La protección de datos personales como derecho fundamental global: bases, fragmentación internacional y propuestas disruptivas para un nuevo constitucionalismo digital

Personal Data Protection as a Global Fundamental Right: Foundations, International Fragmentation, and Disruptive Proposals for a New Digital Constitutionalism

Francisco Lepor Giron[1]
Universidad Latinoamericana y del Caribe – Caracas, Venezuela
fleporeg@ulac.edu.ve

José Alejandro Alvarado De Lima[2]
Universidad de San Buenaventura – Cartagena, Colombia
jose.alvarado@usbctg.edu.co

Jaime Junior Blanco Navarro[3]
Universidad de San Buenaventura – Cartagena, Colombia
jaime.blanco@usbctg.edu.co

Cómo citar/ How to cite: Lepor, F., Alvarado, J. & Blanco, J. (2026). La protección de datos personales como derecho fundamental global: bases, fragmentación internacional y propuestas disruptivas para un nuevo constitucionalismo digital. *Revista Saber, Ciencia y Libertad*, 21(2), 139 – 159. https://doi.org/10.18041/2382-3240/saber.2026v21n2.14043

Resumen

Este ensayo aborda la protección de datos personales como un derecho fundamental autónomo, diferenciado de la privacidad, y analiza su evolución desde los principios de los años ochenta hasta el actual

Fecha de recepción: 4 de abril de 2026
Fecha de evaluación: 22 de mayo de 2026
Fecha de aceptación: 14 de julio de 2026

Este es un artículo Open Access bajo la licencia BY-NC-SA
(http://creativecommons.org/licenses/by-nc-sa/4.0/)
Published by Universidad Libre

1 Especialista en Derecho Penal, Especialista en Derecho Penal Internacional, Especialista en Control de la Gestión Pública e Internacional Humanitario. Doctor en Derecho Internacional Público (Mención Derechos Humanos). Doctor en Pedagogía Crítica. Universidad Latinoamericana del Caribe (ULAC) Venezuela.

2 Especialista en Derecho Internacional de los Derechos Humanos y Cultura de Paz. Magister en Derecho e Integración Económica, Doctor en Política y Gestión de la Educación Superior. Docente Universitario – Universidad de San Buenaventura – Cartagena – Colombia.

3 Abogado, especialista en derecho administrativo y contractual, magister en derecho, docente universitario de pre grado en la Universidad de San Buenaventura seccional Cartagena, miembro del consejo directivo de la USB Colombia, docente de posgrados, asesor jurídico de entidades públicas

escenario de fragmentación normativa internacional. Se examinan críticamente los instrumentos existentes --Convenio 108+, RGPD, decisiones de adecuación, jurisprudencia del TJUE y TEDH-- y se constata una brecha estructural entre la naturaleza global de los flujos de datos y la naturaleza nacional o regional de los mecanismos de tutela. Con base en más de cincuenta años de práctica, el trabajo propone ocho fórmulas inéditas: desde un Tratado de La Haya sobre protección de datos con corte internacional, hasta una licencia digital universal, un defensor global de datos con mediación expedita, cláusulas de revisión tecnológica automática, un botón de pánico digital, responsabilidad penal de directivos algorítmicos, auditoría ciudadana de algoritmos y un fondo de resarcimiento colectivo transfronterizo. Se concluye que la única respuesta a la altura del desafío tecnológico es una combinación de audacia institucional y empoderamiento ciudadano real.

Palabras clave

Derecho internacional; Gobernanza algorítmica; Protección de datos personales; Propuestas de lege ferenda; Transferencias internacionales

Abstract

This essay addresses personal data protection as an autonomous fundamental right, distinct from privacy, and analyzes its evolution from the early 1980s to the current scenario of international normative fragmentation. Existing instrument, Convention 108+, GDPR, adequacy decisions, CJEU and ECtHR case law, are critically examined, revealing a structural gap between the global nature of data flows and the national or regional nature of protection mechanisms. Based on more than fifty years of practice, the paper proposes eight unprecedented formulas: from a Hague Treaty on data protection with an international scope, to a universal digital license, a global data ombudsman with expedited mediation, automatic technological review clauses, a digital panic button, criminal liability for algorithmic executives, citizen auditing of algorithms, and a cross-border collective compensation fund. It concludes that the only response commensurate with the technological challenge is a combination of institutional boldness and genuine citizen empowerment.

Keywords

Algorithmic governance; International law; International transfers; Lege ferenda proposals; Personal data protection.

Introducción

Cuando se comenzó a estudiar el derecho a la intimidad frente a los primeros ficheros automatizados, a finales de los años setenta del siglo pasado, nadie imaginaba que medio siglo después se estaría discutiendo sobre el reconocimiento facial masivo en espacios públicos, la elaboración de perfiles conductuales de menores o la transferencia de datos genéticos entre continentes en cuestión de segundos. Ahora, tengo el privilegio. y a veces la desgracia, de asistir a la transformación más acelerada del derecho en la historia de la humanidad.

La protección de datos personales ha pasado de ser una curiosidad regulatoria a constituir un derecho fundamental autónomo en numerosos ordenamientos y, lo que es más relevante, un campo de conflicto geoestratégico de primera magnitud (TJUE, asunto C-131/12, 2014). Los datos ya no son solo un reflejo de nuestra identidad; son la materia prima de la economía digital, el combustible de la inteligencia artificial y, cada vez más, un arma de control social y dominación geopolítica. Sin embargo, el derecho internacional de la protección de datos permanece anclado en categorías del siglo XX: tratados bilaterales, cláusulas contractuales tipo, decisiones de adecuación que se invalidan cíclicamente y una cooperación administrativa que rara vez alcanza la velocidad de los flujos de datos. Este desfase no es un mero problema técnico; es una crisis de legitimidad del derecho en la era digital.

El presente ensayo no aspira a una exégesis más del RGPD o del Convenio 108. Existen ya excelentes comentarios. Mi propósito es diagnosticar las fracturas estructurales del sistema y atreverme a esbozar soluciones que aún no están sobre la mesa, sabiendo que algunas pueden sonar a provocación, que, en tiempos de parálisis normativa, es un deber intelectual. La literatura académica sobre protección de datos ha crecido exponencialmente desde 2018. Pero la inmensa mayoría de los trabajos se concentra en:

- El análisis dogmático del RGPD.
- Estudios de caso sobre decisiones de autoridades nacionales.
- Propuestas incrementales (mejores cláusulas contractuales, más armonización).

