Autoridad Nacional de Proteção de Dados o “ANPD”, por la Medida Provisoria 869/18 ); Uruguay (véase la Ley N° 18331 del 2008); en Chile, la Ley de Protección de Datos Personales está regulada por la Ley 21.719, publicada el 13 de diciembre de 2024 con vigencia diferida para el 2026. Esta ley crea la Agencia de Protección de Datos Personales (APPD). Además, existe la reforma constitucional del año 2018, Ley No. 21.096, que modificó el artículo 19 No. 4 de la Constitución Política de la República que consagra el derecho a la protección de datos personales o autodeterminación informativa como un derecho independiente del derecho a la vida privada.

La UE, desde la década de los años '90, ha ido elaborando una estrategia política y una disciplina jurídica sobre los datos que incluye también los datos no personales.

En un primer momento las fuentes europeas han planteado la construcción de una “sociedad del conocimiento” (*“Knowledge-based society”* véase el documento “Crecimiento, competitividad y empleo” de 1995; la Estrategia de Lisboa de 2000; “Europa 2020” de 2010) es decir una sociedad-economía basada en el conocimiento, que es el producto del uso de las Tecnologías de la Información y la Comunicación (TIC), de manera coherente con los valores europeos como la dignidad, la solidaridad y la protección del medio ambiente.

En el nuevo milenio, la Comisión ha elaborado una estrategia enfocada sobre los datos y las tecnologías digitales, en el ámbito de documentos como “*2030 Digital Compass: the European way for the Digital Decade*”, de 2021; *Shaping Europe's digital future*” de 19 de febrero de 2020; “*Digitising European Industry Reaping the full benefits of a Digital Single Market*”, de 19 de abril de 2016, sobre el establecimiento de un mercado único digital.

Además, el 19 de febrero de 2020, la Comisión Europea ha publicado una comunicación titulada “Una estrategia europea para los datos”, que forma parte de un paquete más amplio de documentos políticos, que también incluye una “Comunicación sobre la configuración del futuro digital de Europa” y un “Libro Blanco sobre la inteligencia artificial” como enfoque europeo de la excelencia y la confianza.

Para garantizar que la UE coseche los beneficios de un mejor uso de los datos, incluidos una mayor productividad y unos mercados competitivos, pero también mejoras en la salud y el bienestar, el medio ambiente, una gobernanza transparente y unos servicios públicos asequibles, la Estrategia Europea de Datos contribuye a un planteamiento global de la economía de los datos que pretende aumentar el uso y la demanda de datos y de productos y servicios basados en datos en todo el mercado único.

En este contexto, la UE ha ido aprobando muchas normas que se refieren a la gobernanza y circulación de los datos en ámbito económico y no económico, entre las cuales podemos citar: Reglamento (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización (Reglamento de Datos); Reglamento (UE) 2022/1925 sobre mercados disputables y equitativos en el sector digital (Reglamento de Mercados Digitales); Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales); Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Ley de Gobernanza de Datos); Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la libre circulación de los datos no personales; Reglamento (UE) 2024/2847 sobre los requisitos horizontales de ciberseguridad para los productos con elementos digitales; Directiva (UE) 2019/1024 relativa a los datos abiertos y la reutilización de la información del sector público, etc.

El propio Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia (Reglamento de la “Artificial Intelligence Act”, en lo que sigue

AIA) prevé reglas específicas sobre el uso de datos personales y sobre la obligación de garantizar la calidad de los datos (véase el artículo 10 AIA).

#### **IV. Libertad de circulación de los datos y sus límites**

En las fuentes jurídicas e institucionales antemencionadas se destaca en particular la importancia que los datos deban fluir libremente, incluso entre países.

La circulación de datos es un eje fundamental en la economía digital, actuando como catalizador para la innovación, el comercio transfronterizo y el desarrollo social.

La OCDE, por ejemplo, desde su Recomendación de 1980 sobre sus Directrices de Privacidad, reconoce que los flujos transfronterizos de datos personales son esenciales para el comercio. Estas directrices buscan armonizar legislaciones nacionales para evitar obstáculos injustificados, promoviendo principios como el consentimiento informado, la limitación de la finalidad y la seguridad de los datos.

Un informe conjunto de la OCDE con la OMC (2025) cuantificó el impacto económico de la circulación de datos: políticas equilibradas que combinen apertura y garantías de confianza podrían aumentar el PIB global en un 1,77% y las exportaciones en un 3,6%, con beneficios más pronunciados en países en desarrollo (hasta +4% en PIB). Por el contrario, la fragmentación normativa total podría reducir el PIB mundial en 4,5%.

Por otra parte, la normatividad de la Unión Europea en tema de datos tiene como objetivo, ante todo, garantizar la libre circulación de datos. En efecto, el objetivo de garantizar la libre circulación está claramente expresado por el Reglamento (UE) 2018/1807 (véase el artículo 1) y por el Reglamento (UE) 2016/679 (véase el artículo 3, párr. 3, GDPR).

Además, la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público tiene como objetivo promover el uso de datos abiertos y estimular la innovación en productos y servicios. Según el artículo 10 de la Directiva 2019/1024: *“Los Estados miembros apoyarán la disponibilidad de los datos de investigación mediante la adopción de políticas nacionales y actuaciones pertinentes destinadas a hacer que los datos de la investigación financiada*

*públicamente sean plenamente accesibles (“políticas de acceso abierto”) en aplicación del principio de apertura por defecto y de compatibilidad con los principios FAIR”* <sup>6</sup>. La necesidad de garantizar la circulación de datos es funcional al funcionamiento del mercado interno (CIPPITANI, 2023.a: p. 157) y de la investigación científica para construir el así llamado Espacio Europeo de la Investigación (ver el artículo 179 Tratado de Funcionamiento de la Unión Europea; sobre los aspectos jurídicos) (CIPPITANI, 2023b).

Sin embargo, la circulación de datos encuentra límites debidos a la necesidad de proteger intereses fundamentales como el derecho a los datos personales (véase el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y el “habeas data” de las constituciones latinoamericanas), así como intereses económicos o la seguridad (CIPPITANI, 2023c) (véase lo previsto en el artículo 1.2.d de la Directiva 2019/1024).

Pero, la mayoría de los obstáculos dependen de la fragmentación normativa entre países y los conflictos entre soberanía nacional y conectividad global.

La UNCTAD advierte que, sin marcos coordinados, se perpetúan riesgos como la violación de privacidad y la concentración de poder en corporaciones tecnológicas, lo que exige acuerdos internacionales inclusivos que equilibren intereses comerciales, derechos individuales y desarrollo sostenible.

Si bien es importante la protección de intereses fundamentales (como la privacidad o la seguridad), eso puede obstaculizar objetivos de interés general, como la investigación biomédica o la protección de la salud pública.

