

HACIA UN ESPACIO EUROPEO DE DATOS: LECCIONES DE LA CECA PARA SUPERAR LA FRAGMENTACIÓN DIGITAL ANTE LA EMERGENCIA DE LOS SISTEMAS COMPUTACIONALES PLANETARIOS

TOWARDS A EUROPEAN DATA SPACE: LESSONS FROM ECSC TO OVERCOME DIGITAL FRAGMENTATION IN THE AGE OF PLANETARY COMPUTATIONAL SYSTEMS

Joaquín David Rodríguez Álvarez*

RESUMEN: Este artículo analiza la fragmentación digital en la Unión Europea (UE) y sus implicaciones para la soberanía tecnológica en un contexto global marcado por la competencia entre modelos regulatorios. En primer lugar, se examinan los antecedentes normativos europeos y las dificultades que presentan para consolidar un espacio único de datos. A continuación, se aborda la emergencia de los sistemas computacionales planetarios y los obstáculos que genera la falta de interoperabilidad, tanto a escala global como europea. El trabajo contrasta el enfoque descentralizado de la UE con el modelo centralizado de China, que considera los datos un «activo nacional», destacando sus ventajas operativas y los riesgos que

* Profesor Lector, Miembro del Consejo Directivo de la Cátedra Manuel Ballbé en Seguridad Humana y Derecho Global, Departamento de Derecho Público y Ciencias Histórico-Jurídicas, Facultad de Derecho, Universitat Autònoma de Barcelona. Correo electrónico: joaquin.rodriguez@uab.cat ORCID: <https://orcid.org/0000-0002-0524-4501>. El autor agradece al Dr. Carlos Padrós Reig y a la Dra. Roser Martínez Quirante por su apoyo y valiosos consejos durante la elaboración de este artículo. El presente trabajo no ha contado con ninguna financiación directa o indirecta procedente de entidad alguna, pública o privada, con o sin ánimo de lucro. El autor declara no tener ningún conflicto de interés.

plantea para los derechos fundamentales. Sobre esta base, se argumenta que la experiencia histórica de la Comunidad Europea del Carbón y del Acero (CECA) constituye un precedente útil para superar la fragmentación digital mediante mecanismos de soberanía compartida. Finalmente, se proponen medidas concretas: creación de una Agencia Digital Europea con competencias ejecutivas, federalización de datos estratégicos y adopción de normas vinculantes, complementadas con una diplomacia digital orientada a la defensa de valores democráticos. La conclusión subraya que, sin una arquitectura institucional robusta inspirada en el legado de la CECA, la UE corre el riesgo de quedar relegada en la gobernanza mundial de la inteligencia artificial y los datos.

PALABRAS CLAVE: Unión Europea; fragmentación de datos; inteligencia artificial; soberanía digital

ABSTRACT: This article examines digital fragmentation in the European Union (EU) and its implications for technological sovereignty in a global context marked by regulatory competition. First, it reviews the EU's regulatory framework and the challenges these instruments face in consolidating a single data space. It then addresses the emergence of planetary computational systems and the obstacles created by the lack of interoperability, both globally and within Europe. The paper contrasts the EU's decentralized approach with China's centralized model, which treats data as a «national asset», highlighting its operational advantages and the risks it poses to fundamental rights. Building on this comparison, the article argues that the historical experience of the European Coal and Steel Community (ECSC) provides a useful precedent for overcoming digital fragmentation through mechanisms of shared sovereignty. Finally, it proposes concrete measures: the creation of a European Digital Agency with executive powers, the federalization of strategic data, and the adoption of binding standards, complemented by a digital diplomacy strategy aimed at safeguarding democratic values. The conclusion stresses that without a robust institutional architecture inspired by the ECSC legacy, the EU risks being sidelined in the global governance of artificial intelligence and data.

KEYWORDS: European Union; data fragmentation; artificial intelligence; digital sovereignty.

SUMARIO: INTRODUCCIÓN. – 1. ONTOLOGÍA DE LA CRISIS: DATOS HUMANOS, SINTÉTICOS Y EL FANTASMA DE LA CECA: 1.1. Fundamentos estratégicos y diseño de gobernanza en la Unión Europea; 1.2. La CECA como Precedente Histórico de Integración Estratégica vs la Integración de Datos; 1.3. Los datos como recurso estratégico en la economía digital: Federalización, escasez no-sintética y ontología jurídica. 1.3.1. Datos generados por humanos: La paradoja de la escasez en la abundancia; 1.3.2. Datos sintéticos: Entre la promesa de infinitud y la ontología jurídica vacante.— 2. FRAGMENTACIÓN DE DATOS Y SISTEMAS COMPUTACIONALES PLANETARIOS: 2.1. Sistemas Computacionales Planetarios: Un Desafío Jurídico Transnacional; 2.2. Requisitos Operativos de los SCP – Del soft and hard law, 2.3. La guerra silenciosa por los estándares; 2.4. Fragmentación en la Unión Europea: Manifestaciones.— 3. FRONTERAS DIGITALES

EN LA REGULACIÓN DE LA IA: 3.1. El Enfoque de la UE: Regulación de la IA como Producto; 3.2. China: La IA como Infraestructura de Estado y Control Centralizado.— 4. HACIA UN ESPACIO DIGITAL EUROPEO: PROPUESTAS DESDE EL LEGADO DE LA CECA: 4.1. Lecciones Históricas: La CECA como Modelo de Soberanía Compartida; 4.2. Dimensión Geopolítica y ética: de la Diplomacia de Estándares a la IA como Bien Público.— CONCLUSIÓN: UN NUEVO CONTRATO SOCIAL PARA LA ERA DIGITAL.— BIBLIOGRAFÍA

1. ONTOLOGÍA DE LA CRISIS: DATOS HUMANOS, SINTÉTICOS Y EL FANTASMA DE LA CECA

«Europa se forjará en las crisis,
y será la suma de las soluciones adoptadas para esas crisis».

Jean Monnet (1967)

Nuestro presente se encuentra anclado en una crisis multinivel —climática, política y social— que exige intervención a fin de mitigar sus potenciales efectos. Según el *Servicio de Cambio Climático de Copernicus*, Europa registra un aumento de 1,5° C en su temperatura media desde 1990, agravando fenómenos extremos como sequías o inundaciones entre otros (Copernicus 2025), tal y como sucedió en Valencia en el año 2024. Además, políticamente, solo el 51 por 100 de los ciudadanos de la UE confían en sus instituciones (European Union 2024), mientras el 21,7 por 100 de la población vive en riesgo de pobreza o exclusión social (Eurostat 2024), cifras que reflejan una erosión acelerada del contrato social. Unos indicadores que, si son extrapolados a escala global, solo representan la punta del iceberg de un conjunto de crisis sistémicas que afectan a la totalidad del planeta, y cuya visión y comprensión se encuentran limitadas por un complejo mosaico de regulaciones y silos que afectan a la federación de datos y la interoperabilidad de los sistemas computacionales. Y, por tanto, nuestra capacidad de análisis y resolución de los retos que enfrentamos (Catanzariti 2024).

Así, el presente artículo aborda cómo los sistemas planetarios computacionales —conceptualizados por Bratton (2017) en su obra *The Stack*, como una megaestructura accidental de capas interdependientes que articulan lo tecnológico, lo geopolítico y lo ambiental— están llamados a desempeñar un papel crucial frente a algunos de los retos más acuciantes de nuestra era, como el cambio climático, la gobernanza algorítmica o la soberanía digital¹.

¹ Bratton describe *The Stack* como, una arquitectura planetaria accidental emergente compuesta por seis capas interrelacionadas: Tierra, Nube, Ciudad, Dirección, Interfaz y Usuario. Donde el termino accidental se refiere a que estructura no fue diseñada de forma centralizada ni planificada con una lógica unificada, sino que emergió de manera fragmentaria y contingente, como resultado de múltiples decisiones técni-

En este sentido, *The Stack* no solo describe una arquitectura técnica, sino también una nueva forma de soberanía distribuida, que encontraría precedentes teóricos en aproximaciones de tipo neo-medieval (Rodríguez-Alvarez 2023; Cerny 2007), donde el poder y la soberanía ya no residiría exclusivamente en los Estados-nación, sino que estos se encuentran en estados de competencia y colaboración con otros *stakeholders*, además de plataformas, protocolos y algoritmos que operan a escala planetaria. Esta condición plantea desafíos fundamentales para el derecho internacional, que aún se estructuran en torno a lógicas territoriales y soberanías estatales.

Sin embargo, estos sistemas enfrentan significativas barreras de integración y competitividad, tanto bajo el derecho internacional como bajo el derecho de la Unión Europea, lo que contribuye a una creciente fragmentación normativa y operativa. En este sentido, el eje central del presente artículo radica en la tensión entre el reconocimiento de los datos como recurso estratégico —clave para el desarrollo de la inteligencia artificial y la economía digital— y los marcos jurídicos que, en su intento por proteger derechos fundamentales y valores democráticos, terminan por obstaculizar su explotación eficiente en el contexto de la carrera tecnológica global.

Y, aunque si bien es cierto que la legislación europea más reciente intenta corregir estos desequilibrios a nivel interno, la realidad es que todavía enfrenta limitaciones profundas. Así el Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689) que se configura como el primer marco global para regular la IA en la Unión Europea enfrenta problemas que van desde la definición de la IA como producto, a la comprensión de sistemas dinámicos. Mientras que el reglamento de gobernanza de datos (Reglamento (UE) 2022/868) diseñado para impulsar el intercambio de datos públicos colisiona en ocasiones con el RGPD tal y como observaremos más adelante.

En este sentido, es necesario destacar que la Unión Europea (UE) ha emprendido una transformación estructural para establecer un mercado único de datos que posicione a Europa como líder global en la economía de datos (CE, n.d.-b). Esta iniciativa, articulada mediante instrumentos normativos, arquitecturas de gobernanza e inversiones estratégicas, responde a la convicción de que los datos son un recurso no rival cuyo valor aumenta con su uso compartido y ético (CE, n.d.-a). Por lo que el modelo europeo prioriza por tanto el control ciudadano sobre los datos, la equidad competitiva y el alinea-

cas, económicas y políticas tomadas a lo largo del tiempo por actores diversos —desde gobiernos hasta corporaciones tecnológicas y comunidades de usuarios.

Es decir, la noción de «accidental» no implicaría por tanto que sea fortuito o caótico, sino que no responde a un diseño deliberado, sino a una acumulación de infraestructuras que, al interactuar, producen una forma de gobernanza algorítmica global. Esta megaestructura articula desde los recursos materiales (como minerales y energía en la capa Tierra), hasta las plataformas digitales que median nuestras interacciones cotidianas (como la capa Interfaz o Usuario), pasando por infraestructuras críticas como los centros de datos, redes de telecomunicaciones y sistemas de identificación.

miento con valores fundamentales como la privacidad, la transparencia y la sostenibilidad.

1.1. Fundamentos estratégicos y diseño de gobernanza en la Unión Europea

El Espacio Europeo de Datos surge como una iniciativa estratégica anunciada en la Comunicación de la Comisión Europea «Una Estrategia Europea de Datos» (COM(2020) 66 final), cuyo objetivo es crear un mercado único de datos que refuerce la soberanía digital y la competitividad de la Unión. Esta estrategia se articula en torno a la creación de espacios comunes europeos de datos en sectores clave —salud, energía, movilidad, industria, administración pública—, ampliados posteriormente a catorce dominios incluidos patrimonio cultural, turismo e idiomas (CE 2020), con el fin de garantizar la interoperabilidad, la reutilización y la confianza en el intercambio transfronterizo de datos.

Estos espacios son ecosistemas sectoriales interconectados que operan bajo principios comunes:

- Soberanía del titular: Control efectivo por parte de empresas, administraciones o ciudadanos sobre quién accede a sus datos y en qué condiciones.

- Infraestructura confiable: Uso de tecnologías de privacidad (PETs) y seguridad *by design* para el intercambio seguro.

- Acceso no discriminatorio: Reglas transparentes, proporcionales y justas para todos los participantes.

- Modelos de compensación flexible: Posibilidad de compartir datos gratuitamente, mediante licencias o acuerdos *quid-pro-quo*.

Una arquitectura donde el Comité Europeo de Innovación en Datos (CEDI), establecido por la Ley de Gobernanza de Datos (Data Governance Act, DGA), supervisa la armonización de estándares y emite directrices para garantizar coherencia intersectorial (European Commission 2024b; CE, n.d.-b). De esta forma, podemos observar que la UE ha comenzado a desplegar un marco jurídico *ad hoc* para materializar dicha visión conformado por:

- Data Governance Act (DGA): Entró en vigor en 2022 para fomentar el altruismo de datos mediante organizaciones certificadas y regular a los intermediarios. Crea el Registro Europeo de Datos Protegidos del Sector Público.

- Data Act (DA): Aplicable desde enero de 2024, regula el acceso y uso de datos generados por productos conectados (IoT), permitiendo a usuarios y empresas acceder, compartir y portar datos.

- Reglamento del Espacio Europeo de Datos Sanitarios (EHDS): Adoptado en enero de 2025, establece interoperabilidad obligatoria de historias clínicas electrónicas y acceso transfronterizo para pacientes e investigadores (CE 2025c).

Este *corpus* normativo se complementa con la supervisión de autoridades nacionales para garantizar el cumplimiento de RGPD, y normas de competencia y protección al consumidor. Dando pie a una arquitectura técnica que se sustenta en la creación de *Building blocks* europeos, componentes de código abierto como el middleware SIMPL² (CE 2025), que proveen funciones básicas de identidad, catálogo o contratos digitales. A lo que se sumaría el Centro de Apoyo a Espacios de Datos (DSSC), el cual ofrece especificaciones de interoperabilidad, semántica común y asesoramiento para despliegues sectoriales (CE 2025a). Además del Programa Europa Digital (CE 2025b) y Horizonte Europa (CE, n.d.-c).

Situar estos instrumentos en una narrativa de integración es decisivo para el hilo conductor del trabajo: del mismo modo que la CECA articuló un mercado común de recursos estratégicos bajo una autoridad supranacional, los mecanismos anteriores pretenden cimentar un espacio europeo de datos. La pregunta central es si, con el diseño actual, basta la coordinación intergubernamental o si resulta necesaria una capacidad ejecutiva supranacional análoga a la de la CECA.