Existe, sin embargo, una carencia significativa de trabajos que adopten una perspectiva integral, que conecten los principios básicos con la realidad de la ejecución

transfronteriza y que, sobre todo, formulen propuestas verdaderamente rupturistas con base en la experiencia práctica de largo plazo. Como profesional preocupado en el tema, he acumulado una visión privilegiada de los puntos ciegos del sistema. Este ensayo responde a la convicción de que no se puede mejorar aquello que no se diagnostica con honestidad y que las reformas cosméticas, una nueva cláusula tipo, una guía interpretativa más, son insuficientes frente a la magnitud del problema. El valor añadido de este trabajo creo que reside, por tanto, en tres elementos: (i) su perspectiva temporal amplia, (ii) su enfoque crítico no complaciente con los sistemas vigentes, y (iii) la audacia de sus propuestas, que no temen enfrentarse a intereses arraigados.

En el plano teórico doctrinal, conviene subrayar que la protección de datos personales no es simplemente una extensión del derecho a la privacidad o a la intimidad, sino que se articula hoy como un derecho de autonomía informacional: el control que las personas deben ejercer sobre la captura, el tratamiento, la circulación y la utilización de su información personal (Schwartz, 1999). Esta noción conecta con la creciente idea de la protección de datos personales como un derecho de dignidad frente a estructuras de vigilancia y poder algorítmico. Asimismo, en el plano jurisprudencial, decisiones como Google Spain (Asunto C 131/12), en la que el TJUE reconoce el llamado “derecho al olvido” como manifestación del derecho fundamental a la protección de datos, han consolidado esa autonomía, mientras que la jurisprudencia del TEDH ha empezado a articular una protección reforzada frente a la vigilancia masiva (TEDH, Big Brother Watch, 2021).

Entre los objetivos planteados para delimitar la temática de este estudio está el de construir un marco analítico y propositivo integral sobre la protección de datos personales, desde sus fundamentos teóricos hasta su regulación internacional actual, identificando las principales disfunciones del sistema y ofreciendo soluciones inéditas orientadas a garantizar un recurso efectivo y una tutela real de los interesados en un entorno globalizado. Este propósito general, se desprende en los siguientes puntos:

- Sistematizar los principios jurídicos esenciales de la protección de datos, distinguiéndolos claramente del derecho a la privacidad y explicitando las categorías técnicas necesarias para su comprensión.
- Analizar críticamente el entramado normativo internacional (Convenio 108+, RGPD, decisiones de adecuación, jurisprudencia del TJUE y TEDH), señalando sus logros y sus limitaciones estructurales.
- Describir las vías de recurso administrativas y judiciales existentes, evaluando su efectividad real, especialmente en supuestos transfronterizos.

- Identificar las brechas más profundas del sistema: asimetría de poder, fragmentación jurisdiccional, obsolescencia tecnológica de las normas, y falta de protección frente a la vigilancia masiva extranjera.
- Formular propuestas de lege ferenda, concretas y novedosas, que combinen creatividad institucional, innovación tecnológica y garantías procesales.
- Ofrecer un esquema práctico para que los interesados, los profesionales y los responsables de tratamiento puedan orientarse en el estado actual del derecho, mientras se debate su futuro.

Metodología

El abordaje metodológico sobre la fragmentación internacional de la protección de datos, validando así las propuestas de lege ferenda presentadas, el presente trabajo optó por un enfoque jurídico-proyectivo, cuyos fundamentos se hallan en tres ejes fundamentales:

- El eje de la Autonomía Informacional como Base Ontológica. En este punto, la metodología surge de la premisa de que el dato personal es reconocido como la unidad mínima de identidad; encontrando sustento en la Teoría de la Autodeterminación Informativa, conforme a la sentencia del Censo de 1983 del Tribunal Constitucional Federal Alemán. Con estos fundamentos, el enfoque metodológico trató solamente de la protección de datos como una parte importante del derecho a la intimidad, sino que también se constituye en un derecho de autonomía ante estructuras de poder algorítmico. Esta columna legitima el requerimiento de mecanismos como la Licencia Digital Universal, al manejar el control del dato como una extensión directa de la dignidad humana.
- El eje del Realismo Regulatorio, según el Efecto Bruselas. En este escenario, la metodología aplica los lineamientos de Bradford (2020), con el fin de justificar la viabilidad de las propuestas disruptivas. Esto debido a la imposibilidad de lograr una reforma formal de la Carta de la ONU o tratados universales por consenso. En ese sentido, el artículo hace uso del fenómeno del Efecto Bruselas como motor de cambio, identificando cómo los estándares más exigentes (RGPD, 108+) se han convertido en de facto en el estándar global por necesidad de mercado. Por esa razón, las propuestas que se presentan en este estudio se basan en las premisas de la gobernanza de red, en la que los estímulos económicos demandan la convergencia normativa.
- El eje de la Tutela Residual y Competencia Concurrente. En lo referente a las disposiciones de la Corte Internacional y el Puente Procedimental, el enfoque metodológico recurre a la doctrina de las competencias concurrentes (CIJ, Certain Expenses of the United Nations, 1962), ya que a nivel jurídico esto

permite argumentar que, si el Consejo de Seguridad o los mecanismos nacionales dimiten de su responsabilidad de salvaguardar los derechos primordiales por causa del bloqueo geopolítico o por la falta de capacidad, el derecho internacional hace reconocimiento a la legitimidad de vías subsidiarias para garantizar un recurso eficaz. De este modo, se da sustento a la creación de órganos de mediación expedita y cortes internacionales sin necesidad de una revisión constitucional global.

Instrumentos de análisis

La estrategia operativa se refiere a la Ingeniería Institucional, que está conformada por: i) un diagnóstico, para lograr una comparación funcional de legislaciones (UE, LATAM, Asia), detectando así las figuras de ejecución transfronteriza; ii) la auditoría de algoritmos, que se trata de la aplicación del marco de la Sociedad de la Caja Negra (Pasquale, 2015), cuyo fin es el de transformar la opacidad técnica en un problema de derecho procesal y probatorio; y iii) proyección, que favorece el diseño de mecanismos de lege ferenda, permitiendo combinar la técnica procesal existente, como la mediación, la amici curiae, las tasas de compensación, adjunta a nuevas garantías digitales.