Frente a estas tensiones, diversas instituciones europeas han comenzado a proponer un cambio de paradigma. El Supervisor Europeo de Protección de Datos (EDPS), por ejemplo, aboga por una “solidaridad digital” que permita compartir datos de forma responsable en situaciones de emergencia, sin reproducir modelos económicos basados en la vigilancia sistemática (Supervisor Europeo de Protección

---

<sup>6</sup> FAIR se refiere a que los datos sean *Findable, Accessible, Interoperable y Reusable*, tal y como se propone en el artículo *The FAIR Guiding Principles for scientific data management and stewardship* por Mark D. Wilkinson y otros en la revista *Scientific Data*, v.3; 2016. Esta propuesta es ampliamente aceptada en la comunidad científica y ha pasado a formar parte de los documentos y disposiciones normativas de la Unión Europea. En resumen, el significado de estos principios es: Localizables (otros pueden encontrar esos datos), Accesibles (los datos pueden ser accesibles a otros), Interoperables (los datos pueden ser integrados con otros datos y/o pueden ser fácilmente utilizados por máquinas), Reutilizables (los datos pueden ser reutilizados en nuevas investigaciones).

de Datos (EDPS), “Digital solidarity: a European response to data use in emergencies”, 2020). A nivel internacional la Declaración de Roma del G20 apunta hacia una gobernanza transnacional de los datos que combine el respeto de los derechos fundamentales con la promoción del bien común global (Declaración de Roma del G20, Principios n.º 7 y 10, mayo de 2021; CIPPITANI, 2023).

En este contexto, la Ley de Gobernanza de Datos (Reglamento (UE) 2022/868) introduce el concepto jurídico de altruismo de los datos, definido como el tratamiento voluntario de datos personales y no personales por parte de personas físicas y jurídicas sin ánimo de lucro, con fines de interés general como la sanidad, la protección medioambiental o la investigación científica (Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza de datos (*Data Governance Act*), artículos 2.10, 16-22). Este nuevo mecanismo permite a los ciudadanos donar sus datos de manera estructurada y segura a entidades reconocidas oficialmente como organizaciones de altruismo de datos, en un intento de institucionalizar la contribución voluntaria a los bienes comunes digitales (COMISIÓN EUROPEA, 2022: p. 197).

## **V. Problemas jurídicos de la disciplina jurídica de los datos**

La legislación de la UE y de los países latinoamericanos, así como las fuentes de algunas organizaciones internacionales, tratan de reglar el uso de los datos de manera proactiva, a diferencia de lo que ocurre en otros sistemas jurídicos, como el estadounidense, que prefiere dejar la gobernanza del mundo digital a las dinámicas de mercado o, mejor aún, a las políticas de unas pocas empresas multinacionales.

Sin embargo, desde el punto de vista jurídico, se pueden observar algunos problemas que caracterizan la actual disciplina de los datos.

### **V.i. Definición e clasificación de los datos**

“Dato” es probablemente una de las expresiones más utilizadas en la era digital, pero no hay un acuerdo sobre su definición.

Los documentos de la UNESCO, de la OMS y de otras organizaciones internacionales no contienen definiciones de dato, si no de datos personales.

La OCDE no proporciona una única definición formal y estricta de "dato" (véase, por ejemplo, "Recomendación del Consejo sobre Gobernanza de Datos de la Administración Pública" o informes sobre "Inteligencia Artificial en la Sociedad" donde los datos son el "combustible"), pero implícitamente se refiere a los datos como un elemento clave para la gobernanza digital, la formulación de políticas y el análisis económico. En general, se refiere a información estructurada y procesable.

La propia OCDE, así como otras organizaciones como la ONU, la UNESCO, el FMI y el Banco Mundial, se refieren a los datos objeto de análisis estadístico, por ejemplo, para el análisis de la estabilidad macroeconómica y la formulación de políticas o para el monitoreo de los Objetivos de Desarrollo Sostenible (ODS).

Un mayor esfuerzo definitorio se puede encontrar en las fuentes de la Unión Europea. Algunos documentos de la Comisión europea se refieren a la diferencia entre datos, informaciones y conocimientos (EUROPEAN COMMISSION, 2015).

- los datos ("raw data") corresponden a cantidades u otros atributos cuantitativos o cualitativos derivados de la observación, la experimentación, la medición o el cálculo. Los datos no están estructurados, contextualizados ni comentados;

- la información corresponde a un conjunto de datos contextualizados y estructurados, con la intención del productor de darles sentido.

- El conocimiento corresponde a la apropiación cognitiva de la información por parte de un individuo que la organiza, sintetiza y/o resume para hacerla más fácilmente comprensible.

Se trata de una clasificación que viene de las ciencias de la comunicación (ACKOFF R.L., 1989).

Sin embargo, esta distinción no se encuentra en las fuentes jurídicas donde se usan los tres conceptos como si fuesen sinónimos. Es el caso de la legislación de la Unión Europea y de otros sistemas jurídicos sobre los datos personales, que son "toda información sobre una persona física identificada o identificable ("el interesado")" (Artículo 3, 1), GDPR).

En otras fuentes se usan definiciones más amplias, como la contenida en el Data Governance Act (PARLAMENTO EUROPEO & CONSEJO DE LA UNIÓN EUROPEA, 2022), según el cual los datos son: "*toda representación digital de actos, hechos o*

*información, así como su recopilación, incluso como grabación sonora, visual o audiovisual” (art. 2, n. 1, Data Governance Act) y también en la Directiva 2019/1024 que considera los datos de investigación como “documentos en formato digital, distintos de las publicaciones científicas, recopilados o elaborados en el transcurso de actividades de investigación científica y utilizados como prueba en el proceso de investigación, o comúnmente aceptados en la comunidad investigadora como necesarios para validar las conclusiones y los resultados de la investigación” (artículo 2, no. 9).*

Por otro lado, los “conjuntos de datos de alto valor” son aquellos *“documentos cuya reutilización está asociada a considerables beneficios para la sociedad, el medio ambiente y la economía, en particular debido a su idoneidad para la creación de servicios de valor añadido, aplicaciones y puestos de trabajo nuevos, dignos y de calidad, y del número de beneficiarios potenciales de los servicios de valor añadido y aplicaciones basados en tales conjuntos de datos” (artículo 2, no. 10).*

A nivel de organismos internacionales se puede citar *“la norma ISO/IEC 2382-1, según la cual los datos son “una representación reinterpretable de información de una manera formalizada, adecuada para la comunicación, la interpretación o el procesamiento”.* Los datos los pueden crear o escribir personas o estar generados por máquinas o sensores.

Normalmente las fuentes jurídicas definen los datos personales, pero no definen los datos no personales<sup>7</sup>, si no de manera “negativa”, como hace el Data Governance Act de la Unión Europea según el cual los datos no personales son “aquellos que no son datos personales” (artículo 2, no. 4).

Esta clasificación no está suficientemente desarrollada y esconde las características específicas de los datos, sobre todos los “no personales” disciplina importante para reglar aspectos e intereses muy variados (por ejemplo, económicos, de seguridad, etc.).