Y es que, pese al esfuerzo realizado, todavía persisten retos críticos pudiendo destacar: la fragmentación de estándares (Gaia-X vs IDSA), la inclusión de PYMEs y la interconexión efectiva entre espacios para formar un mercado único fluido. La UE aborda esto mediante la labor del CEDI en directrices de interoperabilidad y el fomento de contratos de compartición basados en FAIR³.

De tal forma que el contexto actual y su dinámica de desarrollo nos permite observar que la Unión Europea navega por un dilema existencial: generar un espacio digital consolidado para competir globalmente o sucumbir a la fragmentación digital. Los datos, recurso estratégico del siglo XXI, demandan un marco jurídico unificado que trascienda fronteras y priorice la soberanía digital a través de la creación de organismos federados. Sin ello, el riesgo no

² Smart Open-source Middleware Platform. SIMPL es una plataforma de middleware de código abierto e inteligente, lo que significa, que es un software intermedio que conecta diferentes sistemas, aplicaciones o servicios, permitiendo que se comuniquen entre sí de forma eficiente. Su código fuente está disponible públicamente, lo que permite a instituciones, empresas o desarrolladores adaptarlo, auditarlo y reutilizarlo libremente. Incorpora capacidades avanzadas como automatización, interoperabilidad semántica, y posiblemente algoritmos de IA para facilitar la gestión de datos.

³ El principio FAIR —acrónimo de *Findable, Accessible, Interoperable, Reusable*— fue formulado para guiar la gestión responsable de datos científicos y digitales. Propone que los datos deben ser localizables mediante metadatos estandarizados, accesibles bajo condiciones claras (incluso si requieren autenticación), interoperables mediante formatos y vocabularios comunes, y reutilizables con licencias explícitas y documentación adecuada. Estos principios, ampliamente adoptados por la Unión Europea en el diseño de espacios de datos sectoriales, buscan maximizar el valor social, científico y económico de los datos compartidos.

es solo la pérdida económica, sino la irrelevancia en un orden mundial dictado por quien controle los flujos de información. Un dilema, cuya resolución nos obliga a volver la vista atrás sobre nuestra propia arquitectura jurídico institucional, y los esfuerzos de integración que le dieron forma.

Ya que, pese a los avances realizados, la arquitectura actual presenta limitaciones estructurales: la fragmentación normativa entre Estados miembros, la falta de mecanismos vinculantes para la interoperabilidad y la ausencia de una autoridad supranacional con competencias ejecutivas. Estas carencias contrastan con la lógica de integración que inspiró la Comunidad Europea del Carbón y del Acero, lo que plantea la pregunta central de este trabajo: ¿puede la UE replicar, en el ámbito digital, el modelo de soberanía compartida que permitió superar la fragmentación en sectores estratégicos durante el siglo XX?

1.2. La CECA como Precedente Histórico de Integración Estratégica vs la Integración de Datos

La Unión Europea (UE) se construyó sobre la premisa de que la cooperación en sectores estratégicos podía prevenir conflictos y garantizar una paz y prosperidad duradera para el continente a través de la creación de un sistema de interdependencia compleja, semilla de la actual arquitectura jurídico-institucional. De esta forma, el Tratado de la CECA (CECA 1951), firmado en 1951 por seis Estados (Bélgica, Alemania Occidental, Francia, Italia, Luxemburgo y los Países Bajos), no solo reguló la producción de dos recursos clave para la industria (bélica), carbón y acero, sino que estableció un modelo pionero de soberanía compartida. Su Capítulo I, Art 8 y 9 creó una «Alta Autoridad» supranacional con competencias para imponer decisiones vinculantes, armonizar estándares y redistribuir excedentes entre países. Este mecanismo, impulsado por los padres fundadores de la Unión, entre ellos Jean Monnet y Robert Schuman, demostró que la integración era viable cuando los Estados cedían competencias en áreas críticas.

Si bien ahora, 70 años después, los datos han emergido como el equivalente digital del carbón y el acero: un recurso estratégico que alimenta desde la inteligencia artificial (IA) hasta la ciberseguridad, además de suponer la base de los sistemas computacionales planetarios, clave para resolver, tal y como ya hemos anunciado previamente, algunos de los problemas más acuciantes, como el cambio climático. Pudiendo así comprender que Europa se enfrenta un desafío similar al de 1951: gestionar este recurso estratégico en un marco fragmentado, donde las soberanías nacionales chocan con la necesidad de un mercado único digital, aunque el camino actual dista mucho de la aproximación que se tomó en la década de los 50 del siglo pasado (Lin, 2024).

La referencia a la CECA no es, por tanto, una metáfora histórica, sino una hipótesis institucional concreta. La Alta Autoridad de la CECA combinó poderes ejecutivos (armonización, decisiones vinculantes y facultad sancio-

nadora) con un mandato funcional sobre recursos críticos. La analogía operativa con los datos e infraestructuras digitales actuales reside en que ambos son insumos transversales cuyo aprovechamiento eficiente exige interdependencia regulada. La diferencia contextual —posguerra industrial frente a competencia tecnológica global— no resta validez al precedente, sino que subraya la necesidad de adaptar su lógica: soberanía compartida, reglas comunes exigibles y capacidad de decisión supranacional.

Así, mientras China ha optado por un modelo centralizado, declarando la IA «infraestructura nacional» en su *Plan de Desarrollo de la Nueva Generación de IA* (CERPC 2017), la UE navega entre la idea federal y las realidades políticas de sus Estados miembros creando un mosaico que dificulta la integración estratégica necesaria de este recurso, considerando además los sistemas de IA, como producto, con las subsecuentes implicaciones legales que abordaremos en próximas secciones.

De esta forma, es necesario tener en cuenta que, aunque el Reglamento General de Protección de Datos (RGPD), en vigor desde 2018, heredó el espíritu federalista de la CECA al aspirar a un marco uniforme para gestionar los datos —el «carbón del siglo XXI»— como recurso transnacional, su aplicación ha expuesto fisuras análogas a las que la CECA intentó sellar en los años 50. Mientras la CECA creó una Alta Autoridad con competencias vinculantes para armonizar la producción industrial en lo que podríamos clasificar como un modelo supranacional puro, o de decisión centralizada, el RGPD —y su extensión natural, el Reglamento sobre IA (2024)— opera bajo lo que podríamos definir como un modelo cooperativo: normas comunes diseñadas en Bruselas, ejecutadas por autoridades nacionales, bajo supervisión europea. Es decir, estamos ante un modelo híbrido que no cede interpretaciones esenciales, pero cuyo enfoque basado en la cooperación multinivel, debido a su flexibilidad intrínseca, permite que surjan asimetrías jurídicas (Lin, n.d.) algunas de las cuales van directamente relacionadas con la dotación de recursos y personal de los garantes nacionales.

La fisura, se agrava, además, por la propia velocidad del sistema tecnológico. La innovación en IA o *Big Data* avanza a ritmos exponenciales, exigiendo marcos de armonización mucho más ágiles que los que provee la maquinaria legal de la UE. Mientras un caso judicial tarda años en escalar desde tribunales nacionales al Tribunal de Justicia de la UE (TJUE), una tecnología disruptiva puede haber redefinido mercados enteros, dejando obsoletas las normas diseñadas para regularla. El Reglamento sobre IA de 2024, aunque ambicioso, corre el riesgo de quedar desfasado, sin mecanismos dinámicos para actualizar sus cláusulas ante avances imprevistos.

Este desfase temporal no solo perpetúa la tendencia hacia los silos y la fragmentación de datos, sino que erosiona la competitividad europea. Diluyendo la aspiración de una soberanía digital frente a potencias como EE.UU. o China, cuyos modelos —aunque criticables en aspectos éticos— operan con mayor celeridad y coherencia interna. La pregunta crítica, entonces, es si la

UE debería resucitar el modelo federalista de la CECA —federalismo jerárquico— mediante una «Alta Autoridad Digital» con poderes vinculantes, o si, por el contrario, aceptará que la subsidiariedad nacional y la aceleración tecnológica condenen su espacio digital a la fragmentación crónica.

Fenómeno que se materializaría en la gestación de un paisaje interpretativo fragmentario que se puede ejemplificar a través de diferentes sentencias: así en 2023, un tribunal de Colonia prohibió el uso de *Google Analytics* por transferencias ilegales a EE.UU., interpretando la dirección IP como dato personal bajo criterios maximalistas (Cologne Regional Court 2023), mientras que las autoridades en Países Bajos aplicaron una aproximación más flexible de la misma norma para permitir el flujo de datos agrícolas, priorizando la innovación sectorial (NextCloud 2022). Estas discrepancias no son meramente técnicas, sino sintomáticas de una tensión filosófica entre privacidad como derecho fundamental- Art 8. De la Carta de Derechos fundamentales de la UE, reforzado por el RGPD y datos como motor económico («Estrategia Europea de Datos - Comisión Europea» 2025) —una dicotomía que el Reglamento de Gobernanza de Datos (UE) 2022/868 no resuelve, al promover espacios sectoriales voluntarios sin mecanismos vinculantes (art. 11) (European Commission, 2024).

Este modelo contrasta, tal y como comentábamos previamente, con el enfoque de China, donde la Ley de Seguridad de Datos (2021) define los datos como «activo nacional» (art. 3) (DigiChina 2021), centralizando su control bajo parámetros estatales y proyectándolos globalmente mediante iniciativas como la Nueva Ruta de la Seda Digital, que integra datos de socios internacionales bajo estándares chinos (Nadia 2024). De esta forma, la regulación china exige que todos los proveedores de IA (no solo los de alto riesgo) registren sus sistemas ante el Estado, independientemente del sector o nivel de riesgo. Además, las leyes chinas, como la *Personal Information Protection Law* (PRC 2021), limitan la recolección de datos por empresas privadas, pero otorgan al Estado acceso ilimitado a la información, reforzando la noción de datos como activo nacional interoperable.

Mientras tanto, la UE lucha por conciliar soberanías nacionales en un marco post-CECA debilitado —sin una autoridad supranacional con poderes ejecutivos—, China avanza con un modelo cohesivo que replica, en clave digital, el centralismo jerárquico de la planificación soviética. La paradoja es histórica: la CECA surgió para evitar que el carbón y el acero alimentaran rivalidades; hoy, la UE arriesga que sus datos —y su gobernanza fragmentada— alimenten la dependencia tecnológica. Sin una Alta Autoridad de Datos con competencias análogas a las de la CECA, el sueño federalista podría ceder ante modelos autoritarios que, como China, entienden que, en la era digital, la soberanía no se negocia: se ejerce.

El Reglamento de Gobernanza de Datos ((UE) 2022/868), con sus espacios sectoriales no vinculantes (art. 11), refleja esta ambivalencia: aspira a ser la CECA del siglo XXI, pero sin su columna vertebral institucional. Ya que tal

y como se establece en el Reglamento (UE) 2022/868 el Comité Europeo de Innovación en materia de Datos se estructura como un órgano consultivo sin carácter ejecutivo.

La lección histórica parece ser clara: sin una autoridad supranacional con poderes ejecutivos —no meramente coordinadores—, la UE arriesga que sus datos, como antaño su carbón, se conviertan en campo de batalla de intereses fragmentados, minando su soberanía digital frente a modelos autoritarios cohesionados. Una divergencia jurídica, que agudiza la bifurcación tecnológica y geopolítica. Si bien, y antes de continuar sobre la problemática central del tema tratado, sería necesario realizar un breve inciso, para abordar la comprensión de los datos atendiendo a su generación y ontología como fase previa a avanzar sobre nuestro marco teórico.

1.3. Los datos como recurso estratégico en la economía digital: Federalización, escasez no-sintética y ontología jurídica

La analogía histórica entre los recursos materiales que sustentaron la integración europea bajo la CECA (1951) y los datos en la era digital no es meramente retórica, sino epistemológicamente fértil. Al igual que el carbón y el acero fungieron como insumos transversales para la industria bélica y civil —y, por tanto, como objetos de regulación supranacional—, los datos constituyen hoy el *substrato operativo* de la inteligencia artificial, la gobernanza algorítmica y la innovación tecnológica. Sin embargo, su naturaleza inmaterial y su dualidad ontológica —como *bien económico no rival* (por su capacidad de replicación ilimitada) y *bien jurídico rival* (por su vinculación a derechos fundamentales como la privacidad)— los sitúan en un paradigma regulatorio sin precedentes. Siendo además necesario explorar la tensión entre la escasez práctica de datos generados por humanos y la abundancia artificial de datos sintéticos, a fin de proponer comprender su naturaleza.

1.3.1. Datos generados por humanos: La paradoja de la escasez en la abundancia

Los datos producidos por interacciones humanas —desde transacciones electrónicas hasta registros biométricos— poseen un valor estratégico derivado de su *autenticidad epistémica*: reflejan patrones sociales, culturales y económicos únicos. No obstante, su explotación enfrenta límites asintóticos. Técnicamente, la recolección masiva choca con la ley de rendimientos decrecientes (Leonelli 2016) en minería de datos⁴. Este fenómeno, descrito en la teoría eco-

⁴ A medida que se extraen los conjuntos de datos más accesibles (p. ej., comportamientos en redes sociales), incrementa exponencialmente el coste marginal para obtener información novedosa o de nicho.

nómica como *agotamiento de recursos de acceso abierto* (Karpó 2022; Feeny *et al.* 1990; Frischmann *et al.* 2019), se ve agravado por restricciones jurídicas. El Reglamento General de Protección de Datos (RGPD) de la UE, por ejemplo, permite a los individuos controlar o restringir el uso de sus datos personales (Derecho a la oposición —Art 21—, Derecho a la supresión «olvido» —Art 17—, Derecho a limitar el tratamiento —Art 18—) transformándolos en un recurso escaso no por física limitación, sino por diseño normativo.

De esta forma, la escasez práctica de datos humanos plantea un dilema de acción colectiva: mientras las empresas tecnológicas los tratan como *commodities privatizables* bajo regímenes de propiedad intelectual, algunos Estados defienden su carácter de *interés público* vinculado a la soberanía digital (Zuboff 2019). Esta tensión exige mecanismos de gobernanza que trasciendan el paradigma westfaliano. La federalización de datos —entendida como la creación de instituciones supranacionales con competencias para arbitrar entre derechos individuales, innovación y seguridad— emerge como solución, pero requiere superar un obstáculo técnico-jurídico: cómo garantizar flujos transfronterizos sin erosionar las garantías del RGPD ni caer en el colonialismo de datos⁵ (Mejías and Couldry 2019).