Resultados

Fundamentos Ontológicos y Normativos de la Protección de Datos

El dato personal, reconocida como la unidad mínima de identidad, también se define como el objeto de protección que necesito de actos de rigor. Un dato personal es cualquier información concerniente a una persona física identificada o identificable. Esta definición, aparentemente clara, se ha expandido hasta abarcar no solo los datos obvios (nombre, NIF, dirección, etc.) sino también los seudónimos, las direcciones IP, los identificadores de cookies, los datos de localización, las huellas biométricas y los patrones de conducta inferidos algorítmicamente, entre otros (RGPD, art. 4.1; TJUE, asuntos C-70/10 y C-83/10, 2011) Una lección de medio siglo ha sido que la tecnología siempre encuentra nuevas formas de identificación y el derecho debe responder con principios funcionales, no con listas cerradas.

Los principios cardinales: el patrimonio común de la humanidad digital y los derechos de los interesados

Los principios formulados por la OCDE en 1980 y recogidos en el Convenio 108 siguen siendo el núcleo duro de cualquier legislación digna de ese nombre: lici-

tud y lealtad, limitación de la finalidad, minimización, exactitud, limitación de la conservación, seguridad y, más tardíamente, accountability y privacidad desde el diseño (OCDE, 1980/2013). Ninguna propuesta futura puede abandonarlos; todas deben partir de ellos.

El catálogo mínimo incluye acceso, rectificación, supresión (derecho al olvido), limitación, portabilidad, oposición y no ser objeto de decisiones automatizadas. Pero la experiencia muestra que la mera existencia normativa de estos derechos no basta; se requiere que su ejercicio sea sencillo, gratuito y efectivo. Aquí radica uno de los grandes fracasos del sistema actual: demasiados menús escondidos, demasiadas respuestas evasivas, demasiadas esperas.

El Tablero Internacional: Tratados, Tensiones y el Efecto Bruselas

En este apartado, se exponen tres capas normativas, es decir en una estratificación en la regulación internacional:

- Universal no vinculante: Directrices de la ONU de 1990, informes de Relatores Especiales. Importancia simbólica, pero escasa eficacia práctica.
- Regional vinculante (Consejo de Europa): Convenio 108 (1981) y su modernización (108+, 2018). Único tratado multilateral abierto a todo el mundo (Consejo de Europa, Convenio 108, 1981; Protocolo 108+, 2018). Su gran debilidad: mecanismos de supervisión limitados y ausencia de sanciones directas.
- Regional denso (Unión Europea): RGPD y Directiva de Policía y Justicia. Ha establecido el estándar de facto global por su poder de mercado, no por persuasión jurídica (Bradford, 2020).

El régimen de transferencias internacionales

Los datos que salen de una jurisdicción no deben perder la protección que tenían en ella. Las herramientas actuales, decisiones de adecuación, cláusulas contractuales tipo (SCC), normas corporativas vinculantes (BCR)-- son ingeniosas pero frágiles. El caso Schrems II (TJUE, 2020) demostró que unas SCC no pueden subsanar una legislación extranjera de vigilancia masiva (TJUE, asunto C-311/18, 2020). Esta lección debería haberse interiorizado hace décadas.

El conflicto de sistemas: ¿derecho fundamental o seguridad nacional?

El choque más profundo no es entre Estados, sino entre modelos normativos incompatibles: el modelo europeo (derecho fundamental con límites proporcionados), el modelo estadounidense (sectorial, basado en la confianza del consumidor

y con amplias excepciones de inteligencia) y el modelo chino, que incluye seguridad nacional y control social como ejes (Bradford, 2020). Ningún tratado universal será viable mientras no se resuelva esta contradicción de base. Sin embargo, sería un error reducir la cartografía global a solo esos tres modelos.

En América Latina, la protección de datos ha seguido una trayectoria mixta: países como Argentina (desde 2000) y Uruguay (desde 2008) obtuvieron decisiones de adecuación de la UE, mientras que Brasil (LGPD, 2018) ha optado por un modelo cercano al RGPD; pero con particularidades propias (autoridad nacional sancionadora, tratamiento específico de datos de menores, y un enfoque de "control efectivo" menos burocrático). Colombia, México, Chile y Perú cuentan con leyes de habeas data o protección de datos con influencia del Convenio 108. En África, Sudáfrica (Popia, 2013) ha servido de faro, aunque su implementación enfrenta desafíos de capacidad institucional.

En lo que se refiere a Asia, a Japón y a Corea del Sur, estos han logrado decisiones de adecuación de la UE, mientras que India (PIPL, en tramitación larga) e Indonesia muestran estándares en construcción. Estas experiencias no son meras copias del modelo europeo; incorporan adaptaciones a realidades locales, como la protección de datos de comunidades indígenas, el derecho a la identidad digital inclusiva, o mecanismos de denuncia presencial para poblaciones con bajo acceso a internet. Cualquier arquitectura internacional seria debe integrar esta diversidad, no como excepciones, sino como fuentes de innovación normativa (Greenleaf, 2021; CEJA, 2020).

Vías de Recurso: entre la Administración, los Jueces y el Vacío Transfronterizo.

La doble vía administrativa y judicial y el problema estructural: el interesado frente al gigante extranjero

Siempre se ha creído que el sistema debe ofrecer dos puertas de entrada, no excluyentes: la reclamación ante la autoridad de control (gratuita, ágil, sin necesidad de abogado) y la acción judicial directa (para quienes buscan indemnización o una tutela más rápida). El nuevo Reglamento Procesal del RGPD (UE 2025/2518) mejora la cooperación entre autoridades, pero mantiene plazos excesivos en la práctica.

Cuando el responsable del tratamiento está en un tercer país sin garantías adecuadas, las vías de recurso se evaporan. La Relatora Especial de la ONU lo ha llamado la "brecha global de privacidad" (Relatora Especial ONU, 2018). He sido testigo de decenas de casos en los que ciudadanos europeos veían sus datos reco-

gidos desde Singapur o Rusia sin posibilidad real de quejarse. El Marco Transatlántico UE-EE.UU. (DPF) es un avance relativo, pero sus mecanismos de recurso para extranjeros ante agencias de inteligencia siguen siendo claramente insuficientes, como el TJUE ya advirtió en Schrems II (TJUE, asunto C-311/18, 2020).