Además, la distinción entre datos personales y no personales deja zonas grises a este respecto, de modo que la Comunicación de la Comisión del 29 de mayo de 2019, “Orientaciones sobre el Reglamento relativo a un marco para la libre

---

<sup>7</sup> Véase entre muchas el GDPR, la legislación chilena, el Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), Estrasburgo, 28 de enero de 1981.

circulación de datos no personales en la Unión Europea” (COMISIÓN EUROPEA, 2019: p. 250), también identifica los llamados conjuntos de “datos mixtos”, es decir, un conjunto compuesto tanto por datos personales como por datos no personales. Por ejemplo, los documentos de una empresa u organismo público que contienen el nombre y otra información relativa al representante legal.

En tales casos, si los datos personales y no personales dentro de un conjunto de datos están inextricablemente vinculados, así para regular la parte compuesta por los datos personales, se aplicarán los principios y normas del GDPR (véase el artículo 2 Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018).

Pero no está previsto que pasa con los datos no personales. Así como no se regula la situación de algunos datos personales que tienen una función particular en el ámbito de un contexto específico.

## **V.ii. Indiferencia de los contenidos y neutralidad tecnológica**

Los datos tienen sus especificidades que dependen de la información de su contenido. Por ejemplo, los datos de salud (véase la definición amplia contenida en el considerando 35 de GDPR), son muy diferentes de otros datos y, en particular, los de categorías específicas (datos de salud, datos genéticos, véanse los datos sobre opiniones políticas).

Pero el GDPR y otras normas sobre los datos personales los trata por igual sin diferenciar una tutela de protección ad-hoc según interés y finalidad. Particularmente interesante es la jurisprudencia chilena, pionera en el mundo considerando problemas específicos de datos asociados a las neurotecnologías (ver el caso Emotive/Girardi, Corte Suprema rol N°105065-2023; CORNEJO-PLAZA ET AL., 2024) a datos biométricos (véase la sentencia en el caso WorldCoin, Corte Suprema rol n° 18.566-2024 donde la Corte Suprema ordena a las empresas World coin y world App eliminar datos biométricos de un menor de edad por vulnerar derechos a la privacidad, protección de datos y derechos a la integridad psíquica y física). Esta jurisprudencia evidencia un “excepcionalísimo” de datos biométricos del comportamiento (CORNEJO-PLAZA ET AL, 2024), análogo al excepcionalísimo de los datos genéticos (CIPPITANI, 2018). Por ejemplo, por lo que se refiere a los datos

genéticos, la información genética es común para muchas personas y tiene un contenido informativo (sobre varias características de los sujetos de los datos) que puede desarrollarse durante los años siguientes como consecuencia de la evolución de la tecnología. Los neurodatos podrían permitir conocer aspectos íntimos de las emociones y del pensamiento de las personas incluso una vez que los datos se encuentren anonimizados. De todas estas características, que son importantes en la tutela de los derechos humanos, sin embargo, no se contienen en las fuentes que protegen los datos personales.

Además, las legislaciones sobre los datos personales, así como la europea, no abordan específicamente los temas del tratamiento de datos a través de las neurotecnologías y de la IA, siendo una normatividad que se supone neutral con respecto a las tecnologías a las cuales se aplica. En particular, el uso de la IA representa un desafío para la implementación de principios como el consentimiento, la minimización, la limitación de la finalidad, la transparencia del tratamiento de datos personales. Las dificultades en la aplicación de la disciplina de protección de datos personales a la recopilación y tratamiento de datos utilizados para el entrenamiento de los sistemas de IA se observa, por ejemplo, en las medidas adoptadas por el Garante italiano de la privacy contra OpenAI (véanse las medidas de marzo de 2023 y de diciembre de 2024). Además, la jurisprudencia chilena antemencionada muestra como las neurotecnologías presentan problemas específicos. Además, el uso de datos por los sistemas de IA y por las neurotecnologías necesitan adoptar herramientas técnicas y organizativas que permitan obtener una alta calidad de los datos, a fin de evitar sesgos, discriminaciones, alucinaciones etc. Otras formas de tratamiento de los datos diferentes de la IA y de las neurotecnologías no tienen los mismos problemas. Por lo tanto, es necesario pensar en soluciones que aborden una aplicación de las reglas de protección de datos personales que consideren no solo de las características de los datos.

### **V.iii. Insuficiencia de las disciplinas sobre los datos personales para proteger todos los otros derechos e intereses fundamentales.**

No siempre la disciplina de la protección de datos personales es suficiente para proteger otros derechos fundamentales. El caso de los neurodatos en la jurisprudencia chilena es particularmente interesante.

Desde un punto de vista técnico, no siempre los neurodatos permiten la identificación de su titular de manera directa, sino que normalmente se trata de una mera recolección de información de la actividad eléctrica del cerebro y del sistema nervioso, que requiere de una interpretación de estos para la identificación de la persona en cuestión.

Además, la protección jurídica de los datos personales tiene en consideración los datos específicos y aislados y no la información elaborada desde esos datos. En la realidad virtual, por ejemplo, el problema no surge de los datos aislados, sino del conjunto de datos, de diversa naturaleza, proporcionados por la experiencia inmersiva y procesados con sistemas de inteligencia artificial. El riesgo central de la realidad virtual es que proporciona directamente un perfil completo y dinámico del individuo.

Se debe señalar además, que las neurotecnologías pueden adicionar otros tipos de problemas y afectar derechos diferentes de los previstos en el GDPR o en la legislación de protección de datos personales.

Por ejemplo, uno de los grandes desafíos que presentan el uso de las tecnologías y especialmente las neurotecnologías es en el ámbito de la protección de los derechos de los consumidores (CORNEJO-PLAZA, 2023).

Además, en la literatura se observa que este tipo de tecnología puede provocar problemas de seguridad (CIPPITANI, 2023b) o de protección de derechos como la integridad psíquica, privacidad mental, decisiones libres de sesgos algorítmicos, equidad en el acceso a tecnologías de aumentación cognitiva (CORNEJO-PLAZA & SARACINI, 2023). En esta línea, Chile es pionero en el establecimiento de una protección de los derechos fundamentales frente a un uso disruptivo de las neurotecnologías (Véase la Ley N° 21.383 establece que: “Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas” estableciendo que “El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su

utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella”

## **VI. Cuestiones sobre los derechos y las relaciones jurídicas concernientes los datos**

### **VI.i. Sujetos y obligaciones**

Además de las inconsistencias jurídicas sobre los datos mencionadas en el párrafo anterior, hay un problema más general que consiste en la falta de un estatuto jurídico de los titulares de los datos, y tampoco existe un estatuto jurídico en general del dato como posible objeto de derecho.

En muchos casos es difícil establecer cuáles son los derechos sobre los datos y los titulares de dichos derechos.

EL GDPR y legislaciones similares tienen como objetivo la protección de un derecho fundamental de los interesados, estableciendo obligaciones de los responsables o de los encargados del tratamiento.

