Rev. secr. Trib. perm. revis. 2026, Año 14, Nº 23, e573.
ISSN 2304-7887 (en línea) - ISSN 2307-5163 (impreso)
DOI: 10.16890/rstpr.a14.n23.e573
Artículo original/Artigo original/ Original article/Article original

El derecho de la integración como garante de los derechos humanos ante la irrupción de nuevas tecnologías

O direito da integração como garantidor dos direitos humanos perante a irrupção das novas tecnologias

Integration law as a guarantor of human rights in the face of the emergence of new technologies

Le droit de l'intégration comme garant des droits de l'homme face à l'émergence des nouvelles technologies

*Alfredo López Bravo**

Universidad de Buenos Aires, Facultad de Derecho. Buenos Aires, Argentina.

Resumen: La Unión Europea ha consolidado un rol de liderazgo sistémico en la regulación de las tecnologías emergentes, proyectando estándares normativos con vocación de universalidad. El presente artículo analiza el Derecho de la Integración como un dispositivo jurídico central para la tutela de los derechos humanos frente a los procesos de digitalización acelerada. A tal fin, se examinan tres pilares normativos del modelo europeo: el Reglamento General de Protección de Datos (GDPR), la Ley de Inteligencia Artificial (AI Act) y el Reglamento relativo a los mercados de criptoactivos (MICA). A partir del estudio de la jurisprudencia del Tribunal de Justicia de la Unión Europea y de la evolución de los regímenes de transferencia internacional de datos, se sostiene que la armonización supranacional permite enfrentar las asimetrías de poder propias del ecosistema digital, conciliando innovación

E-mail:alopezbravo@derecho.uba.ar

Recibido: 21/01/2026. Aceptado: 12/03/2026.

Editor responsable: Natasha Suñé . Secretaría del Tribunal Permanente de Revisión, Asunción, Paraguay.

tecnológica, seguridad jurídica y primacía de la dignidad humana. El trabajo concluye que el modelo europeo de integración se erige como un referente de constitucionalismo digital con impacto global.

Resumo: A União Europeia consolidou uma posição de liderança sistêmica na regulação das tecnologias emergentes, estabelecendo padrões normativos com vocação universal. O presente artigo analisa o Direito da Integração como um instrumento jurídico fundamental para a proteção dos direitos humanos diante dos processos acelerados de digitalização. Nesse contexto, são examinados três eixos normativos centrais do modelo europeu: o Regulamento Geral de Proteção de Dados (GDPR), a Lei de Inteligência Artificial (AI Act) e o Regulamento dos Mercados de Criptoativos (MICA). A partir da análise da jurisprudência do Tribunal de Justiça da União Europeia e da evolução dos regimes de transferência internacional de dados, sustenta-se que a harmonização supranacional permite enfrentar as assimetrias de poder do ambiente digital, conciliando inovação tecnológica, segurança jurídica e centralidade da dignidade humana. Conclui-se que o modelo europeu de integração configura um paradigma de constitucionalismo digital com projeção global.

Abstract: The European Union has consolidated a position of systemic leadership in the regulation of emerging technologies, establishing normative standards with global reach. This article examines Integration Law as a central legal framework for the protection of human rights in the context of accelerated digitalization. It focuses on three core regulatory pillars of the European model: the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AI Act), and the Markets in Crypto-Assets Regulation (MICA). Through the analysis of the case law of the Court of Justice of the European Union and the evolution of international data transfer regimes, the article argues that supranational harmonization provides an effective response to the power asymmetries inherent in the digital ecosystem, balancing technological innovation, legal certainty, and the primacy of human dignity. The study concludes that the European integration model represents a leading example of digital constitutionalism with global influence.

Résumé: L'Union européenne a affirmé un rôle de leadership systémique dans la régulation des technologies émergentes, en établissant des normes juridiques à vocation universelle. Le présent article analyse le droit de l'intégration comme un instrument central de protection des droits de l'homme face aux processus accélérés de numérisation. À cette fin, trois piliers normatifs du modèle européen sont examinés : le Règlement général sur la protection des données (RGPD), la loi sur l'intelligence artificielle (AI Act) et le règlement relatif aux marchés de crypto-actifs (MICA). À travers l'étude de la jurisprudence de la Cour de justice de l'Union européenne et de

l'évolution des régimes de transfert international de données, il est soutenu que l'harmonisation supranationale permet de répondre aux asymétries de pouvoir propres à l'environnement numérique, en conciliant innovation technologique, sécurité juridique et primauté de la dignité humaine. L'article conclut que le modèle européen d'intégration constitue une référence majeure du constitutionnalisme numérique à portée globale.

Palabras clave: Derecho de la integración, Derechos Humanos, Nuevas tecnologías, Efecto Bruselas.

Palavras-chave: Direito da integração, Direitos Humanos, Novas tecnologias, Efeito Bruxelas.

Keywords: Integration law, Human Rights, Emerging technologies, Brussels Effect.

Mots-clés: Droit de l'intégration, Droits de l'homme, Nouvelles technologies, Effet Bruxelles.

1. INTRODUCCIÓN

En el actual ecosistema global, signado por una disrupción tecnológica de alcance inédito, la Unión Europea (UE) ha consolidado un paradigma regulatorio que excede largamente la mera estructuración del mercado interior para erigirse como un auténtico modelo de gobernanza digital basado en valores. Este fenómeno, identificado por la doctrina como el denominado "efecto Bruselas"

Bradford[1], pone de manifiesto la capacidad del derecho de la integración europea para proyectar su fuerza normativa más allá de sus fronteras geográficas, estableciendo estándares globales de tutela de los derechos humanos en el marco de los desafíos que proponen las nuevas tecnologías.