En paralelo, la experiencia empírica de casos como Cambridge Analytica o el uso de datos personales en contextos de conflicto armado revela cómo la brecha global adquiere dimensiones políticas y de seguridad internacional. La percepción de la privacidad, según barómetros europeos y encuestas como las del Pew Research Center, muestra una clara asimetría entre sensibilidad ciudadana y efectividad de la tutela legal.

La dimensión olvidada: impacto diferenciado y discriminación interseccional

Un análisis completo de las brechas estructurales no puede ignorar que la vulneración del derecho a la protección de datos afecta de manera desproporcionada a mujeres, minorías raciales, personas LGTBIQ+ y personas con discapacidad. Los algoritmos de selección de personal, concesión de crédito, diagnóstico médico, asignación de vivienda pública o perfilado policial han demostrado reproducir y amplificar sesgos históricos (Barocas, Hardt & Narayanan, 2017). Una mujer solicitante de un préstamo puede ser evaluada con parámetros que penalizan su historial de bajas por maternidad; una persona afrodescendiente puede ser sometida ha perfilado predictivo policial basado en datos de sobrerrepresentación estadística; una persona trans puede ver su nombre legal persistir en bases de datos pese a haberlo rectificado oficialmente.

En este contexto, la propuesta 7, que contiene auditoría ciudadana de algoritmos, ofrece un remedio técnico, pero el diagnóstico debe explicitar que la fragmentación normativa y la asimetría de poder se cruzan con la desigualdad estructural. Cualquier refundación del derecho internacional de la protección de datos debería incorporar un enfoque de derechos humanos interseccional, exigiendo que las evaluaciones de impacto incluyan análisis desagregados por género, raza, edad, discapacidad y orientación sexual, y que las autoridades de control cuenten con competencias específicas para sancionar la discriminación algorítmica indirecta.

El papel de las asociaciones y la acción colectiva

El artículo 80 del RGPD fue una revolución silenciosa. Por primera vez, organizaciones sin ánimo de lucro pueden representar intereses colectivos. Sin embargo, la práctica muestra que las asociaciones enfrentan barreras financieras y procesales. En este punto, se propone ampliar este derecho con la figura del "representante de

interés colectivo acreditado", similar al amici curiae, pero con legitimación activa propia.

DISCUSIÓN

Propuestas inéditas para una refundación del derecho a la protección de datos.

Tras medio siglo, se ha aprendido que las reformas graduales son necesarias, pero nunca suficientes cuando el desfase entre derecho y realidad es tan abismal. Por ello, me tomo la libertad de esbozar ocho propuestas que a continuación presento, esto es:

Propuesta 1. *Tratado de La Haya sobre Protección de Datos (THPD): creación de un tratado multilateral con una Corte Internacional de Protección de Datos competente para conocer reclamaciones individuales. No se trata de una corte más; su rasgo diferencial sería la legitimación activa directa de cualquier persona física, sin necesidad de que su Estado patrocine la demanda. Esta corte coexistiría con los sistemas nacionales, como ocurre con la Corte Interamericana de Derechos Humanos. Su financiación correría a cargo de un fondo basado en una tasa mínima sobre las transacciones digitales internacionales.*

Propuesta 2. *Licencia Digital Universal (LDU): un estándar técnico global, basado en identidades auto soberanas (self-sovereign identity), que permita a cada persona gestionar sus consentimientos, ejercer sus derechos y delegar en un agente de IA personal la negociación de condiciones de tratamiento. Se ha discutido esta idea con ingenieros de privacidad; es técnicamente factible con confidential computing y verifiable credentials (Allen, 2016; Hardman, 2021). Falta voluntad política.*

Propuesta 3. *Defensor Global de Datos y Oficinas de Mediación Expedita (OMED): una red de oficinas de mediación con plazo máximo de 30 días y resoluciones ejecutivas. Lo novedoso: si el responsable no comparece sin justa causa, se le aplica una presunción de veracidad de los hechos alegados por el interesado. El incumplimiento de la resolución acarrea la pérdida de un sello de confianza digital, que los buscadores y plataformas deben mostrar al usuario. La experiencia en sistemas de consumo muestra que la transparencia reputacional es más eficaz que las multas en muchos contextos.*

Propuesta 4. *Cláusula de Revisión Tecnológica Automática (CIRTA): ninguna ley debe quedar atrapada en referencias a tecnologías concretas. Se propone que las normas de protección de datos contengan un anexo técnico dinámico, actualizado semestralmente*

por una comisión independiente de expertos (no legisladores), que defina qué elementos se consideran identificadores o qué técnicas se consideran vigilancia prohibida. La comisión estaría compuesta por representantes de autoridades de control, academia y sociedad civil, excluyendo explícitamente a los grupos de interés económico.

Propuesta 5. *Botón de Pánico Digital y derecho al apagado de emergencia: una de las ideas que más resistencias ha despertado, pero que considero éticamente ineludible. Toda persona en situación de riesgo grave (violencia de género, persecución política, acoso extremo) podría activar un estado de emergencia de datos mediante un gesto sencillo (pulsaciones rápidas en el móvil, aplicación dedicada, oficinas públicas). Durante 72 horas, sin necesidad de autorización judicial previa, todos los responsables de tratamiento deben aislar sus datos en un "búnker digital", asignarle credenciales anónimas temporales y suspender cualquier tratamiento ordinario. Pasadas las 72 horas, se requiere ratificación judicial bajo control de legalidad. El miedo al fraude no puede impedir proteger a las víctimas reales.*

Para desincentivar activaciones maliciosas sin paralizar el uso legítimo, se establecería un sistema de responsabilidad escalonada. Toda persona que active el botón de pánico sin causa justificada y con ánimo de perjudicar a un tercero (por ejemplo, para ocultar pruebas en un litigio, boicotear a un empleador o acosar a un competidor) incurriría en una infracción grave sancionable con una multa significativa (al menos 10.000 euros) y, en caso de daños acreditados, responsabilidad civil por los perjuicios causados. La carga de probar la mala fe correspondería al presunto damnificado, no al activante, invirtiendo la presunción habitual para no desalentar a víctimas genuinas.