Algunas disposiciones se refieren a los “titulares de los datos” (ver por ejemplo el considerando 50 de la Directiva (UE) 2019/1024 que habla de acuerdos entre “titulares” y “reutilizadores” de datos), que se pueden definir como: *“toda persona jurídica, incluidos los organismos del sector público y organizaciones internacionales, o persona física que no sea el interesado con respecto a los datos específicos en cuestión, que, de conformidad con el Derecho de la Unión o nacional aplicable, tenga derecho a conceder acceso a determinados datos personales o no personales o a compartirlos”* (véase el artículo 2, no. 8, Data Governance Act). De otro lado, se define el “usuario de datos” que es aquel sujeto *“que tenga acceso legítimo a determinados datos personales o no personales y el derecho, incluido el que le otorga el Reglamento (UE) 2016/679 en el caso de los datos personales, a usarlos con fines comerciales o no comerciales”* (véase artículo 2, no. 9, Data Governance Act).

Otras disposiciones identifican otros sujetos que tienen una posición respecto a los datos como el “guardián de acceso” (“gatekeeper”), es decir una

empresa prestadora de servicios básicos de plataforma previstos en el Reglamento de Mercados Digitales (“Digital Market Act”)<sup>8</sup>.

Dichas normas establecen obligaciones para los responsables, titulares, guardianes de acceso, pero no toman una posición sobre cuáles derechos se refieren a los datos.

Por ejemplo, el artículo 10, párr. 2, de la Directiva 2019/1024 prevé que se pongan a disposición los datos de investigación financiados por fondos públicos en el caso *“investigadores, organizaciones que realizan actividades de investigación u organizaciones que financian la investigación ya sea que los hayan puesto a disposición del público a través de un repositorio institucional o temático”*. En cambio, no se establecen los derechos sobre los datos de los investigadores y de las organizaciones en el ámbito de los cuales se llevan a cabo las actividades de investigación.

Una posición más clara la encontramos en un ámbito más específico, como es la base jurídica de los programas de financiación de la Unión Europea, donde se pueden encontrar reglas sobre los derechos y los resultados de la actividad realizada, donde por resultados se entienden todo producto del proyecto, tangibles o intangibles, entre los cuales tenemos la propiedad industrial, pero también los datos e informaciones (confidenciales o no) específicas.

Las normas implícitamente admiten que los datos pueden ser objeto de contratos. Además de los acuerdos entre titulares y reutilizadores de datos mencionados arriba, el Derecho de la Unión Europea (ver el Data Governance Act) habla de “reutilización”, “acceso”, “intercambio”, “cesión”, “transferencia”, “licencia” etc. de los datos, que incluye actos voluntarios que se pueden enmarcar en la definición de “contratos”.

Sin embargo, no se dictan reglas específicas aplicables a estos contratos. Además, muchas veces, el hecho que los datos se refieren a derechos fundamentales limita la aplicación de las normas sobre los contratos.

---

<sup>8</sup> Reglamento (UE) 2022/1925 del Parlamento europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

## VI.ii. Datos y bienes

El estatuto jurídico residual del Código Civil no es suficientemente amplio ante la complejidad de la economía digital, propia de una sociedad de la anticipación que trabaja con predicciones de conductas por diseño más que con el razonamiento de los estándares de conducta.

En los códigos civiles, los bienes son “cosas” que forman objeto de derechos (véase el Código Civil Italiano). Los bienes son cosas susceptibles de una evaluación económica (ver artículo 16 del Código Civil Argentino). Por otro lado, “*los bienes se clasifican en corporales e incorpóreas. Los bienes corporales son aquellos que tienen existencia material y pueden ser percibidos por los sentidos, mientras que los incorpóreas son aquellos que consisten en meros derechos, como los créditos o las servidumbres activas*” (ver artículo 565 Código Civil Chileno).

Los datos son difíciles de clasificar como bienes, porque éstos no obedecen en todas sus manifestaciones a la dimensión corpórea e incorpórea de la clasificación de bienes del derecho civil y, como tal, no califican para ser considerados como “cosas” (FUENTEALBA, 2021). Sin embargo, el dato no es ni lo uno ni lo otro, porque se trata de una representación simbólica de la realidad independiente de su soporte. Además, no es cierto que los datos tienen un valor económico.

En virtud de que los datos no consisten en bienes no se podría ejercer sobre ellos la propiedad como derecho de usar, gozar y disponer de ella arbitrariamente (ver artículo 582 del *Código Civil Chileno*), ni tampoco ellos podrían ser sujetos a una “especie de propiedad” sobre cosas incorpóreas (como establece el artículo 583 del *Código Civil Chileno*).

De hecho, la facilidad con la que se pueden copiar, compartir y modificar los datos complica la aplicación de los derechos de propiedad exclusiva.

La aplicación de las normas tradicionales de propiedad relativas a la adquisición, la circulación y la protección de los datos se enfrenta a varios obstáculos. La adquisición de la propiedad, que suele referirse a bienes tangibles, se basa a menudo en la posesión física o la transferencia. Sin embargo, la adquisición de datos puede producirse por diversos medios, como la recopilación, la generación y la agregación, lo que difumina las líneas de la propiedad y el control. Las normas

tradicionales de propiedad que rigen la circulación, como la venta y la transferencia, también se enfrentan a retos en el ámbito digital.

Tampoco se puede aplicar a los datos la disciplina de la “propiedad intelectual”. En efecto, los datos, en cuanto tales, no constituyen una invención patentable ni tampoco son producciones del talento o ingenio. Por lo tanto, existe un inmenso conjunto de resultados y conocimientos que se encuentran expresamente excluidos de categorías como cosas corporales, incorporales y creaciones intelectuales y, como tal, no tienen protección bajo el concepto de propiedad, ni siquiera con “matices”, como ocurre con la denominada propiedad intelectual o industrial.

Sin embargo, la legislación sobre el derecho de autor (véase la Ley N° 17.336 de Chile; Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos) hoy reconoce como objeto de protección las bases de datos cuando constituyen una creación intelectual del autor o para los fabricantes (este último es denominado “derecho sui generis” por el artículo 7 de la Directiva 96/9/CE). El derecho sui generis del fabricante en la economía de datos se justifica por el esfuerzo e inversión destinados a la obtención, verificación y presentación de los datos” (ROMEY & CÓNUL, 2019, p. 199). De todas maneras, la disciplina sobre las bases de datos no prevé una tutela de los datos por sí mismos (como destaca el artículo 3, número 17, de la Ley N° 17.336).

Las fuentes jurídicas europeas parecen apoyar la conclusión de que los datos no se pueden reconducir al concepto de bien. La Directiva (UE) 2019/770 sobre los contratos de suministro de contenidos digitales (UNIÓN EUROPEA, 2019) definen el concepto de “bienes como elementos digitales”, es decir “todo objeto mueble tangible que incorpore contenidos o servicios digitales o esté interconectado con ellos de tal modo que la ausencia de dichos contenidos o servicios digitales impediría que los bienes realizaran sus funciones” (artículo 2, no. 3). Donde por “contenidos digitales” se entienden “los datos producidos y suministrados en formato digital” (artículo 2, no. 1).