1.3.2. *Datos sintéticos: Entre la promesa de infinitud y la ontología jurídica vacante*

Frente a la escasez humana, los datos sintéticos⁶ se presentan como un *recurso post-escasez*. Su valor reside en la capacidad de emular distribuciones estadísticas de datos reales sin contener información identificable, resolviendo así el trilema entre privacidad, utilidad y acceso (Jordon *et al.* 2022). Empresas como OpenAI o NVIDIA los emplean para entrenar modelos de IA en entornos controlados, desde diagnósticos médicos hasta vehículos autónomos. Sin embargo, esta aparente solución encierra una paradoja técnica: los datos sintéticos no son ontológicamente autónomos, sino *meta-recursos* dependientes de la calidad y diversidad de los datos originales. El llamado *problema del espejo*⁷ (van den Broek, Sergeeva, and Huysman 2021) ilustra este

⁵ El término *colonialismo de datos* hace referencia a una dinámica en la que grandes corporaciones tecnológicas o Estados con capacidad de extracción masiva de información imponen sus infraestructuras, estándares y modelos de gobernanza sobre comunidades menos capacitadas para controlar sus propios datos. Según Mejías y Couldry (2019), esta forma de colonialismo no se basa en la ocupación territorial, sino en la apropiación de datos generados por individuos y colectivos, transformándolos en valor económico sin redistribución equitativa ni consentimiento informado. En este marco, los datos se convierten en instrumentos de poder asimétrico, reproduciendo lógicas extractivistas propias del colonialismo histórico.

⁶ Datos generados mediante redes generativas antagónicas (GANs), simulaciones estocásticas o modelos de lenguaje; ejem. ChatGPT.

⁷ El problema del espejo, tal como lo describen van den Broek, Sergeeva y Huysman (2021), se refiere a un riesgo inherente en el uso de datos sintéticos generados

riesgo: si el conjunto de entrenamiento inicial está sesgado (p. ej., subrepresentando minorías étnicas), los datos sintéticos replicarán —y amplificarán— dichos sesgos, perpetuando exclusiones estructurales (Martínez-Quirante and Rodríguez-Álvarez 2020; Martínez-Quirante and Rodríguez-Álvarez 2018; Rodríguez 2016; Rodríguez *et al.* 2019).

Además, es importante tener en cuenta que jurídicamente, los datos sintéticos habitan un limbo normativo. La Directiva de Derechos de Autor de la UE (2001/29/CE) (European Commission 2019) no reconoce autoría no humana, dejando vacante la titularidad sobre datos generados algorítmicamente, lo que a su vez se alinea con casos como la decisión del Tribunal de Justicia de la UE en *Brompton Bicycle* (2020) —ECLI:EU:C:2020:46—, que reiteró la necesidad de originalidad humana para la protección.

Esto nos permite preguntarnos si un dato sintético pertenecer a quien posee el modelo generativo, a quien aportó los datos de entrenamiento o al usuario que activó el proceso. Esta incertidumbre, analizable bajo la teoría de los *derechos de propiedad fraccionados* (Heller 1998), explica cómo la superposición de derechos (ej. entrenamiento vs. generación) genera una «tragedia de los anticomunes»⁸, donde nadie puede explotar el recurso eficientemente. Para los datos sintéticos, esto se traduce en barreras para su comercialización o uso en mercados formales.

Ante esto se abren diversas posibilidades teóricas ante nosotros, como la de un reconocimiento de los datos humanos y sintéticos como pertenecientes a categorías jurídicas distintas. Los primeros, como asociados a *derechos fundamentales* (vinculados a la dignidad humana - RGPD, art. 8 Carta de Derechos Fundamentales), y los segundos, como *bienes comunes artificiales* (sujetos a regulación de mercado, pero con salvaguardias anti-monopólicas). Premisa sobre la cual se podrían estructurar «contratos sociales de acceso condicional», inspirados en la teoría de los *commons* de Elinor Ostrom (Gardner, Ostrom, and Walker 1990). Estos contratos regularían el uso de datos humanos bajo licencias proporcionales (p. ej., acceso a cambio de inversión en bien público) y podrían establecer cuotas éticas para datos sin-

por sistemas de inteligencia artificial, especialmente en procesos como la contratación automatizada. Esto se debe a que los datos sintéticos se crean a partir de conjuntos de datos reales mediante técnicas como redes generativas antagónicas (GANs). Aunque no contienen información personal directa, replican las distribuciones estadísticas de los datos originales. El problema del espejo surge cuando; el conjunto de datos original está sesgado (por ejemplo, subrepresenta a ciertas minorías), cuando los datos sintéticos replican y amplifican esos sesgos, o cuando el sistema de IA refleja (como un espejo) las desigualdades estructurales del mundo real, en lugar de corregirlas.

⁸ La tragedia de los anticomunes, formulada por Michael A. Heller en 1998, es un concepto jurídico-económico que describe una situación inversa a la famosa «tragedia de los comunes». Así, mientras que en la tragedia de los comunes un recurso compartido se sobreexplota porque nadie tiene incentivos para conservarlo, en la tragedia de los anticomunes ocurre lo contrario: un recurso no se utiliza eficientemente porque demasiadas personas tienen derechos de exclusión sobre él.

téticos (requiriendo p. ej. diversidad en conjuntos de entrenamiento). Todo ello integrado en infraestructuras técnicas interoperables: Sistemas de compartición de datos basados en *soberanía federada*, donde los Estados deleguen custodia —no propiedad— a entidades supranacionales, usando tecnologías como blockchain para auditorías trazables y cifrado homomórfico⁹.

En suma, la tensión entre derechos fundamentales, innovación y competencia no puede resolverse solo con coordinación blanda. Si los datos constituyen el sustrato operativo de la economía digital, la respuesta institucional debe elevarse al nivel de recurso estratégico, tal y como ocurrió con el carbón y el acero: reglas uniformes exigibles y un centro ejecutivo europeo capaz de garantizar interoperabilidad y acceso equitativo.

Finalmente, y antes de dar paso a la siguiente sección, sería necesario señalar, que la federalización de datos no es solo un desafío técnico o legal, sino un imperativo filosófico en la tradición ilustrada de Kant: superar el estado de naturaleza hobbesiano en el ciberespacio mediante instituciones que aseguren la paz y la cooperación. Los datos, a diferencia del carbón, no se agotan al quemarlos, pero su explotación irrestricta puede incinerar el tejido social. La tarea es construir una *lex data* que, como el Tratado de la CECA, trascienda intereses nacionales sin obliterar la diversidad. En ello nos va no solo la eficiencia económica, sino la supervivencia de un contrato social digno de la era digital.

2. FRAGMENTACIÓN DE DATOS Y SISTEMAS COMPUTACIONALES PLANETARIOS

2.1. Sistemas Computacionales Planetarios: Un Desafío Jurídico Transnacional

Los sistemas computacionales planetarios (SCP) representan infraestructuras digitales de alcance global, capaces de integrar redes distribuidas de datos, dispositivos del Internet de las Cosas (IoT) y algoritmos de inteligencia artificial (IA) en tiempo real. Es decir, representan una aspiración paradigmática de nuestra era digital (Bratton 2023; 2017): la capacidad de construir redes integradas de sistemas informáticos que puedan operar a escala global, permitiéndonos abordar los desafíos más apremiantes que enfrenta la humanidad. Estas arquitecturas computacionales interconectadas tienen el potencial de revolucionar campos como la salud, la gestión de emergencias, la logística o la administración de recursos naturales, al ofrecer una visión holística y en tiempo real de fenómenos complejos.

⁹ Técnica que permite realizar operaciones matemáticas sobre datos cifrados sin necesidad de descifrarlos para preservar privacidad

Sin embargo, la realidad actual se encuentra lejana de este ideal, pues la fragmentación de los datos y la persistencia de silos de información obstaculizan gravemente el pleno desarrollo de estos sistemas. De esta forma, la incapacidad de integrar y compartir datos de manera eficiente entre diferentes plataformas y jurisdicciones limita nuestra comprensión de los problemas a escala planetaria, comprometiendo nuestra capacidad para tomar decisiones informadas y generar soluciones sistémicas. Si queremos materializar el potencial transformador de los Sistemas Computacionales Planetarios, debemos abordar con urgencia los obstáculos derivados de la fragmentación de datos, pues solo así podremos aprovechar su verdadero potencial para el beneficio de la humanidad.

De esta forma, en el momento actual, el ideal técnico de integración global de datos tropieza con límites jurídicos y de gobernanza que, en Europa, reproducen un patrón conocido: la fragmentación. Precisamente por ello, la lección CECA adquiere relevancia: sin mecanismos ejecutivos comunes, la interoperabilidad queda a merced de interpretaciones nacionales divergentes.

Así, si tomamos como hilo conductor los esfuerzos globales y regionales contra el cambio climático observamos que estos sistemas (SPC) enfrentan un obstáculo paradójico: mientras la ciencia exige integración de datos para modelar fenómenos complejos —desde el deshielo ártico hasta las emisiones de metano agrícola—, los marcos legales y las estructuras de gobernanza promueven su fragmentación. Este problema, que combina limitaciones epistemológicas y fallos institucionales, se manifiesta en ejemplos concretos a escala global y europea, revelando una tensión irresuelta entre soberanía nacional, derechos de acceso a la información y cooperación internacional.

A nivel global, podemos establecer como ejemplo el Acuerdo de París (UNFCCC 2015) que estableció un marco de transparencia (Artículo 13) que obliga a los países a reportar inventarios de emisiones. Sin embargo, la ausencia de estándares legales vinculantes para armonizar metodologías ha derivado en inconsistencias críticas. En 2021, un análisis del *World Resources Institute* expuso que Brasil e Indonesia subestimaban sus emisiones por deforestación en un 20-30 por 100 al priorizar datos terrestres frente a satelitales, cuyo uso no está jurídicamente regulado en el marco de la ONU (Boehm *et al.* 2021). Esta divergencia, permitida por la flexibilidad legal del Acuerdo de París, genera un fenómeno de «doble contabilidad» que socava la confianza en los mecanismos globales de mitigación. Paralelamente, iniciativas como el *Global Ocean Observing System* (GOOS) chocan con restricciones legales: algunos países, amparados en la Convención de la ONU sobre el Derecho del Mar (UN 1982) limitan el acceso a datos oceanográficos recopilados en sus zonas económicas exclusivas, obstaculizando el monitoreo de fenómenos como la acidificación marina.

En la Unión Europea, el conflicto entre legislación y cooperación se agudiza. El Sistema de Comercio de Emisiones (ETS), pilar del Pacto Verde, depende de informes verificados por los Estados miembros. No obstante, en 2023, la Oficina Europea de Lucha contra el Fraude (OLAF) reveló que el 12

por 100 de las instalaciones industriales bajo el ETS incumplían los requisitos de reporte, con países como Polonia y Rumanía operando sistemas de validación incompatibles (OLAF 2023). Esta fragmentación, permitida por el Reglamento ETS (UE 2018/842) (European Commission 2018), que delega en los Estados la implementación técnica, contrasta con el rigor del Reglamento General de Protección de Datos (RGPD), donde la armonización es prioritaria. La paradoja es evidente: mientras el RGPD unifica la privacidad, normas climáticas como el ETS o el Reglamento de Gobernanza de Datos ((UE) 2022/868) carecen de mecanismos legales para imponer interoperabilidad, perpetuando silos.

Jurídicamente, esta fragmentación refleja un choque entre principios antagónicos. Por un lado, el derecho internacional ha iniciado una senda para reconocer los datos climáticos como *bien común global*. La Resolución 76/300 de la ONU (General Assembly UN 2022) reconoce el derecho a un medio ambiente limpio y saludable como derecho humano y aunque no menciona explícitamente los datos climáticos, establece un marco ético-jurídico para tratarlos como recurso esencial para garantizar dicho derecho, mientras que el derecho soberano de los Estados a controlar información territorial se encuentra plenamente consagrado en instrumentos como la Convención de Aarhus («BOE-A-2005-2528 Instrumento de Ratificación Del Convenio Sobre El Acceso a La Información, La Participación Del Público En La Toma de Decisiones y El Acceso a La Justicia En Materia de Medio Ambiente, Hecho En Aarhus (Dinamarca), El 25 de Junio de 1998». 2005)— priorizando la autonomía nacional, subrayando la tensión entre la necesidad de actuar de una forma coordinada y global, con el derecho de los estados.

Algunos ejemplos de la aproximación a los datos climáticos como bien común la podemos encontrar en:

a) Copernicus (UE): El programa de observación terrestre de la UE proporciona datos satelitales sobre cambio climático de forma gratuita y abierta. Su regulación ((UE) 2021/696) (Unión Europea 2021) establece que los datos deben ser «completos, abiertos y gratuitos» (art. 4), reconociendo su valor público.

b) Global Carbon Project: Esta red científica integra datos de emisiones de más de 100 países en un presupuesto global de carbono anual, tratando la información como bien común para la comunidad científica (GCP, n.d.).

c) IPCC: Los informes del Panel Intergubernamental sobre Cambio Climático se basan en datos compartidos por gobiernos bajo el principio de «revisión por pares abierta», aunque con limitaciones en acceso a datos brutos (IPPC 2024)

En este sentido, y por lo que respecta a la Unión Europea, el Reglamento de Gobernanza de Datos ((UE) 2022/868) intentó resolver esta tensión promoviendo espacios de datos sectoriales, pero su Artículo 11 los define como voluntarios, sin fuerza vinculante, tal y como ya hemos mencionado previamente. Dando como resultado la perpetuación de los silos y la fragmentación.

Esta disparidad, amplificada por el reciente Reglamento sobre IA (2024) — establece un modelo de gobernanza mixto, donde la supervisión de sistemas de alto riesgo implica tanto a instituciones europeas como a autoridades nacionales —, evidencia un fracaso en trasladar el modelo de la CECA al siglo XXI: la CECA creó una *Alta Autoridad* con poderes ejecutivos para gestionar el carbón y el acero como recursos compartidos, pero la UE carece de una entidad análoga para los datos.

El contraste con China es aleccionador. Su Ley de Seguridad de Datos (2021) define los datos como «activo nacional» sujeto a control estatal (art. 3), permitiendo proyectos como la Nueva Ruta de la Seda Digital, que integra datos de socios internacionales bajo estándares chinos (DigiChina, 2021). Este modelo, aunque autoritario, evita la fragmentación mediante una arquitectura legal centralizada, mientras la UE navega entre el ideal federal y la realidad intergubernamental.