Adicionalmente, el juez o autoridad de control que ratifique o revoque la medida pasada las 72 horas iniciales deberá emitir una resolución motivada que, si detecta indicios de abuso, los ponga en conocimiento del ministerio fiscal para el ejercicio de las acciones penales que correspondan. Este diseño equilibra la urgencia de la protección con la necesidad de evitar instrumentalizaciones.

Propuesta 6. *Responsabilidad penal de los dirigentes algorítmicos: la multa administrativa, por alta que sea, es internalizada por las grandes empresas como un coste operativo. La única forma de cambiar la conducta de los directivos es introducir tipos penales para quienes, a sabiendas, diseñen o permitan tratamientos sistemáticamente ilegales que afecten a más de 10.000 personas. Propongo penas de prisión de 2 a 6 años e inhabilitación para ejercer cargos directivos. No es una idea cómoda; pero la historia del derecho muestra que solo la amenaza penal efectiva ha logrado modificar conductas arraigadas en el mundo empresarial (piénsese en el derecho ambiental o en la lucha contra la corrupción) (Tiedemann, 2018).*

Propuesta 7. *Auditoría de algoritmos ciudadana (AAC): todo ciudadano afectado por una decisión algorítmica relevante (crédito, empleo, diagnóstico médico) debe poder solicitar a la autoridad de control una auditoría técnica independiente del algoritmo. El responsable está obligado a poner el modelo (código fuente o entorno de pruebas equivalentes) a disposición de un auditor designado por la autoridad, bajo confidencialidad. Si la auditoría revela discriminación o violación de datos, la autoridad puede ordenar el reentrenamiento o suspensión del algoritmo. Es el equivalente a la prueba pericial, pero para cajas negras (Barocas, Hardt & Narayanan, 2017; Wachter, Mittelstadt & Russell, 2018).*

Conviene distinguir esta auditoría ciudadana del llamado "derecho a la explicación" individualizada que algunos autores deducen del considerando 71 del RGPD (Wachter et al, 2018). Mientras que la explicación se refiere a que un afectado conozca, en lenguaje comprensible, por qué un algoritmo tomó una decisión concreta que le afecta (v. gr., denegación de un crédito), la auditoría ciudadana aquí propuesta tiene un alcance colectivo y estructural: busca detectar sesgos sistémicos que puedan afectar a miles o millones de personas. Ambos derechos son complementarios y deberían coexistir en una legislación moderna. Por ello, añado como corolario de esta propuesta que toda ley de protección de datos debería consagrar explícitamente el derecho del interesado a recibir, previa solicitud, una explicación significativa de la lógica del algoritmo, de su funcionamiento y de los factores determinantes de la decisión, sin que el responsable pueda excusarse en la complejidad técnica o en el secreto empresarial para denegarla.

Propuesta 8. *Fondo de resarcimiento colectivo transfronterizo: Cuando una violación masiva afecta a ciudadanos de múltiples países y el responsable se encuentra en una jurisdicción no cooperante, se activa un fondo financiero internacional nutrido por una tasa del 0,1% sobre los ingresos globales de las grandes empresas tecnológicas (facturación mundial superior a 1.000 millones de euros). Una Comisión Internacional de Reclamaciones, compuesta por representantes de autoridades de control, puede conceder indemnizaciones a tanto alzado a los afectados. Este fondo no sustituye a la acción judicial, sino que opera como último recurso cuando todas las vías ordinarias han fracasado.*

Propuesta 9. *(complementaria) -- Datos sintéticos como alternativa estructural: una de las líneas de innovación más prometedoras para la protección de datos es la generación de datos sintéticos: conjuntos de datos artificiales que mantienen las propiedades estadísticas y las correlaciones de los datos reales, pero que no corresponden a ninguna persona física identificable. Cuando la técnica madure, podría resolver numerosos problemas estructurales: las transferencias internacionales de datos podrían realizarse con datos sintéticos sin necesidad de decisiones de ade-*

cuación o SCC; los entrenamientos de inteligencia artificial podrían prescindir de datos personales sensibles; la investigación médica podría compartir patrones epidemiológicos sin exponer historiales clínicos reales. Propongo que el Laboratorio.

Normativo Tecnológico-Cívico (sección 9.3) priorice el desarrollo de estándares internacionales para la certificación de datos sintéticos, definiendo umbrales de calidad estadística y niveles de privacidad diferencial. Si dentro de diez años la tecnología ha demostrado su fiabilidad, podríamos estar ante un cambio de paradigma: pasar de un derecho de protección reactivo (control sobre datos reales) a un derecho de anonimización proactiva (obligación de usar datos sintéticos siempre que sea técnicamente factible y no se sacrifican fines legítimos). Se advierte, no obstante, que hoy los datos sintéticos no sustituyen completamente a los reales para ciertos fines (como la identificación única o la trazabilidad forense), por lo que esta propuesta es de horizonte medio (5-10 años) y debe ir acompañada de investigación continua y auditorías independientes.

Propuesta integradora: un marco pragmático plurilateral y escalonado para la tutela global.

Las ocho propuestas precedentes, por audaces que sean, exigen un diseño institucional que combine universalismo normativo con realismo político. No se trata de soñar con un derecho global uniforme, sino de construir un núcleo mínimo de cooperación que pueda crecer por imitación y efecto de mercado, sin depender de la unanimidad de los Estados. Propongo un esquema plurilateral, escalonado y tecnológicamente operable, articulado en tres niveles complementarios.

Núcleo mínimo interpartes: la Plataforma de Mínimos

El primer nivel corresponde a una Plataforma de Mínimos interpartes, que se constituiría mediante un acuerdo político-jurídico entre un bloque inicial de jurisdicciones afines: Unión Europea, Estados miembros del Consejo de Europa adherentes al Convenio en su versión modernizada, países de América Latina con legislaciones avanzadas en protección de datos, Canadá y, en su caso, coaliciones africanas o asiáticas con estándares mínimos compatibles (Greenleaf, 2021; CEJA, 2020). Esta coalición no aspiraría a ser universal, sino a generar un núcleo duro de normas ius cogens aplicables a los flujos de datos entre sus miembros (ICJ, Barcelona Traction, 1970).

Los estándares que integrarían este núcleo incluirían, al menos: el reconocimiento expreso del derecho a la protección de datos personales como derecho fundamental autónomo; la garantía de un recurso efectivo transfronterizo (adminis-

trativo y judicial) accesible sin abogado para el interesado; la obligación de transparencia algorítmica mínima en decisiones automatizadas con impacto relevante; la instauración de medidas de protección de emergencia ex ante (botón de pánico digital adaptado); y la adopción de un sistema de presunciones reputacionales vinculado a sellos de confianza digital, que puedan ser retirados por incumplimiento.