Los datos se podrían enmarcar en una categoría heterogénea de conceptos llamados “nuevos bienes” (PEUKERT, 2008, p.1) que es una traducción de “new properties” utilizada en la literatura norteamericana, en particular, por primera vez

por Charles A. Reich en 1964 en *The Yale Law Journal* para representar las formas de riqueza entonces incipientes<sup>9</sup>.

Sin embargo, el concepto de “*new properties*”, en realidad no prevé una disciplina jurídica para los datos, si no reconoce la dificultad de aplicar la disciplina de los bienes y afirma la necesidad del desarrollo de nuevos derechos.

### **VI.iii. Datos y contratos**

Si los datos no son cosas o bienes, esto no significa que ellos no son relevantes para el derecho civil.

Como afirma la Comunicación “La construcción de una economía de los datos europea” del 10 de enero del 2017 se opina que “*La ‘economía de los datos’ se caracteriza por un ecosistema en el que diferentes tipos de agentes del mercado –como fabricantes, investigadores y proveedores de infraestructuras– colaboran para garantizar que los datos sean accesibles y utilizables. Esto permite a dichos agentes extraer valor de esos datos, creando toda una gama de aplicaciones con un gran potencial para mejorar la vida cotidiana (por ejemplo, la gestión del tráfico, la optimización de las cosechas o la atención sanitaria a distancia)*” (COMISIÓN EUROPEA, 2019: p.9).

Los datos pueden ser objeto de obligaciones contractuales, especialmente en el contexto de la economía digital.

Desde el punto de vista del derecho civil los datos son una referencia de la prestación debida (sea de dar, hacer, no hacer, etc.) y ellas son el objeto de las obligaciones necesarias para extinguir la obligación (cfr. el artículo 1174 Código Civil Italiano; artículos 1553 y 1555 del Código Civil Chileno). El dato, en cuanto referencia de una prestación, contiene un interés patrimonial o no patrimonial (por ejemplo, cultural o científico) (cfr. artículo 725 Código Civil y Comercial Argentino; artículo 1174 Código Civil de Italia; artículo 1568 del Código Civil Chileno), aunque la prestación sea normalmente medible desde el punto de vista monetario (artículo 1174 Código Civil Italiano).

---

<sup>9</sup> C. A. Reich, en el artículo *The New Property*, en la revista *Yale Law Journal* observó la aparición de nuevas formas de riqueza representadas principalmente por derechos o estatus y/o “concesiones” de carácter administrativo (“*largesse*”), todas ellas consideradas conjuntamente con el trabajo, principal fuente de riqueza de los hombres (REICH, 1964)

El dato, por tanto, aunque no sea un bien o una cosa, puede ser considerado como elemento relevante en la representación del caso jurídico<sup>10</sup>. Los elementos del caso concreto constituyen la representación superficial del comportamiento prescrito, tal y como se ve desde diferentes perspectivas.

Sin embargo, los datos como referencia de prestaciones y por tanto de obligaciones y contratos, están sujetos a limitaciones, como resulta ser el caso de los datos personales.

Como se ha mencionado, la Directiva (UE) 2019/770 reconoce expresamente que, en los contratos de suministro de contenidos o servicios digitales, el consumidor puede proporcionar datos personales como contraprestación, en lugar de un pago monetario.

Esto implica que los datos personales pueden ser objeto de obligaciones contractuales, pero siempre dentro de los límites y garantías establecidos por el GDPR y la normativa de protección de datos, que como se ha dicho anteriormente, en Europa y Latinoamérica, busca proteger un derecho fundamental que prevalece por sobre los intereses económicos<sup>11</sup>.

La entrega de datos personales como contraprestación contractual, en primer lugar no implica la transmisión de un derecho de propiedad que no es técnicamente viable por el derecho civil; en segundo lugar, la necesidad de la protección de un derecho fundamental tiene como consecuencia que la persona interesada otorgue una autorización limitada y condicionada para su tratamiento, al respeto de estrictos principios (licitud, lealtad, transparencia, minimización, limitación de la finalidad, etc.) y derechos del interesado (acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento).

En efecto como opina la Comisión Europea “La privacidad no es una mercancía de intercambio” (COMISIÓN EUROPEA, 2017).

---

<sup>10</sup> Como opina IRTI (1984: p.76), los elementos del caso jurídicos son sujetos, objetos, intereses, valores, etc. que no son entidades prejurídicas y absolutas si no que son funcionales a la representación jurídica del comportamiento.

<sup>11</sup> TJUE, sentencia del 13 de mayo de 2014, *Google Spain*, C-131/12, EU:C:2014:317.

## VII. Relevancia jurídica de los datos: necesidad de garantizar la calidad de los datos

La creciente relevancia jurídica de los datos hace necesario una gobernanza que les otorgue un estatuto jurídico sui generis debido a la especial relevancia que implican en la economía digital e incluso en el ecosistema digital. Al contrario, como se ha visto, los datos están al centro de los derechos y relaciones de naturaleza personal, colectiva y patrimonial.

Un interesante ejemplo de esta tendencia es el Reglamento de la AIA, el cual se preocupa de *“instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos para el entrenamiento, la validación y la prueba sean de alta calidad”* (UNIÓN EUROPEA, 2024; cons. 67).

El artículo 26, párr. 1, establece que *“Los responsables del despliegue de sistemas de IA de alto riesgo adoptarán medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen”*.

Se trata de la afirmación del principio de “accountability” previsto incluso en el artículo 25 GDPR.

Entre las medidas que debe adoptar el responsable es importante la Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo, previsto per el artículo 27 AIA, análogamente al artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo complementará dicha evaluación de impacto relativa a la protección de datos.

La exigencia de la una gestión del riesgo es sostenida por el CONSEJO DE EUROPA (2017: párr. 2.).

Sin embargo, permanecen los problemas que se han destacado en la búsqueda de un equilibrio entre el Reglamento de la AIA y otras normativas en materia de datos.

Como se afirma en el considerando 67 *“Los conjuntos de datos deben tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los colectivos de personas cuando se utilizan sistemas de IA de alto riesgo, prestando una*

*atención especial a la mitigación de los posibles sesgos en los conjuntos de datos que puedan afectar a la salud y la seguridad de las personas físicas, tener repercusiones negativas en los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando los datos de salida influyan en la información de entrada de futuras operaciones (bucles de retroalimentación)” (ver también al artículo 10, párr. 2 y 3).*

La cuestión de la calidad de los datos está planteado también por el “considerando” 71 GDPR que prevé que *“el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrijan los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error”* y la posibilidad que el tratamiento sea discriminatorio.