Desde la filosofía de la ciencia, esta crisis podría ser descrita como un caso de *incomensurabilidad paradigmática* (Kuhn 1962): los datos se producen bajo marcos legales y epistemológicos tan dispares que su integración exige no solo cooperación técnica, sino un nuevo contrato social. Como advierte Floridi (2013), los datos son «recursos de agencia»: su gestión condiciona quién puede actuar frente a la crisis climática.

De esta forma podemos comprender porque el ejemplo del cambio climático resulta así altamente ilustrativo sobre los potenciales y limitaciones de los SCP, cuya relevancia jurídica radica en su capacidad para operar más allá de las fronteras nacionales, desafiando los marcos legales tradicionales basados en jurisdicciones territoriales. Estas infraestructuras no solo sustentan aplicaciones críticas, sino que también plantean interrogantes sobre soberanía, seguridad y equidad en el acceso a los datos.

2.2. Requisitos Operativos de los SCP – Del *soft* and *hard law*

La operatividad de los SCP depende de tres pilares interconectados: interoperabilidad técnica, legal y geopolítica. Así, en primer lugar, la interoperabilidad técnica exige protocolos comunes (*soft law*), como el cifrado TLS 1.3 o el formato semántico JSON-LD, para garantizar compatibilidad entre sistemas. Sin embargo, y a modo de ejemplo, divergencias como el uso de los estándares SM (Shang Mi) 2/3¹⁰ en China limitan la integración global.

Desde una perspectiva técnica, los algoritmos SM2 y SM3 no cumplen los requisitos del Reglamento eIDAS 910/2015 (European Commission 2014), cuyo Anexo II exige el uso de estándares reconocidos como ECC (ETSI EN

¹⁰ Los algoritmos SM2 y SM3 forman parte del estándar criptográfico nacional chino conocido como *Shang Mi* (SM), desarrollado por la Oficina de Normas de China. SM2 es un algoritmo de cifrado basado en curvas elípticas, mientras que SM3 es una función hash.

319 142-1) para firmas electrónicas, ni con la Directiva NIS (2016/1148) (European Commission 2016), que en su Artículo 14 demanda criptografía certificada por esquemas reconocidos (ej: *ETSI, Common Criteria*). Además, el Reglamento de Ciberseguridad (Reglamento 2019/881) (European Commission 2019) establece en su Artículo 54 que solo se admiten algoritmos evaluados bajo marcos europeos, excluyendo implícitamente los SM2/SM3 en sectores regulados, por carecer de auditorías independientes y transparencia en su diseño. A ello se suma el RGPD (Artículo 32), que exige medidas técnicas «adecuadas» para proteger datos personales sobre lo que el EDPB (*European Data Protection Board*) considera que el uso de criptografía no certificada en la UE (como SM2/SM3) podría incumplir este artículo, especialmente en transferencias a terceros países (Opinión 05/2021) (EDPB 2021), agravando riesgos ya identificados en sentencias como *Schrems II* (C-311/18) (CURIA 2020).

En segundo lugar, la interoperabilidad legal, choca tal y como ya hemos adelantado con regulaciones contradictorias (Catanzariti 2024). A modo de ilustración, mientras el Reglamento General de Protección de Datos (GDPR) de la UE restringe transferencias internacionales bajo el principio de «nivel adecuado de protección» (art. 45), la Ley de Seguridad de Datos de China (2021) obliga a almacenar datos «críticos» en servidores locales (art. 21), subordinando la privacidad a intereses estatales. Este conflicto se ejemplifica además con otras jurisdicciones. A modo de ejemplo podemos citar *Schrems II* (2020), donde el Tribunal de Justicia de la UE invalidó el acuerdo *Privacy Shield* con EE.UU. por riesgos de vigilancia masiva, afectando a miles de empresas que dependían de flujos transatlánticos (CURIA 2020).

Finalmente, la interoperabilidad geopolítica, es una conclusión lógica de las dos anteriores y, implica acuerdos internacionales que faciliten flujos de datos. La UE por ejemplo ha promovido cláusulas de protección en tratados como el *EU-Japan Economic Partnership* («EU-Japan Economic Partnership Agreement» 2019), mientras China expande su influencia mediante la Nueva Ruta de la Seda Digital, instalando centros de datos en 17 países africanos bajo estándares como el GB/T 35273 (PRC 2020), que permite acceso estatal sin consentimiento tal y como abordaremos más adelante. Esta competencia por estándares globales refleja una «guerra silenciosa»: en foros como la ISO/IEC, donde China impulsa normas técnicas compatibles con su marco legal, mientras la UE defiende principios basados en la Carta de Derechos de la UE.

Un ejemplo de las dinámicas de interoperabilidad geopolítica sería el conocido como efecto Bruselas. Fenómeno mediante el cual la Unión Europea, aprovechando el tamaño y la influencia de su mercado único, ha sido capaz de establecer regulaciones y estándares que, debido a la necesidad de las empresas globales de acceder al mercado europeo, son adoptados a nivel mundial. Este efecto ha permitido a la UE ejercer una influencia regulatoria desproporcionada en áreas como la protección de datos, la seguridad de los productos y las normas ambientales, efectivamente «exportando» sus regulaciones más allá de sus fronteras y moldeando las prácticas empresariales y los estándares tecnológicos a escala global. Una influencia que empieza a

ser contestada desde otros espacios del globo, fundamentalmente China, que solo en el espacio de la IA se encuentra trabajando en 50 nuevos estándares con un horizonte puesto en 2026 (Jiang, 2024).

Así mismo, resulta interesante observar como en el ámbito específico de la regulación de la Inteligencia Artificial, podríamos estar presenciando lo que algunos expertos denominan un «efecto Bruselas inverso». A diferencia de lo ocurrido con el Reglamento General de Protección de Datos (RGPD), el Reglamento de IA de la UE no parece estar generando el mismo nivel de adopción global. Mientras que varios países están estudiando el enfoque basado en riesgos de la UE, muchos optan por no seguir directamente su modelo regulatorio. Esta divergencia se debe a varios factores: la naturaleza específica de la tecnología de IA, que difiere de la regulación de datos más generalista; las raíces de la ley en principios de responsabilidad de productos de la UE, que no son fácilmente transferibles a otros sistemas legales; y la importancia estratégica y económica de la IA, que lleva a los países a adaptar sus regulaciones a sus propias condiciones de mercado y objetivos de innovación.

Ejemplos de esta tendencia incluyen el enfoque «pro-innovación» del Reino Unido (UKGOV 2022), la promesa de Argentina de una regulación menos restrictiva con potenciales impactos sobre las libertades y derechos ciudadanos (Gonzalez 2024), y los sandbox regulatorios favorables a la innovación en Emiratos Árabes Unidos (UAE 2024) y Singapur (Singapore 2024). Este panorama sugiere que, en lugar de una convergencia global hacia el modelo de la UE, podríamos ver una mayor fragmentación en la regulación de la IA a nivel mundial.

En este contexto de divergencia regulatoria, es importante considerar también los enfoques de otros actores clave en el desarrollo de la IA. En Estados Unidos, el proyecto de ley SB-1047¹¹ de California podría generar un «efecto California» en la regulación de la IA (California 2024). Sin embargo, su alcance se limita principalmente a exigir que las empresas de Silicon Valley implementen salvaguardas en sus servicios de modelos de fundación, lo que podría aumentar los costos de las API y afectar la cadena de suministro de IA, pero no necesariamente provocar una alineación global en las prácticas de seguridad de IA.

Por otro lado, China está impulsando una estandarización integral de todos los niveles del sistema tecnológico de IA, tanto a nivel doméstico como global, a través de su Iniciativa Global de Gobernanza de IA (Cong and Ye-ping 2023). Dado el papel crucial de China en el comercio mundial, este en-

¹¹ El proyecto de ley SB-1047, titulado *Safe and Secure Innovation for Frontier Artificial Intelligence Models Act*, fue presentado en California en 2024 con el objetivo de establecer requisitos de seguridad para los modelos de inteligencia artificial de frontera. La propuesta busca que las empresas desarrolladoras implementen salvaguardas técnicas en sus sistemas —como pruebas de alineación, monitoreo de capacidades emergentes y mecanismos de apagado— especialmente en modelos fundacionales de gran escala.

foque podría tener éxito en la estandarización de especificaciones y prácticas de IA, aunque probablemente se limite a las cadenas de suministro centradas en China, como las asociadas al programa de la «Nueva Ruta de la Seda» (China.org.cn 2024). Este «efecto Pekín» ilustra cómo las potencias tecnológicas están desarrollando enfoques distintivos para la regulación de la IA, contribuyendo así a un panorama regulatorio global cada vez más diverso y complejo.

Teóricamente, este escenario se explica mediante dos enfoques:

1) «El código es ley» (Lessig): La premisa de Lawrence Lessig adquiere relevancia crítica al analizar estándares técnicos que operan como marcos normativos implícitos. Al margen de lo anteriormente mencionado, y a modo de ejemplo, en la Unión Europea, el protocolo TLS 1.3 (Transport Layer Security), adoptado formalmente bajo el Reglamento eIDAS (Comisión Europea 2024) (art. 3(27)) como estándar para comunicaciones seguras, ejemplifica esta dinámica. Ya que la mayoría de páginas web europeas emplean TLS 1.3, se produce una exclusión *de facto* a entidades que utilicen cifrados no certificados (ej: RSA-1024). Un caso interesante es el del *Health Data Hub* francés, obligado en 2021 a migrar sus servidores de AWS a OVHcloud tras identificarse que las claves TLS 1.3 se gestionaban en EE.UU., violando el art. 48 del GDPR sobre transferencias internacionales (Dillet 2020). En paralelo, China ha institucionalizado el estándar SM4 mediante su Ley de Criptografía Comercial (2019) (Huaxia 2019), exigiendo su uso en sectores estratégicos como finanzas y energía. Empresas como *Alipay* deben cifrar transacciones con SM4, incompatible con el AES-256 europeo. Esto genera barreras de interoperabilidad, así como costos adicionales para empresas extranjeras evidenciando cómo la arquitectura técnica delimita fronteras digitales excluyentes.

2) Autopoiesis jurídica (Luhmann): La teoría de Niklas Luhmann sobre sistemas autopoieticos —entidades que se autorreproducen y priorizan coherencia interna— se materializa en la sentencia *Schrems II* (CURIA 2020). Al invalidar el acuerdo *Privacy Shield* UE-EE.UU., el Tribunal de Justicia de la UE priorizó la lógica interna del GDPR (arts. 44-46). Este hermetismo se replica en China bajo su Ley de Seguridad de Datos (2021), que obliga a empresas como *Tesla* a almacenar datos localmente, incluso si contradice estándares globales como ISO/IEC 27001. Ambos sistemas —UE y China— operan como circuitos cerrados, donde la autorreferencialidad legal prevalece sobre la interoperabilidad técnica.

Así, el sueño de la configuración de sistemas computacionales planetarios se encuentra hoy más lejos debido a la fragmentación y creación sistemática de silos a través de la configuración de ordenamientos jurídicos y sistemas de estándares auto referenciados que desembocan en una bifurcación del ciberespacio, que se traduce entre otras manifestaciones, en una guerra silenciosa por los estándares internacionales.

2.3. La guerra silenciosa por los estándares

En este escenario, los estándares tecnológicos internacionales se erigen como los nuevos tratados que delimitan las fronteras invisibles del ciberespacio y moldean las realidades cotidianas. De esta forma, es imprescindible comprender que la importancia de los estándares tecnológicos trasciende el ámbito puramente técnico, convirtiéndose en el nuevo terreno donde se libran las batallas por la hegemonía global (LAZARD 2023; Aschenbrenner 2024). Es decir, lejos de ser meras especificaciones técnicas, representarían la cristalización de visiones contrapuestas sobre el futuro de la humanidad y su relación con la tecnología. En un mundo cada vez más interconectado, pero paradójicamente fragmentado, estos estándares determinan no solo la interoperabilidad de los sistemas, sino también los flujos de información, el alcance de la privacidad, y la distribución del poder económico y político.

Esta creciente importancia de los estándares tecnológicos como campo de batalla por la supremacía global, ha conllevado un creciente interés entorno a las dinámicas de la UIT (Unión Internacional de Telecomunicaciones, UN). Así el artículo «*Who drives the international standardization of telecommunication and digitalisation?*», publicado en la revista *Global Policy* (2023), explora el creciente papel de China y Rusia en el proceso de estandarización de las telecomunicaciones. El estudio argumenta que la UIT, históricamente un actor central en la configuración de normas que rigen las telecomunicaciones a nivel mundial se ha vuelto más politizada en los últimos años debido a la bifurcación tecnológica entre Estados Unidos y China.

El artículo utiliza un conjunto de datos que analiza las contribuciones de más de 800 actores, tanto gubernamentales como privados, a la UIT entre 2000 y 2022. Estos datos revelan un cambio significativo en el panorama de las contribuciones a la UIT, donde los actores chinos se han convertido en los más activos, superando a Estados Unidos y la Unión Europea. El estudio se basa en un conjunto de datos que incluye 49.076 contribuciones de 1.686 actores, de las cuales 807 son únicos tras corregir distintas ortografías. Este conteo incluye 153 gobiernos nacionales y 654 actores privados. (Klotz 2023)

El análisis revela que China se ha convertido en líder en contribuciones, aportando un total de 16.952 (35 por 100) de las presentaciones, realizadas por 78 actores chinos. Le sigue Corea del Sur, con 5.963 contribuciones (12 por 100) de 15 actores, y Estados Unidos, que cuenta con 132 actores contribuyentes que hicieron 4.479 presentaciones, lo que representa cerca del 9 por 100 del total de contribuciones a la UIT entre 2000 y 2022.

La Figura 1 ilustra la primera conclusión del conjunto de datos. Con diferencia, China es el país del que proviene la mayoría de las Contribuciones, con un total de 16.952 (35 por 100) recibidas de 78 actores chinos. El segundo mayor número de Contribuciones (5.963; 12 por 100) fue recibido de 15 actores coreanos. Estados Unidos tiene el mayor número de actores contribu-

yentes (132), y su número de Contribuciones presentadas (4.479) representa alrededor del 9 por 100 del total de Contribuciones que la UIT recibió entre 2000 y 2022.