El valor añadido de este núcleo no es solo normativo, sino económico-reputacional: las empresas que operen en esa esfera se verán obligadas a alinearse con un estándar de facto, bajo la amenaza coyuntural de perder acceso a mercados estratégicos o a infraestructuras digitales esenciales (tiendas de aplicaciones, pasarelas de pago, plataformas de anuncios). Así, el modelo deja de ser exclusivamente "top-down" y se refuerza por la lógica de red típica de la economía digital.

Mecanismo de cooperación judicial y administrativa reforzada: el Puente Procedimental

El segundo nivel se corresponde con un Puente Procedimental, órgano técnico-jurídico de cooperación entre autoridades de control y tribunales de los Estados miembros. Su función central sería la de acelerar la efectividad de las resoluciones transfronterizas sin depender de la buena voluntad discrecional de los Estados. Su mandato podría articularse en tres ejes: Órdenes multilaterales de asistencia: decididas por un panel de coordinación, que permitan a una autoridad de control de un Estado miembro solicitar preservación de datos, bloqueo temporal de transferencias, o suspensión de tratamientos en jurisdicciones asociadas, con plazos estrictos de ejecución (p. ej., 30 días para la adopción de medidas provisionales). Procedimiento acelerado frente a la vigilancia extranjera: cuando el tratamiento involucre a agencias de inteligencia de terceros países, el Puente Procedimental podría activar un panel de revisión independiente (jueces y técnicos) que evalúe la proporcionalidad y la legalidad de las solicitudes, sin necesidad de recurrir exclusivamente a tribunales nacionales cerrados al debate público (TEDH, Big Brother Watch, 2021).

Presunciones y carga de la prueba ajustada: a nivel procedimental, el sistema podría incorporar la idea ya esbozada en la OMED: la presunción de veracidad de los hechos alegados por el interesado cuando el responsable no comparece sin justa causa, así como la posibilidad de que la autoridad de control imponga sanciones reputacionales (pérdida de sello de confianza, bloqueo parcial de servicios) cuando persista el incumplimiento. Este Puente Procedimental no pretende reemplazar los sistemas nacionales, sino actuar como un sistema de refuerzo que, en la práctica, se convierta en el camino de referencia para la resolución de conflictos

transfronterizos de alta complejidad. La experiencia de la cooperación en materia de protección de datos dentro de la UE muestra que la mejora de mecanismos administrativos es insuficiente si no se acompaña de vías de ejecución rápida y de incentivos reputacionales claros (Bradford, 2020).

Laboratorio normativo tecnológico-cívico: la innovación regulatoria

El tercer nivel responde a la preocupación por la obsolescencia tecnológica de las normas. Se trata de conformar un Laboratorio Normativo Tecnológico-Cívico, compuesto por una comisión técnica independiente con representantes de autoridades de control, academia, sociedad civil, ingenieros de privacidad y seguridad, y periodistas. Su mandato no sería crear nuevo derecho interno, sino alimentar la Cláusula de Revisión Tecnológica Automática (CIRTA), actualizando semestralmente los anexos técnicos sobre identificadores, técnicas de vigilancia prohibida y criterios para la evaluación de riesgos; diseñar y supervisar proyectos piloto de normas experimentales (por ejemplo, la Licencia Digital Universal, el agente de IA personal, el botón de pánico digital o los mecanismos de auditoría ciudadana de algoritmos) bajo esquemas de "regulación sand-box" con límites de tiempo y evaluación pública (Barocas, et al, 2017).

El laboratorio debería publicar informes periódicos sobre métricas de impacto (número de quejas resueltas, tiempo medio de respuesta, incidencia de violaciones en grupos vulnerables, efectos sobre la confianza ciudadana), sirviendo como base empírica para la escalada de esas soluciones desde el marco experimental al núcleo mínimo. Así, el derecho dejaría de ser meramente reactivo y se transformaría en un instrumento de anticipación normativa, guiado por datos y pruebas piloto, no solo por declaraciones políticas.

Mecanismos de cumplimiento frente a jurisdicciones no cooperantes

Ninguna arquitectura global puede ser viable si no se plantea la pregunta incómoda: ¿y si el responsable está en una jurisdicción sin garantías o claramente no cooperante? Aquí conviene combinar presunciones reputacionales, medidas de mercado y sanciones económicas. En primer lugar, el pasaporte de conformidad interoperable podría convertirse en un requisito de acceso a determinados mercados: una plataforma domiciliada en un tercer país no cooperante solo podría operar en los Estados miembros si demuestra, por auditoría externa o sellos reconocidos, que cumple el núcleo mínimo. La denegación de ese pasaporte podría traducirse en bloqueos de acceso por parte de intermediarios clave (operadores de pago, plataformas de distribución, redes de anuncios), con base en acuerdos contractuales previos entre estos y las autoridades.

En segundo lugar, se podría prever una tasa selectiva sobre transacciones digitales realizadas por empresas domiciliadas en jurisdicciones no cooperantes, cuyo producto financie el fondo de resarcimiento colectivo transfronterizo. Esta tasa no sería una multa, sino una contraprestación económica por la externalidad negativa que genera la falta de cooperación, y estaría sujeta a revisión periódica si el Estado en cuestión se incorpora al núcleo mínimo o modifica su régimen de vigilancia. En tercer lugar, cabría desarrollar paneles de arbitraje vinculantes para empresas, financiados por ese mismo fondo, que permitan a los interesados acceder a decisiones económicas rápidas sin necesidad de someterse a la jurisdicción de origen del gigante.