Los criterios generales para construir sistemas de calidad están establecidos por el artículo 10 del Reglamento de la AIA, que prevé que los conjuntos de datos de entrenamiento, validación y prueba deberán someterse a prácticas de gobernanza y gestión que se centrarán, en particular, en lo siguiente: las decisiones pertinentes relativas al diseño; los procesos de recogida de datos y el origen de los datos; las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, la actualización, el enriquecimiento y la agregación. Se deberá adoptar medidas para evitar *detectar, prevenir y mitigar “posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones”* (UNIÓN EUROPEA, 2024: art. 10, párr. 2, f, e, i)

El Consejo de Europa en su *Guidelines on Artificial Intelligence and data protection*, 25 de enero 2019 recomienda (punto 4) evaluar de forma crítica la calidad, la naturaleza, el origen y la cantidad de datos personales utilizados, reduciendo los datos innecesarios, redundantes o marginales durante las fases de desarrollo y entrenamiento, y supervisando después la precisión del modelo a

medida que se alimenta con nuevos datos y el uso de datos sintéticos<sup>12</sup> para minimizar la cantidad de datos personales procesados por las aplicaciones de IA.

En particular se debe tener en cuenta el riesgo de que los datos y los modelos algorítmicos descontextualizados tengan repercusiones negativas sobre las personas y la sociedad.

### **VIII. Intereses colectivos y bienes comunes**

Los datos, como se ha visto, son el punto de encuentro por múltiples intereses individuales, de carácter no patrimonial (por ejemplo, la protección de los datos personales o la salud mental) y patrimonial (los datos como referencia de prestaciones).

Por otro lado, a los datos se asocian intereses colectivos como la seguridad, el funcionamiento del mercado digital, la calidad, y otros.

Este último aspecto parece establecer un enlace entre la situación jurídica de los datos y la teoría de los bienes comunes (*commons*), que ha sido desarrollada a partir desde una perspectiva interdisciplinaria (entre economía, sociología, ciencia política y derecho) especialmente en la obra de Elinor OSTROM (1990), ganadora del Premio Nobel de Economía en 2009.

La teoría de los bienes comunes proporciona un marco para comprender la gestión y la utilización de los recursos compartidos, a los que pueden acceder múltiples individuos o entidades (FENNELL, 2011).

El concepto de los bienes comunes ha evolucionado significativamente a lo largo del tiempo, pasando de la gestión de recursos tangibles como la tierra y el agua a abarcar recursos intangibles como el conocimiento, la cultura y los datos (DANI, 2014). Se habla de “datos comunes” para indicar la aplicación de los *commons* a los datos (por ejemplo, GROSSMAN, 2023). En esencia, la teoría aborda los retos de la asignación de recursos, la sostenibilidad y el acceso equitativo en situaciones en las que los derechos de propiedad tradicionales están mal definidos o son inadecuados (BOLLIER, 2024).

---

<sup>12</sup> Los datos sintéticos se generan a partir de un modelo de datos construido sobre datos reales. Deben ser representativos de los datos reales originales. Véase la definición de datos sintéticos (OCDE, 2007)

La teoría de los bienes comunes difiere significativamente del concepto de propiedad tal y como lo articulan los pandectistas y lo codifican los códigos civiles europeos (HOFFMANN, 2012). En particular, dicha teoría contrasta con la propiedad privada, en la que se asignan derechos exclusivos a un único propietario, y con la propiedad estatal, en la que el gobierno controla el acceso y el uso (BOLLIER, 2020).

La aplicación del marco de los bienes comunes a los datos y la información, pero tiene que considerar que los datos, a diferencia de otros bienes comunes como los recursos genéticos o el agua, son “bienes” no rivales (“non-rivalrous goods”), es decir que su uso por parte de un individuo no disminuye su disponibilidad para otros (KERBER, 2016). A diferencia de los recursos físicos, los datos y la información pueden ser accedidos, compartidos y modificados simultáneamente por múltiples usuarios sin agotarse.

Sin embargo, incluso para los datos y la información aún pueden realizarse la “tragedy of commons” aunque de diversas maneras de los otros bienes comunes (NAGLE, 2018). Por ejemplo, el uso excesivo de datos personales sin las debidas salvaguardas de privacidad puede conducir a una pérdida de confianza y voluntad de compartir datos, agotando efectivamente el recurso. Del mismo modo, la difusión de información errónea y desinformación puede contaminar el ecosistema de la información, dificultando el acceso a información fiable y precisa (ESTRATEGIA EUROPEA DE DATOS, 2020).

En realidad la teoría de los bienes comunes no establece un régimen de propiedad sobre los “commons”. El interés para esa teoría, incluso en el ámbito de los datos, es que ella hace hincapié en el acceso compartido y la gobernanza colectiva de los recursos (VALK & RYAN, 2025), promoviendo la colaboración, la innovación, el acceso generalizado y la distribución equitativa (VALK & RYAN, 2025).

Es esencial reconocer que los derechos sobre los datos van más allá de la mera posesión o el control.

El derecho contractual, en particular, debe evolucionar para abordar los matices de los acuerdos de intercambio de datos dentro de los datos comunes. Es posible que sea necesario modificar las condiciones contractuales estándar, como las relativas a la propiedad, la responsabilidad y la confidencialidad, para reflejar los principios de los bienes comunes (DUCUING & REICH, 2023). En lugar de asignar

derechos de propiedad exclusivos a una sola parte, los acuerdos de intercambio de datos dentro de un bien común pueden establecer la propiedad compartida o las responsabilidades de administración entre múltiples partes interesadas. Este enfoque reconoce que los datos suelen tener múltiples contribuyentes y beneficiarios, y que un enfoque colaborativo de la gobernanza de los datos puede fomentar la innovación y maximizar el valor social de los datos. Los datos no son propiedad como los bienes tradicionales, por lo que los argumentos a favor de la propiedad de los datos se ven superados por los argumentos a favor del acceso abierto (DETERMANN, 2018).

Además, el derecho contractual debe abordar la cuestión del acceso y el uso de los datos dentro de un bien común de datos. En lugar de restringir el acceso en función de intereses de propiedad, los acuerdos de intercambio de datos pueden conceder amplios derechos de acceso a una comunidad definida de usuarios, con sujeción a determinadas condiciones y limitaciones. Estas condiciones pueden incluir requisitos de privacidad, seguridad y uso ético de los datos, así como la obligación de contribuir al patrimonio común compartiendo nuevos datos o conocimientos derivados de los datos compartidos (MCGUIRE, ROBERTS, AAS & EVANS, 2019).

## **IX. Gobernanza de la economía digital**

La teoría de los bienes comunes subraya la importancia de los diferentes intereses en juego al elaborar una gestión adecuada de los datos, en lo que llamamos con propiedad su “gobernanza”.

La necesidad de gobernar la economía y la sociedad digital impone acciones jurídicas y políticas como fomentar la libre circulación de los datos que se basen en acceso abierto y en la solidaridad digital, aunque tutelando intereses a vez en contraposición como la privacidad, la libertad económica, la libertad de investigación, el derecho de acceder a las informaciones de la pública administración, la seguridad y el orden público, etc.