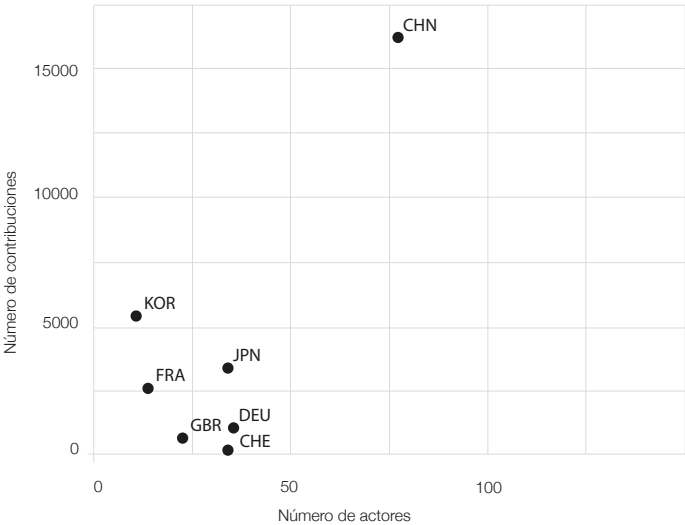


Ilustración 1: Número de actores y el total de Contribuciones presentadas por país, 2000–2022. Fuente: Klotz, 2023.

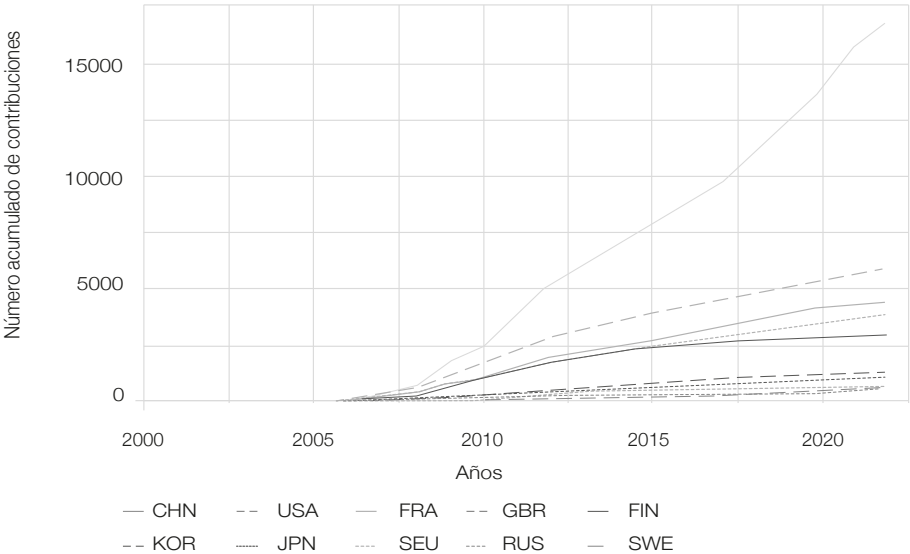


Ilustración 2: Número acumulado de Contribuciones presentadas por los 10 principales países, 2002-2022 Fuente: Klotz, 2023.

Tal y como se puede observar en la Ilustración 2 el número de Contribuciones recibidas de los 10 países más activos. Destaca el aumento de las Contribuciones por parte de actores chinos. En 2002, esas Contribuciones representaban alrededor del 4 por 100 del total de Contribuciones anuales. Para 2004, representaban el 8 por 100; en 2010, el 31 por 100; en 2015, el 33 por 100; y en 2021, el 55 por 100 del total de Contribuciones anuales.

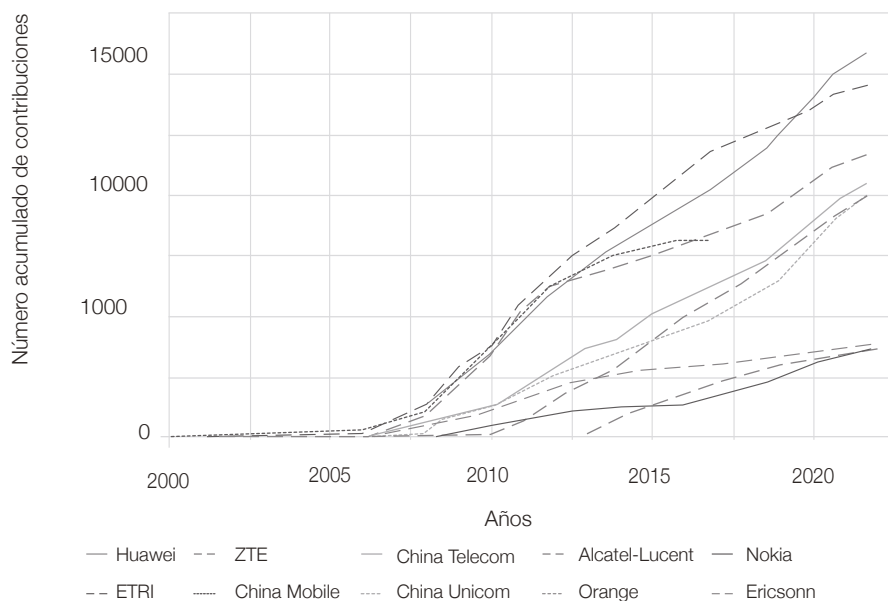


Ilustración 3: Número acumulado de Contribuciones presentadas por las 10 principales empresas, 2000–2022. Fuente: Klotz, 2023.

Así mismo, la Ilustración 3 presenta el número de Contribuciones recibidas de las 10 empresas más activas, de las cuales cinco son chinas. En conjunto, Huawei, ZTE, China Mobile, China Unicom y China Telecom representan casi una cuarta parte del total de Contribuciones recibidas entre 2000 y 2022. Los otros 5 principales contribuyentes incluyen ETRI (Instituto de Investigación en Electrónica y Telecomunicaciones, Corea), Alcatel-Lucent (Francia), Ericsson (Suecia), Orange (Francia) y Nokia (Finlandia).

De esta forma, el estudio revela que las contribuciones de actores chinos han aumentado significativamente en la UIT, pasando del 4 por 100 de las contribuciones totales en 2002 al 55 por 100 en 2021. Este crecimiento se observa especialmente en áreas como el transporte, y las tecnologías *cloud*. China Telecom, China Mobile, China Unicom y Huawei, junto con ZTE, representan casi un cuarto de las contribuciones totales en la UIT entre 2000 y 2022.

Además, y aunque no tan marcado como el de China, el estudio también observa un aumento de las contribuciones de actores rusos en la UIT, lo que

sugiere un esfuerzo concertado por parte de Moscú para influir en la configuración de las normas. El dataset utilizado permite observar, de esta forma, que desplazamiento del poder en la UIT tiene implicaciones potenciales significativas para el futuro de las telecomunicaciones y la gobernanza digital a nivel mundial.

2.4. Fragmentación en la Unión Europea: Manifestaciones

En lo que se refiere a la fragmentación de datos en la Unión Europea, es necesario en primer lugar tener en cuenta que se trata de un fenómeno multifacético, arraigado en tensiones históricas entre la integración supranacional y la soberanía nacional. A diferencia de los sistemas computacionales planetarios —analizados previamente en su dimensión global—, esta sección se centra en las dinámicas internas de la UE y su contraste con el modelo centralizado de China, donde la fragmentación es mínima pero estratégicamente dirigida.

La divergencia en la aplicación del Reglamento General de Protección de Datos (GDPR), anteriormente mencionada, constituye un fenómeno documentado que fractura la armonización normativa, pese a su carácter directamente aplicable bajo el art. 288 del Tratado de Funcionamiento de la UE (TFUE). Así, aunque el GDPR establece principios uniformes, su interpretación y ejecución (dotación presupuestaria y de recursos humanos a los garantes nacionales) varían significativamente entre Estados miembros, generando inseguridad jurídica y asimetrías competitivas.

Esta fragmentación se ve exacerbada por una doble disparidad estructural: por un lado, los sistemas tecnológicos (ej. inteligencia artificial, reconocimiento facial) evolucionan en ciclos iterativos de meses, mientras los mecanismos legales de la UE operan en escalas temporales plurianuales — como la evaluación del GDPR iniciada en 2021, que derivó en debates sobre reformas limitadas que continuaban en curso en 2024—; por otro, los tiempos de resolución de recursos judiciales dilatan aún más la coherencia normativa. Un recurso interpuesto ante un tribunal nacional puede tardar 2-3 años en escalar al Tribunal de Justicia de la UE (TJUE) mediante cuestión prejudicial, según datos del Informe de la Eurocámara sobre eficiencia judicial (CEPEJ 2024). Por ejemplo, el caso *C-311/18 (Schrems II)*, que invalidó el Privacy Shield, tardó 22 meses en resolverse, período en el que empresas y Estados operaron bajo criterios divergentes. Esta lentitud, sumada a la velocidad exponencial de innovaciones como el *blockchain* o el metaverso, obliga a los Estados a aplicar criterios propios ante vacíos regulatorios, profundizando la descoordinación. Así, mientras Alemania implementó en 2023 guías vinculantes para la estandarización de algoritmos (Fernández Hernández 2023; European Commission 2024), países como Italia se mostraban más dependientes de resoluciones judiciales *ad hoc*, según el Informe de la Comisión Europea sobre GDPR (European Commission 2024). Pudiendo destacar diversos ejemplos de cómo esta fragmentación se materializa en nuestra realidad.

Así, se observa por ejemplo una gran disparidad en la imposición de multas y criterios de proporcionalidad. El caso Google LLC v. CNIL (Colchen 2022) ejemplifica una interpretación estricta del art. 20 GDPR, resultando en una multa de 60 millones de euros (CNIL 2021). En contraste, Rumanía ha impuesto solo 0,7 millones de euros en multas acumuladas desde 2018, priorizando advertencias sobre sanciones. Cuantitativamente, España aplicó el 11 por 100 del total de multas GDPR en la UE (más de 900 sanciones), mientras Rumanía solo el 1 por 100 (apenas 200 sanciones) (European Commission 2024). Una tendencia que se encuentra ligada a los recursos, tanto económicos como humanos que cada estado miembro dedica a su agencia de protección de datos. Produciendo disparidades más que significativas (EDPB 2023; «GDPR Enforcement Tracker - List of GDPR Fines», n.d.; Alexiadis *et al.* 2023).

Además también podemos citar interpretaciones divergentes del «interés legítimo» (art. 6.1(f) GDPR), la cual se evidencia en casos como el de *Deutsche Wohnen*, donde el Tribunal Federal alemán confirmó una multa de 14,5 millones de euros por almacenar datos de inquilinos sin base legal, cuestión que escalaría finalmente hasta el TJUE por cuestiones más de tipo procedimental (CURIA 2023). En contraste, el Garante italiano permitió a empresas de telecomunicaciones procesar datos de ubicación bajo el mismo artículo para «mejorar servicios», aplicando un criterio más flexible (GPDP - 10040382 n.d.) A lo que se podrían sumar otras ineficiencias como pueden ser las inconsistencias en plazos y procedimientos administrativos. Divergencias todas ellas, que acaban generando un mosaico con importantes consecuencias jurídicas y económicas significativas.

Finalmente, la tensión entre privacidad e innovación no hace más que agravar el problema. Mientras el RGPD prioriza la protección de datos (art. 5), el El Reglamento de Gobernanza de Datos (Reglamento (UE) 2022/868) promueve la reutilización de datos públicos para impulsar la inteligencia artificial (IA). Esta dualidad crea incertidumbre mientras que, en China, no existe tal dilema. La Ley de Seguridad de Datos (2021) subordina la privacidad al interés estatal, a lo que habría que sumar la Ley de Ciberseguridad (DigiChina 2017): el artículo 28 obliga a las empresas a cooperar con autoridades en investigaciones de seguridad nacional, sin necesidad de orden judicial. Y la ley de Inteligencia Nacional (PRC 2017) que permite a las agencias de seguridad acceder a datos personales y corporativos sin notificación. Permitiendo al gobierno acceder a datos sin consentimiento y eliminando barreras para proyectos estratégicos como el Sistema de Crédito Social. Así, y mientras la UE todavía debate la mejor manera de manejar los historiales médicos transfronterizos, China ya ha centralizado datos de más de mil millones de ciudadanos, usando esta información para entrenar algoritmos de inteligencia artificial.

De esta forma, las asimetrías en la aplicación del Reglamento General de Protección de Datos y la coexistencia de regímenes sectoriales dispares evidencian que la coordinación actual es insuficiente. Una instancia ejecutiva europea específica para datos e IA permitiría resolver contradicciones, agilizar la interoperabilidad y homogeneizar criterios de supervisión.

Esta situación refleja un dilema teórico que Elinor Ostrom abordó sobre la gestión de recursos comunes: la necesidad de equilibrar normas colectivas con la autonomía local. La UE enfrenta dificultades derivadas de su diversidad intrínseca, mientras que China opta por la centralización, a menudo a expensas de los derechos individuales. Finalmente, es necesario añadir, que la problemática relativa a la configuración y explotación de SPC, no se restringe únicamente al tráfico de datos, sino que también se ve profundamente afectada por la propia configuración de los sistemas de Inteligencia Artificial, y su comprensión desde el derecho.

3. FRONTERAS DIGITALES EN LA REGULACIÓN DE LA IA

3.1. El Enfoque de la UE: Regulación de la IA como Producto

En el contexto actual de crisis, el desarrollo de la Inteligencia Artificial, y más especialmente la carrera por la Inteligencia Artificial General, se ha convertido en el caballo de batalla entre superpotencias, al entender estas que estamos ante un juego de suma cero en el que el ganador se lo lleva todo (*winner takes it all*). Sea esto cierto o no, la realidad es que existe una carrera acelerada por hacerse con una superioridad en el ámbito, lo que ha llevado a acelerar procesos tanto de regulación (Caso Europeo y Chino) como de desregularización (caso americano bajo la actual administración Trump).

En este sentido, la Unión Europea ha consolidado un modelo regulatorio que asimila la inteligencia artificial (IA) a un producto comercial, tal y como hemos mencionado anteriormente, sujeto a estándares de seguridad y responsabilidad análogos a los aplicables a bienes físicos. Así, la nueva Directiva de Responsabilidad por Productos Defectuosos («Directiva - 2024/2853» 2024) marca un hito al incluir de manera explícita al «software» y los «sistemas de IA» dentro de la definición jurídica de «producto». Este enfoque busca cerrar vacíos legales históricos, de la Directiva 85/374/CEE (EU 1985), asegurando que los desarrolladores asuman responsabilidad incluso si los defectos emergen tras actualizaciones postcomercialización. Es decir, podemos considerar que la transformación digital ha reconfigurado la naturaleza de los bienes y servicios, desafiando los marcos legales diseñados para productos físicos.