Garantías procesales y equilibrio con otros derechos fundamentales

Cualquier arquitectura tan ambiciosa suscita la crítica legítima de que, en aras de la eficacia, se debiliten otras libertades. Por ello, es imprescindible incorporar, desde el diseño, un test de proporcionalidad multimodal aplicable a la intervención estatal y a la interferencia algorítmica. Este test exigiría, en toda medida que limite la protección de datos o la libertad de expresión, que las autoridades demuestren: la necesidad de la intervención frente a un fin legítimo (seguridad nacional, prevención del delito, protección de menores, etc.); la idoneidad de los medios elegidos (sin recurrir a técnicas de vigilancia masiva cuando existan alternativas menos intrusivas) (TEDH, Big Brother Watch, 2021); la subsidiariedad (la medida debe ser la menos intrusiva posible); y la revisión independiente por parte del Puente Procedimental o de tribunales especializados. Además, el sistema debe salvaguardar la libertad de prensa y de investigación periodística, permitiendo ciertos usos de datos personales cuando se orienten a la revelación de injusticias, abusos o violaciones sistémicas de derechos humanos, siempre que se cumpla un criterio de proporcionalidad estricta y con supervisión judicial.

La protección de datos personales no debe leerse como una categoría exclusivamente europea. Su desarrollo en América Latina (Brasil con la LGPD, Argentina, Colombia, México), Sudáfrica (POPIA), India, Corea del Sur o Japón muestra que el estándar se está globalizando no solo como regla de mercado, sino como pilar de la democracia digital (Greenleaf, 2021; CEJA, 2020). La “protección de datos del Sur Global” exige no solo la transferencia de modelos europeos, sino la incorporación de su experiencia jurídica y de derechos humanos a la arquitectura de la Plataforma de Mínimos.

Viabilidad política y hoja de ruta escalonada

*L*a viabilidad de este esquema no debe medirse desde la perspectiva de la perfección, sino desde la de la prueba progresiva. Podría plantearse una hoja de ruta en tres fases:

Fase 1 (24 meses): *conformación de la coalición fundadora, adopción del Núcleo mínimo interpartes, diseño de la CIRTA y puesta en marcha de pilotos tecnológicos (Licencia Digital Universal, botón de pánico, agentes personales) en dos o tres jurisdicciones piloto con evaluación pública de impacto.*

Fase 2 (36--60 meses): *entrada en funcionamiento del Puente Procedimental, creación operativa del fondo de resarcimiento colectivo transfronterizo y generalización de mecanismos de auditoría ciudadana de algoritmos.*

Fase 3 (5--8 años): *expansión plurilateral del núcleo, integración progresiva de Estados no fundadores y negociación de un marco similar a un Tratado de La Haya sobre Protección de Datos, con cláusulas de adhesión, mecanismos de revisión y procedimientos de denuncia graduados. Es preciso reconocer que este diseño, por ambicioso que sea, se enfrenta a limitaciones políticas profundas: la resistencia de Estados de seguridad intensiva (por ejemplo, ciertos regímenes de inteligencia en EE. UU., China o Rusia), la inercia de la diplomacia tradicional y la presión de grandes plataformas que se benefician de la fragmentación normativa. La Plataforma de Mínimos no resolverá automáticamente estas tensiones, pero sí puede crear un núcleo de presión institucional y reputacional capaz de empujar, paso a paso, hacia un estándar global mínimo de protección.*

Indicadores de éxito y cierre de esta etapa

Para que el debate no se quede en el plano de la teoría, conviene fijar indicadores de éxito concretos que permitan medir, a medio plazo, la eficacia de este esquema: reducción del tiempo medio de resolución transfronteriza a menos de 90 días, desde la presentación de la reclamación hasta la decisión ejecutiva.

Adopción de auditorías ciudadanas de algoritmos en al menos 10 jurisdicciones dentro de 4 años, con publicación obligatoria de informes técnicos.

Creación operativa del fondo de resarcimiento, con la condena de al menos una gran violación masiva en la que hayan fracasado todas las vías ordinarias, y liquidación efectiva de indemnizaciones a los afectados.

Incremento medible de la confianza ciudadana en los sistemas de protección de datos, según encuestas de percepción y uso de mecanismos de ejercicio de derechos (solicitud de acceso, oposición, portabilidad).

En síntesis, una refundación realista de la protección de datos en clave internacional no exige la utopía de un derecho global homogéneo ni la renuncia a la soberanía de los Estados. Demanda, eso sí, voluntad política, diseño institucional creativo y el coraje de convertir principios abstractos en mecanismos ejecutables, dotados de nervios económicos y de sanciones reputacionales. El camino hacia un constitucionalismo digital efectivo debe ser escalonado, tecnológicamente informado y, sobre todo, socialmente legitimado: impensable sin la participación de ciudadanos, ingenieros, periodistas y activistas. La protección de datos no es un problema de especialistas solitarios; es el campo de batalla donde se decide si la dignidad humana en la era digital será mera fórmula retórica o un derecho verdaderamente tutelado.

Conclusiones

Tras este recorrido, que no ha pretendido ser exhaustivo, sino riguroso y provocador, me permito extraer ocho conclusiones firmes:

- La protección de datos personales es un derecho fundamental autónomo, no un mero aspecto de la privacidad. Exige principios propios y mecanismos específicos.
- El sistema internacional actual es fragmentario, asimétrico e ineficaz para proteger a los ciudadanos frente a flujos globales de datos. El RGPD es un logro notable, pero no resuelve los problemas de ejecución transfronteriza.
- Las vías de recurso existentes funcionan razonablemente bien en contextos domésticos o europeos, pero se derrumban cuando el responsable está en una jurisdicción sin garantías o cuando se trata de agencias de inteligencia extranjeras.
- La cooperación administrativa entre autoridades de control ha mejorado, pero sigue siendo demasiado lenta y burocrática para la velocidad de los tratamientos de datos.
- Las reformas incrementales son necesarias pero insuficientes. Se requiere una combinación de audacia institucional (corte internacional, fondo de resarcimiento, responsabilidad penal) y empoderamiento tecnológico (licencia digital, agente personal, botón de pánico).
- La tecnología puede ser parte de la solución, no solo del problema. La identidad auto-soberana, el confidential computing, los contratos inteligentes y los

auditores algorítmicos ofrecen herramientas para un nuevo constitucionalismo digital.

- La comunidad internacional debería embarcarse en la negociación de un Tratado de La Haya sobre Protección de Datos, que no aspire a uniformar el mundo. Imposible, sino a establecer un mínimo común normativo y, sobre todo, un mecanismo de tutela judicial efectiva para todos los seres humanos, con independencia de dónde residan o dónde se almacenen sus datos.
- La protección de datos del siglo XXI no puede diseñarse desde los despachos de Bruselas o Washington exclusivamente. Debe ser co-construida con la ciudadanía, los ingenieros, los periodistas y los activistas. El derecho es una herramienta de libertad, no un manual de instrucciones para burócratas.