Sin embargo, la gobernanza de los datos requiere una cuidadosa consideración de varios factores. Es importante fomentar una cultura de colaboración y confianza entre los usuarios de datos, animándolos a compartir sus

datos y conocimientos en beneficio de la comunidad en su conjunto (DEVINENI, 2023). En el contexto de la investigación, los datos abiertos facilitan un cambio en la cultura de la investigación y mejoran la disponibilidad de herramientas de analíticas de datos (BARKER ET AL., 2019). La transparencia en las prácticas relacionadas con los datos es fundamental, y abarca los métodos de recopilación de datos, los procedimientos de almacenamiento, los usos previstos y las salvaguardias contra el uso indebido (PERUCCI & SWANSON, 2024). Esta transparencia se extiende a la comunicación con los participantes sobre la finalidad y las posibles aplicaciones de los datos.

La gobernanza de los datos también depende de la disponibilidad de recursos para apoyar la curación, la armonización y el desarrollo de infraestructuras de datos (GROSSMAN, 2023). La inversión en normas de datos, esquemas de metadatos y herramientas de interoperabilidad puede facilitar la integración y el análisis de datos, lo que permite a los investigadores y profesionales extraer información valiosa de diversas fuentes de datos (DECHERCHI ET AL., 2021). Además, proporcionar formación y asistencia técnica a los usuarios de datos puede ayudarles a utilizar eficazmente los datos disponibles a través de los reservorios comunes, maximizando el impacto de las iniciativas de intercambio de datos. Los datos agrícolas pueden ofrecer compromiso, privacidad, control y reparto de beneficios; los recopiladores de datos de pequeñas y medianas empresas necesitan herramientas jurídicas sofisticadas y la capacidad de promocionar su participación en la apertura de datos; y los usuarios de datos necesitan acceso abierto (BAARBÉ ET AL., 2019).

Un modelo de gobernanza sólido debe incluir un sistema de seguimiento y evaluación para garantizar que los datos comunes funcionan eficazmente y alcanzan los objetivos previstos. Esto puede implicar el seguimiento de los patrones de uso de los datos, la evaluación del impacto del intercambio de datos en la innovación y el desarrollo económico, y la solicitud de comentarios a los usuarios de los datos y a las partes interesadas. Los datos como “bienes comunes” y la perspectiva de mercado compartido sobre los espacios de datos no son mutuamente excluyentes (VALK & RYAN, 2025).

La gobernanza de los datos tiene que proporcionar mecanismos para garantizar que el interés público se incluya en la arquitectura del espacio de datos, estableciendo regímenes ex ante con principios de diseño alineados con el interés público, definiendo para quién, por qué y con quién.

Este enfoque promueve la reutilización de los datos y la colaboración, lo que permite a los investigadores, innovadores y responsables políticos aprovechar los datos para el bien público (VAYENA ET AL, 2015).

La gobernanza de los datos debe encargarse de abordar cuestiones como los derechos de acceso, la calidad de los datos y la resolución de conflictos, además de establecer las normas y políticas para los datos comunes (HRISTOVA ET AL., 2023). Es esencial contar con normas y directrices claras para garantizar un uso equitativo y responsable de los datos. Además, la gobernanza de los datos implica una estrategia orientada a la educación y concientización de las personas hacia un adecuado uso de los datos, solo así las personas tendrán confianza en ser solidarios e incluso altruistas con datos que, si bien pueden ser confidenciales, son a su vez ricos en información específica para mejorar procesos, combatir pandemias o bien consolidar investigaciones.

Para lograr esta finalidad, es necesario superar los problemas jurídicos, algunos de los cuales se han destacado en este trabajo.

## X. Bibliografía

- ACKOFF, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis*, 16, pp. 3–9.
- BAARBÉ, J., BLOM, M., & DE BEER, J. (2019). A proposed “agricultural data commons” in support of food security. *The African Journal of Information and Communication (AJIC)*, 23, 1–17. Accesible en: <https://doi.org/10.23962/10539/27534>
- BARKER, M., OLABARRIAGA, S. D., WILKINS-DIEHR, N., GESING, S., KATZ, D. S., SHAHAND, S., HENWOOD, S., GLATARD, T., JEFFERY, K., CORRIE, B., TRELOAR, A., GLAVES, H., WYBORN, L., HONG, N. C., & COSTA, A. (2019). The global impact of science gateways, virtual research environments and virtual laboratories. *Future Generation*

- Computer Systems*, 95, pp. 240–248. Accesible en: <https://doi.org/10.1016/j.future.2018.12.026>
- BOLLIER, D. (2020). Commoning as a transformative social paradigm. In *Routledge eBooks* (p. 348). Accesible en: <https://doi.org/10.4324/9780367313401-28>
- BOLLIER, D. (2024). Challenges in expanding the commonsverse. *International Journal of the Commons*, 18(1), pp. 288–303. Accesible en: <https://doi.org/10.5334/ijc.1389>
- CIPPITANI, R. (2018). Genetic research and exceptions to the protection of personal data. In R. Arnold, R. Cippitani & V. Colcelli (Eds.), *Genetic Information and Individual Rights* (pp. 54–79). Universität Regensburg. Accesible en: <https://doi.org/10.5283/epub.36785>
- CIPPITANI, R. (2022). The ‘digital transnational solidarity’ and protection of the health: Commentary to Principle no. 7 of the Rome Declaration. *International Journal of Risk & Safety in Medicine*, 33 (2), pp. 167–176. Accesible en: <https://doi.org/10.3233/JRS-227002>
- CIPPITANI, R. (2023a). *Rights and relations within the European Union law*. Ali&no.
- CIPPITANI, R. (2023b). *La dimensión jurídica del Espacio Europeo de la Investigación*. CNR Editions.
- CIPPITANI, R. (2023c). La noción de “seguridad” en el Derecho de la Unión Europea. *Criminogenesis*, 2023, pp. 163–181.
- CIPPITANI, R., & CORNEJO-PLAZA, M. I. (2025). Convergencia reglamentaria Eurolatinoamericana en materia de datos. In C. F. Molina del Pozo, V. Saldaña Ortega & J. M. López Jiménez (Eds.), *La Unión Europea y la CELAC: Hacia una revitalización de las relaciones entre los territorios* (pp. 141–164). Editorial Dykinson. Accesible en: <https://doi.org/10.14679/3998>
- COMISIÓN EUROPEA. (2017). *La construcción de una economía de los datos europea*. Accesible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017DC0009>
- COMISIÓN EUROPEA. (2019). *Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea*. Accesible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52019DC0250>