De esta forma, el núcleo de la reforma radica en que expande la definición de «producto» para incluir: Software integrado (ej.: sistemas de control de vehículos autónomos), Software independiente (ej.: aplicaciones médicas), y Sistemas de IA (desde algoritmos predictivos hasta herramientas de generación de contenido). Esta equiparación jurídica entre bienes físicos y digitales respondería tanto a críticas doctrinales como a fallos judiciales como el Caso UsedSoft (CJUE, C-128/11) (Curia 2012) donde ya se reconoció el software como «bien» transable, sentando bases para su regulación como producto.

Uno de los cambios más significativos se encuentran en que la nueva directiva («Directiva - 2024/2853» 2024), impone responsabilidad a los fabricantes por defectos surgidos tras actualizaciones de software o IA, siempre que estas sean controladas por el propio desarrollador. Este enfoque aborda casos como el escándalo de las actualizaciones de autonomía en vehículos Tesla (ME 2024), donde actualizaciones remotas redujeron la capacidad de baterías sin consentimiento explícito. Así la nueva Directiva establece que: Los fabricantes deben garantizar la seguridad no solo en el lanzamiento inicial, sino en todo el ciclo de vida del producto. Y que la responsabilidad persiste incluso si el defecto se manifiesta años después, siempre que derive del diseño original o de una actualización gestionada por el fabricante.

Si bien y pese a su ambición, la revisión enfrenta críticas doctrinales. En primer lugar, la ambigüedad en el «control» de actualizaciones genera incertidumbre: ¿se incluyen parches desarrollados por subcontratistas o comunidades de código abierto? Segundo, la IA autónoma plantea un dilema no resuelto: si un sistema de aprendizaje automático genera defectos imprevisibles (ej.: *sesgos emergentes en algoritmos de reclutamiento*), la atribución de responsabilidad podría diluirse. El Considerando 23 reconoce este problema, pero delega su solución a futuras interpretaciones jurisprudenciales.

Además, la exención por cumplimiento normativo crea una tensión con otros reglamentos. Por ejemplo, un sistema de IA certificado bajo el Reglamento de IA podría presumirse «no defectuoso», aun cuando cause daños por falta de transparencia explicable. Esto subraya la necesidad de coordinación inter-regulatoria.

De esta forma, la nueva directiva marca un contraste nítido con la Directiva de 1985: En primer lugar y en lo referente al Ámbito subjetivo: Mientras el régimen anterior limitaba la responsabilidad a fabricantes de bienes físicos, la revisión engloba a desarrolladores de software y proveedores de IA. En segundo lugar y en lo que se refiere a la Temporalidad: La responsabilidad ya no se extingue en el momento de la comercialización, sino que se extiende a actualizaciones sucesivas. Y finalmente en tercer lugar, la Carga de la prueba se invierte en casos donde el producto incumple estándares de seguridad técnicos (ej.: normas ISO/IEC 25010 para software), facilitando a las víctimas acceder a indemnizaciones.

Así para las empresas, la revisión implica mayores costos de cumplimiento, incluyendo: Auditorías continuas de software y IA, mecanismos de trazabilidad para actualizaciones, así como seguros de responsabilidad civil adaptados a riesgos digitales. Mientras que, para los consumidores, supone una protección reforzada. Casos como el fallo en el sistema de diagnóstico médico IBM Watson Health (*Bernal 2018*), donde errores algorítmicos causaron tratamientos incorrectos, podrían derivar en indemnizaciones automáticas sin necesidad de demostrar negligencia.

Así y aunque el Reglamento de IA no define textualmente la IA como producto, varios artículos reflejan una lógica regulatoria análoga a la de bienes

físicos. El art. 6, por ejemplo, clasifica sistemas de IA de alto riesgo en función de su integración en sectores ya regulados (salud, transporte), replicando el enfoque aplicado a productos médicos o maquinaria industrial. El art. 61, por su parte, exige a los proveedores monitorear sistemas de alto riesgo tras su comercialización, imitando los mecanismos de vigilancia de mercado para productos tradicionales. Finalmente, el art. 2(3) remite expresamente a normas de la UE aplicables a productos físicos, reforzando la asimilación funcional entre ambos ámbitos.

De esta forma, podemos afirmar que el entramado jurídico —entre legislación emergente, precedentes y diseño regulatorio— consolida la IA como un «*producto*» en términos prácticos, aunque persistan debates sobre su encaje formal en categorías legales concebidas originariamente para realidades tecnológicas estáticas, suscitando debates, derivados de la propia naturaleza dinámica de sistemas como ChatGPT, cuyos algoritmos se actualizan continuamente con nuevos datos. Michael Veale, experto en derecho digital, advierte que la trazabilidad de responsabilidades se complica cuando un sistema evoluciona *postcomercialización*: «¿Quién responde si un modelo de IA desarrolla sesgos meses después de su lanzamiento, mediante aprendizaje autónomo?». El AI Act no aborda explícitamente este vacío, dejando a los Estados miembros la tarea de definir protocolos de actualización y supervisión continua (art. 59) (Veale and Borgesius 2021; Edwards and Veale 2017).

A esto se suma el solapamiento normativo. Mientras el art. 10 del AI Act exige transparencia en los datos de entrenamiento —incluyendo fuentes y posibles sesgos—, el art. 20 del Data Act restringe el acceso a información comercial confidencial, generando tensiones entre transparencia y protección de secretos empresariales. Estas divergencias reflejan la tensión entre armonización supranacional y soberanía nacional, un legado del principio de atribución de competencias (art. 5 TUE). Mientras la UE regula la IA como producto, China la trata como infraestructura crítica, supervisada centralmente por el Estado. Este enfoque, aunque eficiente en coordinación, elimina salvaguardas fundamentales: La mayoría de empresas chinas de IA admiten compartir datos con el gobierno sin consentimiento («World Report 2025: China» 2025), si bien, algunos de sus principios articuladores merecen ser tenidos en cuenta.

Tratar la inteligencia artificial con lógicas de «producto» aporta certezas, pero corre el riesgo de reforzar la fragmentación si no se acompaña de una autoridad europea que garantice actualizaciones normativas ágiles y criterios uniformes de evaluación y vigilancia.

3.2. China: La IA como Infraestructura de Estado y Control Centralizado

En contraste con el enfoque europeo, China ha construido un paradigma regulatorio donde la inteligencia artificial (IA) opera como infraestructura crítica, subordinada a objetivos de seguridad nacional y planificación estatal. La Ley de Seguridad de Datos (2021) (DigiChina 2021) consagra los datos como «activo nacional» tal y como ya habíamos mencionado previamente, sujetos a supervisión exclusiva de la *Cyberspace Administration of China* (CAC) (CA 2025), organismo que responde directamente al Partido Comunista. Este marco legal no solo prioriza el control estatal sobre la privacidad individual, sino que sirve como herramienta para proyectos geoestratégicos como el Sistema de Crédito Social (Hou and Fu 2024) y la Nueva Ruta de la Seda Digital.

El Sistema de Crédito Social, implementado desde 2014, integra datos judiciales, financieros y sociales de 1.400 millones de ciudadanos para asignar puntuaciones que determinan acceso a servicios públicos, empleo o viajes (Hou and Fu 2024). En 2022, 23 millones de personas fueron bloqueadas en transporte aéreo por «baja puntuación» (Zhao and Liu 2025). Paralelamente, la Nueva Ruta de la Seda Digital exporta infraestructuras tecnológicas chinas —como centros de datos de Huawei en África— bajo estándares como el GB/T 35273, que permite al gobierno acceder a datos sin consentimiento. En 2023, 17 países africanos, incluyendo Etiopía y Kenia, adoptaron estos sistemas, consolidando la influencia tecnológica china en el continente (Nadia 2024; Winter 2020; Zhang, Tsang, and Fuschi 2020).

Así, en el modelo chino, el marco legal prioriza la responsabilidad estatal en infraestructuras críticas. Si bien la Ley de Ciberseguridad (2017) (DigiChina 2017), en su capítulo IV, desarrolla las responsabilidades individuales, por negligencia, en casos que comprometan datos o sistemas críticos, sin requerir intención maliciosa. En materia diplomática, China ha firmado acuerdos bilaterales para promover sus estándares tecnológicos, como el memorándum con Arabia Saudita en 2022 sobre cooperación en 5G e IA. Académicos como Rogier Creemers (Universidad de Leiden) destacan que este modelo equilibra control estatal y disciplina individual, pero limita mecanismos independientes de rendición de cuentas, centralizando la supervisión en entidades como la Comisión Nacional de Supervisión.

Además, debemos tener en cuenta que la centralización estatal facilita la interoperabilidad técnica: el 90 por 100 de las empresas chinas utilizan proveedores de nube locales como Alibaba Cloud o Tencent Cloud, frente al 30 por 100 en la UE (Eurostat, 2023). Esta uniformidad se logra mediante subsidios estatales a empresas que adopten estándares nacionales, como el GB/T 35273 para datos personales. No obstante, el modelo sacrifica flexibilidad: mientras la UE fomenta ecosistemas descentralizados de startups, China dirige sus recursos a través de planes quinquenales, priorizando megaproyectos alineados con la estrategia del Partido Comunista.

Ejemplo de ello son las Smart Cities de Shenzhen y Hangzhou, donde sensores IoT y cámaras de vigilancia con IA monitorean en tiempo real a 25 millones de habitantes. Estos proyectos, financiados con €24.000 millones del presupuesto estatal (2021-2025), han reducido la criminalidad en un 40 por 100, pero también normalizado la vigilancia masiva.

De esta forma, podemos afirmar que el modelo chino ofrece eficiencia operativa y coordinación, pero lo hace a costa de garantías esenciales: la ausencia de contrapesos institucionales, la subordinación de la privacidad al interés estatal y la normalización de la vigilancia masiva. Este marco no solo concentra poder en la *Cyberspace Administration of China*, sino que exporta su arquitectura regulatoria mediante la Nueva Ruta de la Seda Digital, condicionando infraestructuras críticas en terceros países a estándares que priorizan el control estatal sobre la protección de derechos.

Para la Unión Europea, el desafío no consiste en replicar este centralismo, sino en demostrar que la cohesión puede lograrse sin sacrificar el Estado de Derecho. Ello exige instituciones supranacionales con competencias ejecutivas, inspiradas en la lógica de la CECA, que permitan armonizar normas y garantizar interoperabilidad bajo principios democráticos y control jurisdiccional.

4. HACIA UN ESPACIO DIGITAL EUROPEO: PROPUESTAS DESDE EL LEGADO DE LA CECA

4.1. Lecciones Históricas: La CECA como Modelo de Soberanía Compartida

El Tratado de la Comunidad Europea del Carbón y del Acero (CECA) no solo gestionó recursos estratégicos, sino que estableció un modelo de gobernanza supranacional mediante instituciones con poderes ejecutivos. Su «Alta Autoridad» —predecesora de la Comisión Europea— podía imponer multas a Estados incumplidores, armonizar estándares de producción y redistribuir excedentes entre países (art. 8 CECA). Este modelo, basado en la cesión parcial de soberanía, ofrece un marco inspirador para la gobernanza de datos.

Tres lecciones operativas de la CECA para el ámbito digital:

1. Soberanía compartida efectiva, con competencias ejecutivas para armonizar e imponer decisiones;
2. Mandato funcional claro sobre recursos estratégicos transversales (hoy: datos e infraestructuras digitales);
3. Mecanismos financieros condicionados a estándares comunes, para alinear incentivos y acelerar la convergencia técnica.

La analogía es clara: así como el carbón y el acero fueron pilares de la industria posbélica, los datos y la Inteligencia Artificial son el motor de la economía digital. La UE podría replicar el modelo de la CECA mediante:

1. Una Agencia Digital Europea con competencias para armonizar estándares técnicos y resolver disputas transfronterizas.

2. Protocolos vinculantes de intercambio de datos estratégicos, similares a la «poolización» de recursos en la CECA, aplicables a sectores como la salud o la energía.

Sin embargo, iniciativas actuales como el *Data Governance Act* (DGA) carecen de este alcance. Su art. 11 permite a los Estados miembros añadir requisitos adicionales, perpetuando la fragmentación.

La Comunidad Europea del Carbón y del Acero (CECA) demostró que la cesión estratégica de soberanía en áreas críticas no diluye la autonomía nacional, sino que construye interdependencias positivas. En la era digital, este principio exige trascender la regulación fragmentaria de la inteligencia artificial (IA) como mero «producto» —lógica del AI Act— para adoptar un enfoque sistémico que comprenda la IA como *infraestructura de gobernanza*. Así como la CECA gestionó el carbón y el acero como recursos transversales, la UE necesita una Alta Autoridad Digital con competencias ejecutivas para armonizar estándares técnicos, gestionar datos estratégicos y supervisar ecosistemas de IA bajo un paradigma de soberanía compartida.

El modelo actual, basado en agencias descentralizadas (ej.: ENISA para ciberseguridad) y comités de ética no vinculantes, reproduce la debilidad del Tratado CECA revisado en 1967, que diluyó la Alta Autoridad en estructuras intergubernamentales (Dinan, 2004). Una Agencia Europea de Datos e IA (AEDIA), inspirada en el art. 8 del Tratado CECA, podría:

1. Unificar estándares de interoperabilidad para sistemas de IA, exigiendo certificaciones dinámicas que evolucionen con los algoritmos (ej.: auditorías continuas de modelos generativos como GPT-5).

2. Gestionar «pools» paneuropeos de datos estratégicos (sanitarios, climáticos, logísticos) mediante tecnologías federativas (blockchain soberana, cifrado homomórfico), evitando silos nacionales.

3. Ejercer supervisión directa sobre Big Tech, aplicando sanciones proporcionales a su impacto sistémico (ej.: cuotas obligatorias de datos abiertos para acceder al mercado único).

La AEDIA operaría bajo un Consejo Científico-Jurídico, integrando expertos en ética computacional y derecho digital, con mandato para actualizar marcos normativos cada 18 meses —ciclo que refleja la velocidad exponencial de la innovación en IA—. Además, la CECA no solo reguló, sino que financió la modernización industrial mediante préstamos condicionados a estándares comunes. Un Fondo Europeo de Interoperabilidad podría replicar este modelo en la era digital:

A fin de Financiar proyectos de IA pública que prioricen bienes comunes (ej.: modelos climáticos abiertos, diagnósticos médicos federados), condicionando los fondos a la adopción de protocolos de la AEDIA. Así como crear mercados prioritarios para empresas que compartan datos no personales (ej.:

patrones de movilidad urbana) bajo licencias de uso ético, similar a los «contratos de concesión» de la CECA para minas de carbón.