El derecho a controlar nuestros datos es el derecho a ser dueños de nuestra identidad. Y sin identidad propia, no hay democracia que valga. Hecha, pues, la anatomía del derecho, sus principios, sus fracturas, sus utopías, me queda solo por decir, que la protección de datos no es una materia para especialistas solitarios encerrados en bibliotecas. Es una cuestión de vida cotidiana: la madre que no quiere que rastreen los pasos de su hija menor, el trabajador que sospecha que un algoritmo decide su despido, el activista que sabe que su historial de búsquedas puede costarle la libertad en un país que no comparte sus convicciones.

Recuerdo las cartas de ciudadanos anónimos preguntando con miedo: "¿alguien puede hacer algo para que me dejen en paz?". Este ensayo es mi respuesta definitiva: sí, el derecho puede hacer algo, pero solo si tenemos el valor de reinventarlo. Las ocho propuestas que he esbozado no son recetas mágicas; son semillas. Algunas germinarán, otras morirán. Pero mi deber de jurista no es garantizar el éxito, sino no callarse ante la evidencia de que el sistema actual deja a millones de personas sin protección real frente a los flujos globales de datos. Cierro este escrito con la misma convicción con la que lo abrí: la dignidad humana en la era digital pasa por el control efectivo de nuestra información. Ni un solo byte menos. Que el debate comience, o, mejor dicho, que continúe, porque nunca debió detenerse.

Referencias

Allen, C. (2016). *The path to self-sovereign identity.* Life With Alacrity. https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Barocas, S., Hardt, M., & Narayanan, A. (2017). *Fairness and machine learning.* MIT Press. https://fairmlbook.org

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world.* Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Consejo de Europa. (1981). *Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.* https://www.coe.int/en/web/data-protection/convention108

Consejo de Europa. (2018). *Protocolo de enmienda al Convenio 108 (Convenio 108+).* https://www.coe.int/en/web/data-protection/convention108-plus

Corte Internacional de Justicia. (1962). *Certain Expenses of the United Nations (Article 17, paragraph 2, of the Charter). Advisory Opinion.* https://www.icj-cij.org/case/49

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report, 172,* 10–13. https://ssrn.com/abstract=3858974

Hardman, J. (2021). *Verifiable credentials: A guide to digital identity.* Medium. https://medium.com/@jameshardman/verifiable-credentials-a-guide-to-digital-identity-2021

Organización para la Cooperación y el Desarrollo Económicos. (1980/2013). *Guidelines on the protection of privacy and transborder flows of personal data.* https://www.oecd.org/sti/ieconomy/privacy

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* Harvard University Press. https://doi.org/10.4159/harvard.9780674736061

Relatora Especial de Naciones Unidas sobre el derecho a la privacidad. (2018). *Informe anual sobre la brecha global de privacidad.* Naciones Unidas. https://undocs.org/A/73/438

Schwartz, P. M. (1999). Privacy and democracy in cyberspace. *Vanderbilt Law Review, 52*(4), 1609–1701. https://doi.org/10.2139/ssrn.2096224

Tiedemann, K. (2014). Corporate criminal liability as a third track. In D. Brodowski, M. Espinoza de los Monteros de la Parra, & J. Vogel (Eds.), *Regulating corporate criminal liability* (pp. 11–18). Springer. https://doi.org/10.1007/978-3-319-05993-8_2

Tribunal de Justicia de la Unión Europea. (2011). *Asuntos acumulados C-70/10 y C-83/10.* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62010CJ0070

Tribunal de Justicia de la Unión Europea. (2014). *Asunto C-131/12, Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos.* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131

Tribunal de Justicia de la Unión Europea. (2020). *Asunto C-311/18, Data Protection Commissioner contra Facebook Ireland y Maximilian Schrems (Schrems II).* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62018CJ0311

Tribunal Europeo de Derechos Humanos. (2021). *Big Brother Watch and Others v. the United Kingdom.* https://hudoc.echr.coe.int/eng?i=001-210077

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology, 31*(2), 841–887. https://doi.org/10.2139/ssrn.3063289

Abreviaturas

AEPD. Agencia Española de Protección de Datos. **BCR.** Binding Corporate Rules (Normas Corporativas Vinculantes). **CEDH.** Convenio Europeo de Derechos Humanos. **CEPD.** Comité Europeo de Protección de Datos (EDPB). **CIRTA.** Cláusula de Revisión Tecnológica Automática (propuesta). **CNIL.** Commission Nationale de l'Informatique et des Libertés (Francia).

Convenio 108+. Convenio modernizado del Consejo de Europa *(El **Convenio 108+** es la denominación abreviada del Protocolo de Enmienda al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado por el Consejo de Europa en 2018 como actualización del histórico Convenio 108 de 1981. Constituye el **primer y único tratado internacional multilateral jurídicamente vinculante** en materia de protección de datos personales abierto a cualquier país del mundo, no solo a los miembros del Consejo de Europa. Su principal aportación fue modernizar los principios originales incorporando conceptos como la privacidad desde el diseño, la responsabilidad proactiva (accountability), la protección reforzada de datos genéticos y biométricos, el derecho a no ser objeto de decisiones automatizadas y un régimen actualizado para las transferencias internacionales de datos. Actualmente cuenta con 55 Estados parte en su versión original y 33 en la modernizada, sirviendo como referente para las decisiones de adecuación de la Comisión Europea y como puente normativo entre Europa, América Latina (Argentina, Uruguay, México) y otras regiones. El símbolo **"+"** forma parte de su denominación oficial y expresa precisamente esa vocación de mejora y actualización del convenio original).*

DPF. Data Privacy Framework (Marco UE-EE.UU.).

DPO. Data Protection Officer (Delegado de Protección de Datos).

LDU. Licencia Digital Universal (propuesta).

OMED. Oficina de Mediación en Protección de Datos (propuesta).

RGPD. Reglamento General de Protección de Datos (UE) 2016/679.

SCC. Standard Contractual Clauses (Cláusulas Contractuales Tipo).

TEDH. Tribunal Europeo de Derechos Humanos.

THPD. Tratado de La Haya sobre Protección de Datos (propuesta).

TIA. Transfer Impact Assessment (Evaluación de impacto de la transferencia).

TJUE. Tribunal de Justicia de la Unión Europea.