- COMISIÓN EUROPEA. (2022). *Proposal for a Regulation on the European Health Data Space*. Accesible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197>
- CONSEJO DE EUROPA. (2017). *Directrices sobre la protección de las personas con respecto al tratamiento de datos personales en un mundo de big data*. Accesible en: <https://rm.coe.int/16806ebe7a>
- CONSULTANCY.EU. (2024). *Global eco-digital economy to double in next five years*. Accesible en: <https://www.consultancy.eu/news/9716/global-eco-digital-economy-to-double-in-next-five-years>
- CORNEJO-PLAZA, M. I. (2023). Consideraciones éticas de la neurociencia del consumidor. In S. Barona Vilar (Ed.), *Derecho del consumo y protección del consumidor sustentable en la sociedad digital del siglo XXI* (pp. 117–132).
- CORNEJO-PLAZA, M. I., & CIPPITANI, R., & PASQUINO, V. (2024). Chilean Supreme Court ruling on the protection of brain activity: Neurorights, personal data protection, and neurodata. *Frontiers in Psychology, 15*. Accesible en: <https://doi.org/10.3389/fpsyg.2024.1330439>
- CORNEJO-PLAZA, M. I., & SARACINI, C. (2023). On pharmacological neuroenhancement as part of the new neurorights' pioneering legislation in Chile: A perspective. *Frontiers in Psychology, 14*.
- DANI, A. (2014). *Le risorse naturali come beni comuni*. Accesible en: <https://art.torvergata.it/handle/2108/73867>
- DECHERCHI, S., PEDRINI, E., MORDENTI, M., CAVALLI, A., & SANGIORGI, L. (2021). Opportunities and challenges for machine learning in rare diseases. *Frontiers in Medicine, 8*. Accesible en: <https://doi.org/10.3389/fmed.2021.747612>
- DETERMANN, L. (2018). No one owns data. *SSRN Electronic Journal*. Accesible en: <https://doi.org/10.2139/ssrn.3123957>
- DEVINENI, S. K. (2023). Bridging the data divide: Secure sharing and governance for effective cross-agency and industry collaboration. *Journal of Artificial Intelligence & Cloud Computing, 1*(2). Accesible en: [https://doi.org/10.47363/jaicc/\(2\)188](https://doi.org/10.47363/jaicc/(2)188)

- DUCUING, C., & REICH, R. H. (2023). Data governance: Digital product passports as a case study. *Competition and Regulation in Network Industries*, 24(1), pp. 3–19. Accesible en: <https://doi.org/10.1177/17835917231152799>
- EUROPEAN COMMISSION. (2015). *Creating value through open data: Study on the impact of re-use of public data resources*. Publications Office of the European Union. Accesible en: [https://data.europa.eu/sites/default/files/creating\\_value\\_through\\_open\\_data\\_0.pdf](https://data.europa.eu/sites/default/files/creating_value_through_open_data_0.pdf)
- EUROPEAN COMMISSION. (2024). *European data market study 2024–2026*. Publications Office of the European Union. Accesible en: <https://digital-strategy.ec.europa.eu/es/library/european-data-market-study-2024-2026>
- FENNELL, L. A. (2011). Commons, anticommons, semicommons. In *Edward Elgar Publishing eBooks*. Accesible en: <https://doi.org/10.4337/9781849808972.00007>
- FUENTEALBA, N. J. (2021). El derecho de propiedad sobre los datos. *Revista Chilena de Derecho Privado, (temático)*, Santiago. Accesible en: <https://doi.org/10.4067/S0718-80722021000300101>
- GROSSMAN, R. L. (2023). Ten lessons for data sharing with a data commons. *Scientific Data*, 10(1). Accesible en: <https://doi.org/10.1038/s41597-023-02029-x>
- HOFFMANN, S. (2012). Property, possession and natural resource management: Towards a conceptual clarification. *Journal of Institutional Economics*, 9(1), pp. 39–59. Accesible en: <https://doi.org/10.1017/S1744137412000264>
- HRISTOVA, T., MAGEE, L., & KEARNEY, E. (2023). Academic institutions in multilateral data governance: Emerging arrangements for negotiating risk, value and ethics in the big data economy. *arXiv*. Accesible en: <https://doi.org/10.48550/arxiv.2301.12347>
- IRTI, N. (1984). *Norme e fatti*. Giuffrè.
- KERBER, W. (2016). ¿A new (intellectual) property right for non-personal data? An economic analysis. *RePEc: Research Papers in Economics*. Accesible en: <https://econpapers.repec.org/RePEc:mar:magkse:201637>

- MCGUIRE, A. L., ROBERTS, J., AAS, S., & EVANS, B. J. (2019). Who owns the data in a medical information commons? *The Journal of Law, Medicine & Ethics*, 47(1), pp. 62–69. Accesible en: <https://doi.org/10.1177/1073110519840485>
- NAGLE, F. (2018). The digital commons: Tragedy or opportunity? A reflection on the 50th anniversary of Hardin's tragedy of the commons. *SSRN Electronic Journal*. Accesible en: <https://doi.org/10.2139/ssrn.3301005>
- OCDE. (2007). *Glossary of statistical terms*. Accesible en: [http://ec.europa.eu/eurostat/ramon/coded\\_files/OECD\\_glossary\\_stat\\_terms.pdf](http://ec.europa.eu/eurostat/ramon/coded_files/OECD_glossary_stat_terms.pdf)
- OSTROM, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press.
- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (2022). *Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)*. Diario Oficial de la Unión Europea, L 152, pp. 1–44. Accesible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R0868>
- PERUCCI, F., & SWANSON, E. (2024). Building trust and facilitating use of data. *Statistical Journal of the IAOS*, 40(1), pp. 71–82. Accesible en: <https://doi.org/10.3233/SJI-240006>
- PEUKERT, A. (2008). *Guterzuordnung als Rechtsprinzip*. Tübingen.
- REICH, C. A. (1964). The new property. *Yale Law Journal*, 73, pp. 733–787.
- ROMEU I CÓNSUL, R. (2019). Las nuevas bases de datos: Big Data, desestructuración e inteligencia artificial. In S. Navas Navarro (Dir.), *Nuevos desafíos para el derecho de autor: Robótica, inteligencia artificial y tecnología* (pp. 199–216). Editorial Beus.
- UNIÓN EUROPEA. (2019). *Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales*. Diario Oficial de la Unión Europea. Accesible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019L0770>
- UNIÓN EUROPEA. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas*

*en materia de inteligencia artificial y se modifican los Reglamentos (CE) n.º 300/2008, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). Diario Oficial de la Unión Europea, L 207, 12.7.2024, p. 1-234. Accesible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689>*

VALK, O. M. C. VAN DER, & RYAN, M. (2025). Data for the common good in the common European data space. *Data & Policy*, 7, e5. Accesible en: <https://doi.org/10.1017/dap.2025.5>

VAYENA, E., SALATHÉ, M., MADOFF, L. C., & BROWNSTEIN, J. S. (2015). Ethical challenges of big data in public health. *PLoS Computational Biology*, 11(2).



**Todas nuestras actividades en:**  
**[www.derecho.uba.ar/institucional/centro-estudios-integracion-regional-y-ddhh/](http://www.derecho.uba.ar/institucional/centro-estudios-integracion-regional-y-ddhh/)**