4.2. Dimensión Geopolítica y ética: de la Diplomacia de Estándares a la IA como Bien Público

China ha convertido la IA en un instrumento de poder blando mediante la Nueva Ruta de la Seda Digital, exportando infraestructuras con estándares compatibles con su marco autoritario (Zhang, 2023). Frente a esto, la UE debe: Negociar cláusulas espejo en acuerdos comerciales, exigiendo equivalencia en protección de datos y transparencia algorítmica para acceder al mercado único (ej.: condicionar el acceso de empresas estadounidenses a la adopción de normas GDPR). Liderar una Alianza de Democracias Digitales con socios como Canadá, Japón y Corea del Sur, creando un «Espacio de Datos Transatlántico» con estándares éticos comunes y moratorias compartidas sobre usos bélicos de la IA. Esta estrategia evitaría la bifurcación tecnológica actual, donde la UE queda atrapada entre el modelo estadounidense de capitalismo de datos y el autoritarismo digital chino. Como señaló la Comisión Von der Leyen: «*La soberanía europea no se construye contra otros, sino mediante alianzas basadas en valores*» (European Commission, 2023).

Así, una «Alta Autoridad Digital» —adaptada al siglo XXI— permitiría traducir valores europeos en reglas exigibles y ofrecería un punto focal para la diplomacia regulatoria. Así, la interdependencia dejaría de ser una fuente de vulnerabilidad y pasaría a ser un activo estratégico, como sucedió con el carbón y el acero.

Por otro lado, y en lo que se refiere a la gobernanza ética de la IA, el enfoque regulatorio Europeo que comprender la IA como producto —centrada en riesgos sectoriales— ignora su naturaleza dual: herramienta técnica y arquitectura de poder social. La UE debe redefinir la IA como *infraestructura de interés público*, sujeta a principios de transparencia radical (acceso a códigos fuente de sistemas críticos) y responsabilidad solidaria (fabricantes, usuarios y Estados como corresponsables ante daños sistémicos). Esto implicaría: Crear un Registro Paneuropeo de Modelos de IA, con metadatos auditables sobre datos de entrenamiento y sesgos detectados (inspirado en el Registro de Sustancias Químicas REACH). Así como el establecimiento de tribunales especializados en IA, adscritos al TJUE, para resolver disputas transfronterizas sobre responsabilidad civil o discriminación algorítmica.

CONCLUSIÓN: UN NUEVO CONTRATO SOCIAL PARA LA ERA DIGITAL

La fragmentación digital en la Unión Europea (UE) representa un desafío existencial en un mundo donde los datos y los sistemas computacionales

planetarios (SCP) se han erigido como pilares estratégicos para abordar crisis globales, desde el cambio climático hasta la erosión del contrato social. Este artículo ha demostrado que, ante la emergencia de un orden tecnológico dominado por modelos centralizados como el chino o dinámicas hipercompetitivas como la estadounidense, la UE enfrenta una disyuntiva histórica: avanzar hacia una integración federalista inspirada en el legado de la Comunidad Europea del Carbón y del Acero (CECA) o arriesgarse a la irrelevancia geopolítica.

En este sentido, el Tratado de la CECA (1951) ofrece un modelo paradigmático de gestión supranacional de recursos estratégicos. Su Alta Autoridad —con competencias ejecutivas y capacidad para imponer armonización— resolvió tensiones entre soberanías nacionales mediante interdependencia institucionalizada. En la actualidad, los datos exigen un enfoque similar: la creación de una Agencia Digital Europea con poderes vinculantes para federar datos críticos (climáticos, sanitarios, logísticos), estandarizar protocolos técnicos y supervisar ecosistemas de inteligencia artificial (IA). Esta entidad, análoga a la CECA, evitaría la fragmentación actual derivada de marcos regulatorios lentos, autoridades nacionales divergentes y estándares sectoriales incompatibles.

El análisis contrastante entre la UE y China revela dos modelos antagónicos. Mientras la UE navega entre la protección de derechos fundamentales (RGPD) y la innovación, su regulación fragmentaria —ejemplificada por el Reglamento de IA (2024) y el Reglamento de Gobernanza de Datos (2022)— perpetúa silos y asimetrías. China, en cambio, ha convertido los datos en «activo nacional» bajo control estatal, priorizando cohesión estratégica sobre privacidad. La paradoja es evidente: la UE aspira a un equilibrio ético, pero su arquitectura intergubernamental limita su capacidad para competir con modelos autoritarios más ágiles.

Para superar esta encrucijada, se proponen tres ejes de acción:

- **Federalización de datos:** Establecer «pools» paneuropeos de datos estratégicos gestionados mediante tecnologías federadas (blockchain soberana, cifrado homomórfico), garantizando acceso equitativo y cumplimiento ético.
- **Diplomacia de estándares:** Promover cláusulas espejo en acuerdos comerciales que exijan adhesión a normas europeas (RGPD, AI Act) para acceder al mercado único, contrarrestando la influencia de estándares chinos o estadounidenses.
- **Innovación ética:** Reconocer la IA como bien público, sujeto a auditorías continuas, transparencia algorítmica y responsabilidad solidaria entre Estados, empresas y usuarios.

La UE no puede permitirse repetir los errores de la CECA revisada (1967), que diluyó su autoridad supranacional en estructuras intergubernamentales. La crisis climática, la creciente desconfianza ciudadana y la carrera por la IA exigen un nuevo contrato digital basado en principios ilustrados: coopera-

ción, derechos fundamentales y soberanía compartida. Sin una Agencia Digital e Inteligencia Artificial Europea con dientes jurídicos, Europa verá cómo su modelo de gobernanza —aunque éticamente superior— queda marginado frente a sistemas menos democráticos pero más cohesionados.

En definitiva, la construcción de un Espacio Europeo de Datos e Inteligencia Artificial no es solo una cuestión técnica o legal, sino un imperativo político. Al igual que el carbón y el acero forjaron la paz posbélica, los datos y la IA pueden cimentar la relevancia geopolítica de la UE en el siglo XXI. Pero ello requiere audacia para trascender nacionalismos digitales y voluntad para replicar, en clave moderna, el espíritu federalista de los padres fundadores. El tiempo de actuar es ahora: en la era de los sistemas computacionales planetarios, la fragmentación no es una opción.

BIBLIOGRAFÍA

- Alexiadis, Peter, Tony Shortall, Alejandro Guerrero, and Nikos Nikolinakos. 2023. «Coherence versus Fragmentation: Institutional Challenges to EU Digital Markets Regulation». *Business Law International* 24. <https://heinonline.org/HOL/Page?handle=hein.journals/blawintl24&id=253&div=&collection=>.
- Aschenbrenner, Leopold. 2024. «The Decade Ahead». *Situational Awareness*. San Francisco: Situational Awareness.
- Bernal, Natasha. 2018. «IBM Watson AI Criticised after Giving ‘unsafe’ Cancer Treatment Advice». *The Telegraph*. July 27, 2018. <https://www.telegraph.co.uk/technology/2018/07/27/ibm-watson-ai-criticised-giving-unsafe-cancer-treatment-advice/>.
- «BOE-A-2005-2528 Instrumento de Ratificación Del Convenio Sobre El Acceso a La Información, La Participación Del Público En La Toma de Decisiones y El Acceso a La Justicia En Materia de Medio Ambiente, Hecho En Aarhus (Dinamarca), El 25 de Junio de 1998». 2005. *BOE*. February 16, 2005. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2005-2528.
- Boehm, Sophie, Katie Lebling, Kelly Levin, Hanna Fekete, Joel Jaeger, Richard Waite, Anna Nilsson, *et al.* 2021. “State of Climate Action 2021: Systems Transformations Required to Limit Global Warming to 1,5°C.” *World Resources Institute*. <https://doi.org/10.46830/wriprt.21.00048>.
- Bratton, Benjamin. 2017. *The Stack: On Software and Sovereignty*. MIT. https://books.google.com/books/about/The_Stack.html?hl=es&id=dEGdCwAAQBAJ.
- . 2023. «Antikythera ». 2023. <https://research.antikythera.org/>.
- Broek, Elmira van den, Anastasia Sergeeva, and Marleen Huysman. 2021. «When the Machine Meets the Expert: An Ethnography of Developing Ai for Hiring». *MIS Quarterly: Management Information Systems* 45 (3): 1557. <https://doi.org/10.25300/MISQ/2021/16559>.
- CA. 2025. «Cyber Space Administration of China中央网络安全和信息化委员会办公室». CN. 2025. <https://www.cac.gov.cn/>.
- California. 2024. «Bill Text - SB-1047 Safe and Secure Innovation for Frontier Artificial Intelligence Models Act». California Legislative Information. 2024. https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1047.
- Catanzariti, Mariavittoria. 2024. *Disconnecting Sovereignty : How Data Fragmentation Reshapes the Law*. Padua: Springer. https://books.google.com/books/about/Disconnecting_Sovereignty.html?hl=es&id=L48YEQAQBAJ.

- CE. 2020. «COM(2020) 66 Final Una Estrategia Europea de Datos». Comisión Europea. February 19, 2020. <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066>.
- . 2025a. «Centro de Apoyo a Los Espacios de Datos | Configurar El Futuro Digital de Europa». Comisión Europea. 2025. <https://digital-strategy.ec.europa.eu/es/news/data-spaces-support-centre>.
- . 2025b. «El Programa Europa Digital | Configurar El Futuro Digital de Europa». Comisión Europea. 2025. <https://digital-strategy.ec.europa.eu/es/activities/digital-programme>.
- . 2025c. «Reglamento Relativo al Espacio Europeo de Datos de Salud (EEDS) - Comisión Europea». Comisión Europea. 2025. https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_es.
- . n.d.-a. «Espacios Comunes Europeos de Datos | Configurar El Futuro Digital de Europa». Comisión Europea. Accessed July 16, 2025. <https://digital-strategy.ec.europa.eu/es/policies/data-spaces>.
- . n.d.-b. «Estrategia Europea de Datos - Comisión Europea». Comisión Europea. Accessed July 16, 2025. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es.
- . n.d.-c. «Horizon Europe». Comisión Europea. Accessed July 16, 2025. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
- CEPEJ. 2024. «The CEPEJ Publishes Its New Evaluation Report on European Judicial Systems - European Commission for the Efficiency of Justice (CEPEJ)». CEPEJ. October 16, 2024. <https://www.coe.int/en/web/cepej/-/the-cepej-publishes-its-new-evaluation-report-on-european-judicial-systems>.
- Cerny, Philip G. 2007. «Neomedievalism, Civil War and the New Security Dilemma: Globalisation as Durable Disorder». *Http://Dx.Doi.Org/10.1080/13698249808402366* 1 (1): 36–64. <https://doi.org/10.1080/13698249808402366>.
- China.org.cn. 2024. «Belt and Road Initiative: Business Community Drives Innovative Cooperation and Exchanges within BRI». China.Org.Cn. September 21, 2024.
- CNIL. 2021. «SAN-2021-023». December 31.
- Colchen, Gabrielle. 2022. «Francia Impone Multas Millonarias a Google y Facebook Por Su Política de Cookies». France24. June 1, 2022. <https://www.france24.com/es/econom%C3%ADa-y-tecnolog%C3%ADa/20220106-google-facebook-multa-francia-cookies>.
- Cologne Regional Court. 2023. «Center North Rhine-Westphalia e.V., Vertr. d. d. Vorstand Wolfgang Schuldzinski, Mintropstraße 27, 40215 Düsseldorf», December 1, 2023. <https://drive.google.com/file/d/1jL27otUWwCzJKZtnk8GAm-ynxMdKZECd/view>.
- Comisión Europea. 2024. «Reglamento EIDAS | Configurar El Futuro Digital de Europa». April 4, 2024. <https://digital-strategy.ec.europa.eu/es/policies/eidas-regulation>.
- Cong, Wang, and Yin Yeping. 2023. «China Launches Global AI Governance Initiative, Offering an Open Approach in Contrast to US Blockade - Global Times». Global Times. 2023. <https://www.globaltimes.cn/page/202310/1300092.shtml>.
- CERPC -Consejo de Estado de la República Popular de China-. 2017. «国务院关于印发新一代人工智能发展规划的通知_科技_中国政府网». 2017. https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.
- Copernicus. 2025. «Global Climate Highlights 2024 ». European Commission. January 10, 2025. <https://climate.copernicus.eu/global-climate-highlights-2024>.
- Curia. 2012. «C-128/11 - UsedSoft». Curia. July 3, 2012. <https://curia.europa.eu/juris/liste.jsf?num=C-128/11>.
- CURIA. 2020. « C-311/18 - Facebook Ireland y Schrems». InfoCuria. July 16, 2020. <https://curia.europa.eu/juris/liste.jsf?num=C-311/18&language=ES>.

- . 2023. Asunto C-807/21 Deutsche Wohnen SE contra Staatsanwaltschaft Berlin.
- DigiChina. 2017. «Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)». Stanford University. June 1, 2017. <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>.
- . 2021. «Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)». Stanford. September 1, 2021. <https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/>.
- Dillet, Romain. 2020. «France's Health Data Hub to Move to European Cloud Infrastructure to Avoid EU-US Data Transfers | TechCrunch». October 12, 2020. https://techcrunch.com/2020/10/12/frances-health-data-hub-to-move-to-european-cloud-infrastructure-to-avoid-eu-us-data-transfers/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2x1LmNvbS8&guce_referrer_sig=AQAAAHDEq-Z8c3Mokj99NQIMNYS1sQlXcN6T3Pp9Bcr3rO0erUZevSvX3WDOIGMX0Vbg1b5d_t70-Z1PTX1INPh_KdBGSPb3RFM_8dgO98jBUolCp772RqDs8aWCb9KXcdyqJfqHwV3lTPZh3DvpnyQyTPc6UHABq2hD0gJnZw_eqyQd.
- «Directiva - 2024/2853». 2024. EUR-Lex. October 23, 2024. <https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32024L2853>.
- CE. 2025. «Simpl: Cloud-to-Edge Federations Empowering EU Data Spaces | Shaping Europe's Digital Future». European Commission. 2025. <https://digital-strategy.ec.europa.eu/en/policies/simpl>.
- EDPB. 2021. «Opinion 05/2021 on the Draft Administrative Arrangement for the Transfer of Personal Data between the Haut Conseil Du Commissariat Aux Comptes (H3C) and the Public Company Accounting Oversight Board (PCAOB) | European Data Protection Board». EDPB. February 2, 2021. https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-052021-draft-administrative-arrangement_en.
- . 2023. «Contribution of the EDPB to the Report on the Application of the GDPR under Article 97 - 2023 | European Data Protection Board». EDPB. 2023. https://www.edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-report-application-gdpr-under-article-97-2023_en.
- Edwards, Lilian, and Michael Veale. 2017. «Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For». *Duke Law & Technology Review* 16. <https://heinonline.org/HOL/Page?handle=hein.journals/dltr16&id=18&div=&collection=>.
- «Estrategia Europea de Datos - Comisión Europea». 2025. Comisión Europea. 2025. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es.
- EU. 1985. «Directiva - 85/374 ». EUR-Lex. July 25, 1985. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:31985L0374>.
- «EU-Japan Economic Partnership Agreement». 2019. European Commission. February 1, 2019. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan/eu-japan-agreement_en.
- European Commission. 2016. «Directiva - 2016/1148 - ES - EUR-Lex». EUR-Lex. June 7, 2016. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32016L1148>.
- . 2018. «Reglamento - 2018/842». EUR-Lex. May 30, 2018. <https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32018R0842>.
- . 2019. «Directiva - 2019/790 - ES - Copyright - EUR-Lex». Eur-Lex. April 17, 2019. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32019L0790>.
- . 2024. «Second Report on the Application of the General Data Protection Regulation - COM/2024/357 Final». Eur-Lex. 2024. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024DC0357>.

- European Commission. 2014. «Reglamento - 910/2014 - ES - e-IDAS - EUR - Lex». EUR-Lex. July 23, 2014. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32014R0910>.
- . 2019. «Reglamento - 2019/881 - ES - EUR-Lex». EUR-Lex. April 17, 2019. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32019R0881>.
- . 2024a. «AI Act | Shaping Europe's Digital Future». EC. 2024. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.
- . 2024b. «European Data Governance Act | Shaping Europe's Digital Future». European Commission. 2024. <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>.
- European Union. 2024. «Standard Eurobarometer 102 - Autumn 2024 - November 2024 – Eurobarometer Survey». Eurobarometer 102. 2024. <https://europa.eu/eurobarometer/surveys/detail/3215>.
- Eurostat. 2024. «Living Conditions in Europe - Poverty and Social Exclusion - Statistics Explained». EU. June 2024. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Living_conditions_in_Europe_-_poverty_and_social_exclusion.
- Feeny, David, Fikret Berkes, Bonnie J. McCay, and James M. Acheson. 1990. «The Tragedy of the Commons: Twenty-Two Years Later». *Human Ecology* 18 (1): 1–19. <https://doi.org/10.1007/BF00889070>.
- Fernández Hernández, Carlos. 2023. «Alemania Avanza En El Diseño de La Estandarización de La Inteligencia Artificial». *DiarioLaLey*. May 3, 2023. https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAA AAAAEAC2NQUVeQAYFf41zEZa2rlYPuXTXm4hoEa_pTGgH2smaZOr23zu-6G3iER768951Jtp7OBp6T5iUGlltaTkKKTrfEaVugl0zOcFCoblpfFzUOvWWcj-yhbto_F1fqcYDGsQSSboPKGRvO76Tw8HjvdOKIV1zjiBY5dSiX2BgCPH9VZer2a-X9Xu5VECwCfcaRk5KY4Ti9FduGVUPz0hiNBKc9LYXiHejpfL102K9-DpY9_7_xc9hGNDjhTCTfeXx3_QE34AAAAWKE.
- Floridi, L. 2013. «The Philosophy of Information». [https://books.google.es/books?hl=es&lr=&id=l8RoAgAAQBAJ&oi=fnd&pg=PR5&dq=Luciano+Floridi+\(2013&ots=p4HK5R9rDd&sig=0E5yFGd3nZDWx75J5jUjDaWFBns](https://books.google.es/books?hl=es&lr=&id=l8RoAgAAQBAJ&oi=fnd&pg=PR5&dq=Luciano+Floridi+(2013&ots=p4HK5R9rDd&sig=0E5yFGd3nZDWx75J5jUjDaWFBns).
- Frischmann, BM, A Marciano, GB Ramello - Journal of Economic, and undefined 2019. 2019. «Retrospectives: Tragedy of the Commons after 50 Years». *Acateweb.Org* 33 (4): 211–28. <https://doi.org/10.1257/jep.33.4.211>.
- GPDPI «Garante per La Protezione Dei Dati Personali (Italy) - 10040382 - GDPRhub». n.d. GDPRhub. Accessed March 25, 2025. [https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_\(Italy\)_-10040382](https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-10040382).
- Gardner, Roy, Elinor Ostrom, and James M. Walker. 1990. «The Nature of Common-Pool Resource Problems». *Rationality and Society* 2 (3): 335–58. <https://doi.org/10.1177/1043463190002003005>.
- GCP. n.d. «Global Carbon Project (GCP)». Global Carbon Project (GCP). Accessed March 21, 2025.
- «GDPR Enforcement Tracker - List of GDPR Fines». n.d. Accessed March 25, 2025. <https://www.enforcementtracker.com/>.
- General Assembly UN. 2022. «Resolución 76/300 de La ONU, 2022». United Nations. 2022. <https://docs.un.org/en/A/76/L.75>.
- Gonzalez, Fernando. 2024. «El Gobierno de Javier Milei Usará IA Para Patrullar Las Redes Sociales y, Según Dice, Predecir Delitos». *Wired*. August 1, 2024.
- Heller, Michael A. 1998. «The Tragedy of the Anticommons: Property in the Transition from Marx to Markets». *Harvard Law Review* 112 (3): 622. <https://doi.org/10.2307/1342203>.
- Hou, Rui, and Diana Fu. 2024. «Sorting Citizens: Governing via China's Social Credit System». *Governance* 37 (1): 59–78. <https://doi.org/10.1111/GOVE.12751>.

- Huaxia. 2019. «China Focus: China Adopts Law on Cryptography - Xinhua | English. News.Cn». Xinhuanet. October 26, 2019. http://www.xinhuanet.com/english/2019-10/26/c_138505655.htm.
- IPPC. 2024. «IPCC». 2024. <https://www.ipcc.ch/languages-2/spanish/>.
- Jiang, Ben. 2024. «China Eyes at Least 50 Sets of AI Standards by 2026, from Chips to Applications and Safety». *SouthChina Post*, July 2, 2024.
- Jordon, James, Lukasz Szpruch, Florimond Houssiau, Mirko Bottarelli, Giovanni Cherubin, Carsten Maple, Samuel N. Cohen, and Adrian Weller. 2022. «Synthetic Data – What, Why and How?». May. <https://arxiv.org/abs/2205.03257v1>.
- Karpo, Jonathan M. 2022. «The Tragedy of ‘The Tragedy of the Commons’: Hardin versus the Property Rights Theorists». *Https://Doi.Org/10.1086/718857* 65 (S1): S65–84. <https://doi.org/10.1086/718857>.
- Klotz, Sebastian. 2023. «Who Drives the International Standardisation of Telecommunication and Digitalisation? Introducing a New Data Set». *Global Policy* 14 (3): 558–68. <https://doi.org/10.1111/1758-5899.13223>.
- Kuhn, Thomas S. 1962. «Historical Structure of Scientific Discovery». *Science* 136 (3518): 760–64. <https://doi.org/10.1126/SCIENCE.136.3518.760>.
- Lazard. 2023. «The Geopolitics of Artificial Intelligence».
- Leonelli, Sabina. 2016. «Locating Ethics in Data Science: Responsibility and Accountability in Global and Distributed Knowledge Production Systems». *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374 (2083). <https://doi.org/10.1098/RSTA.2016.0122>.
- Lin, Yiran. 2024. «More Than an Enforcement Problem: The General Data Protection Regulation, Legal Fragmentation, and Transnational Data Governance. Columbia Journal of Transnational Law 1(64) 1-39. Accessed March 25, 2025. https://openurl.ebsco.com/EPDB%3Agcd%3A2%3A29525906/detailv2?sid=ebsco%3Aplink%3Aascholar&iid=ebsco%3Agcd%3A175996185&crl=c&link_origin=scholar.google.es.
- Martinez- Quirante, Roser, and Joaquín Rodríguez-Álvarez. 2020. «El Lado Oscuro de La Inteligencia Artificial ». *IDEES*, no. 48 (May). <https://revistaidees.cat/es/el-lado-oscuro-de-la-inteligencia-artificial/>.
- Martinez-Quirante, Roser, and Joaquín Rodríguez-Alvarez. 2018. *Inteligencia Artificial y Armas Letales Autónomas: Un Nuevo Reto Para Naciones Unidas*. Oviedo: Trea.
- Mejías, Ulises A, and Nick Couldry. 2019. «Colonialismo de Datos: Repensando La Relación de Los Datos Masivos Con El Sujeto Contemporáneo». *Virtualis* 10 (18): 78–97. <https://doi.org/10.2123/VIRTUALIS.V10I18.289>.
- ME «Tesla, Obligada a Pagar Por Sus Polémicas Actualizaciones Remotas». 2024. Movilidad Eléctrica. September 25, 2024. <https://movilidadelectrica.com/tesla-obligada-a-indemnizar-clientes-por-sus-polemicas-actualizaciones-remotas/>.
- Nadia, Helmy. 2024. «Digital Silk Road as Part of the Chinese National Strategy - Modern Diplomacy». *ModernDiplomacy*. April 7, 2024. <https://moderndiplomacy.eu/2024/04/07/digital-silk-road-as-part-of-the-chinese-national-strategy/>.
- NextCloud. 2022. «Europa Intensifica La Lucha Por La Soberanía Digital y Prohíbe 365 y Workspace En Más Lugares - Nextcloud». NextCloud. November 29, 2022. <https://nextcloud.com/es/blog/europa-intensifica-la-lucha-por-la-soberania-digital-y-prohibe-365-y-workspace-en-mas-lugares/>.
- OLAF. 2023. «The OLAF Report 2023». European Anti-Fraud Office. December 31, 2023. https://ec.europa.eu/olaf-report/2023/index_en.html.
- PRC. 2017. «PRC National Intelligence Law (as Amended in 2018)». *ChinaLaw* . June 27, 2017. <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>.
- . 2020. «GB/T 35273-2020 PDF English». State Administration for Market Regulation, Standardization Administration of PRC. March 6, 2020. <https://www.chineses-tandard.net/PDF.aspx/GBT35273-2020>.

- . 2021. «Personal Information Protection Law of the People's Republic of China - PIPL». PIPL. August 20, 2021. <https://personalinformationprotectionlaw.com/>.
- Rodríguez, Joaquín. 2016. *La Civilización Ausente: Tecnología y Sociedad En La Era de La Incertidumbre*. 1st ed. Oviedo: Trea.
- Rodríguez, Joaquín, Xavi Mojal, Tica Font, and Pere Brunet. 2019. «Nuevas Armas Contra La Ética y Las Personas: Drones Armados y Drones Autónomos». Barcelona. http://arxiu.centredelas.org/images/INFORMES_i_altres_PDF/informe39_DronesArmados_CAST_web_DEF.pdf.
- Rodriguez-Alvarez, Joaquin David. 2023. «Crisis Climática y Transición Energética: Del Neomedievalismo al Tecnomedievalismo». *Revista de Ciencias Sociales Segunda Época* 13 (44): 77–109. <https://portalrecerca.uab.cat/en/publications/crisis-clim%C3%A1tica-y-transici%C3%B3n-energ%C3%A9tica-del-neomedievalismo-al-t>.
- Singapore. 2024. «National AI Strategy». Smart Nation Singapore. September 24, 2024.
- CECA. 1951. «Tratado Constitutivo de La Comunidad Europea Del Carbón y Del Acero, Tratado CECA». Eur-Lex. 1951. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:xy0022>.
- UAE. 2024. «UAE Strategy for Artificial Intelligence». UAW. September 24, 2024.
- UKGOV. 2022. «National AI Strategy». Government UK. December 18, 2022.
- UN. 1982. «BOE-A-1997-3296 Instrumento de Ratificación de La Convención de Las Naciones Unidas Sobre El Derecho Del Mar, Hecho En Montego Bay El 10 de Diciembre de 1982». BOE. December 10, 1982. <https://www.boe.es/buscar/doc.php?id=BOE-A-1997-3296>.
- UNFCCC. 2015. «The Paris Agreement ». UN. December 12, 2015. <https://unfccc.int/process-and-meetings/the-paris-agreement>.
- Unión Europea. 2021. «BOE.Es - DOUE-L-2021-80615 Reglamento (UE) 2021/696 Del Parlamento Europeo y Del Consejo de 28 de Abril de 2021 Por El Que Se Crean El Programa Espacial de La Unión y La Agencia de La Unión Europea Para El Programa Espacial y Por El Que Se Derogan Los Reglamentos (UE) No 912/2010, (UE) No 1285/2013 y (UE) No 377/2014 y La Decisión No 541/2014/UE». BOE. May 12, 2021. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80615>.
- Veale, Michael, and Frederik Zuiderveen Borgesius. 2021. «Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach». *Computer Law Review International* 22 (4): 97–112. <https://doi.org/10.9785/CRI-2021-220402>.
- Winter, T. 2020. «Silk Road Diplomacy: Geopolitics and Histories of Connectivity». *International Journal of Cultural Policy* 26 (7): 898–912. <https://doi.org/10.1080/10286632.2020.1765164>.
- «World Report 2025: China». 2025. HRW. 2025. <https://www.hrw.org/world-report/2025/country-chapters/china>.
- Zhang, Y, D Tsang, and DL Fuschi. 2020. «Chinese Multinationals on the New Silk Route: Managing Political Risk by Branding the Nation». *Thunderbird International Bussines Review* 62 (3): 291–303. <https://doi.org/10.1002/tie.22131>.
- Zhao, Hailing, and Tingting Liu. 2025. «China's Social Credit System and the Family: Punishment and Collective Resistance». *Economy and Society*, January. <https://doi.org/10.1080/03085147.2024.2422187>.
- Zuboff, Shoshana. 2019. «Surveillance Capitalism and the Challenge of Collective Action». *New Labor Forum* 28 (1): 10–29. https://doi.org/10.1177/1095796018819461/ASSET/953342DD-F595-40AA-9440-5E9F95C61AEB/ASSETS/IMAGES/LARGE/10.1177_1095796018819461-FIG1.JPG.