En este contexto de transformación digital acelerada, el derecho de la integración europeo no se limita a operar como un instrumento de facilitación comercial, sino que se configura como un dispositivo central de gobernanza destinado a la protección efectiva de los derechos fundamentales. Tal como lo define Ricardo Basaldúa, esta rama jurídica regula el conjunto de acciones orientadas a la reducción o eliminación de las discriminaciones económicas entre los Estados comprometidos en un proceso de unificación progresiva[2].

1 BRADFORD, Anu. Define el *Brussels Effect* como el fenómeno mediante el cual la Unión Europea, a partir de su poder regulatorio y de mercado, externaliza unilateralmente sus normas internas, convirtiéndolas de facto en estándares globales, aun sin recurrir a mecanismos formales de cooperación internacional. "The Brussels Effect", Northwestern University Law Review, vol. 107, n.º 1, 2012, pp. 1–67, esp. p. 2..

2 BASALDÚA, Ricardo Xavier. Derecho de la Integración. Buenos Aires: Abeledo Perrot, 2023, p. 49

Esta nota distintiva resulta particularmente relevante en materia de nuevas tecnologías, en tanto la integración procura construir un "nuevo ámbito económico" que trascienda la fragmentación de los espacios nacionales, frente a la insuficiencia estructural de las regulaciones estatales individuales para abordar fenómenos de alcance global como los propios del entorno digital.

Desde una perspectiva complementaria, Sandra Negro introduce un elemento diferenciador fundamental al destacar la singularidad de los procesos de integración frente a los esquemas clásicos de cooperación internacional. Mientras que las organizaciones internacionales tradicionales se estructuran, en general, sobre mecanismos de cooperación intergubernamental, en los procesos de integración se verifica —o al menos se tiende a verificar— una transferencia de competencias hacia instituciones dotadas de autonomía propia[3]. Esta cesión de soberanía constituye el presupuesto de la supranacionalidad, rasgo indispensable para que bloques como la Unión Europea puedan dictar normas de aplicación inmediata y efecto directo, tales como el Reglamento General de Protección de Datos (GDPR por su sigla en inglés), la regulacion europea de Criptoactivos (MICA por su denominación en inglés) o la Ley de Inteligencia Artificial (*AI Act* por su referencia en inglés), garantizando así una regulación uniforme que no quede supeditada a los tiempos, muchas veces dilatados, de los procesos de incorporación al derecho interno.

En esta misma línea, se subraya que el Derecho de la Integración se aparta deliberadamente de la concepción "conservadora" del Derecho Internacional Público clásico, orientada primordialmente a la preservación de la integridad territorial y del status quo estatal. Por el contrario, el derecho de la integración persigue la creación de nuevos órdenes jurídicos en espacios ampliados, a partir de la reasignación de competencias previamente concentradas en los Estados nacionales[4]. Esta autonomía normativa es la que habilita a los bloques regionales a desempeñar un rol protagónico en el emergente constitucionalismo o soberanía digital", asegurando que los procesos de innovación tecnológica se encuentren subordinados al estado de derecho, y no a la inversa.

Sobre estas bases, el presente artículo examina la arquitectura jurídica de la Unión Europea a partir de tres ejes estructurantes: el régimen de protección de datos personales, la regulación pionera de la inteligencia artificial y la conformación del mercado de criptoactivos. Se sostiene como hipótesis central que la integración regional europea, al dotar al bloque de una capacidad regulatoria unificada, permite enfrentar las profundas asimetrías de poder existentes entre los grandes actores tecnológicos y los ciudadanos, asegurando la primacía de un entramado normativo orientado

3 NEGRO, Sandra C., Derecho de la Integración. Manual, 2.ª ed. revisada, ampliada y actualizada, Buenos Aires, BdeF Editores, 2013, pp. 42 – 45.

4 BASALDÚA, Ricardo Xavier. *Op. cit.*, pp. 27–29

a la tutela efectiva de los derechos humanos y al ejercicio —efectivo o al menos pretendido— de mecanismos de control sobre las nuevas dimensiones virtuales que se han consolidado en el entorno digital.

2. LA PROTECCIÓN DE DATOS PERSONALES COMO DERECHO FUNDAMENTAL

2.1. Ontología y alcance del dato personal en la era del Big Data

En el marco del constitucionalismo o soberanía digital, el dato personal no puede ser concebido meramente como un insumo económico ni como un recurso transable dentro de los mercados digitales, sino como una proyección directa de la personalidad jurídica y de la dignidad humana. Esta concepción axiológica se encuentra en la base del modelo europeo de protección de datos y explica su configuración como derecho fundamental autónomo, reconocido explícitamente en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea[5].

Desde una perspectiva normativa, el dato personal comprende toda información relativa a una persona física identificada o identificable[6], ya sea de manera directa o indirecta. Sin embargo, la emergencia de tecnologías de procesamiento masivo de información —big data, machine learning e inteligencia artificial— ha ampliado de forma exponencial el alcance material de esta noción. Elementos que tradicionalmente se consideraban neutros o carentes de relevancia jurídica, tales como metadatos, direcciones IP dinámicas, identificadores en línea, historiales de navegación o patrones de comportamiento digital, adquieren hoy una capacidad inédita de reidentificación, correlación y perfilamiento.

Este fenómeno erosiona las fronteras clásicas entre datos personales y no personales, y pone en crisis los enfoques regulatorios basados exclusivamente en la intención declarada del responsable del tratamiento. En efecto, el poder predictivo de los algoritmos permite inferir atributos sensibles —como orientación política, estado de salud o preferencias ideológicas— a partir de datos aparentemente inocuos, lo que genera un riesgo estructural para la autodeterminación informativa, entendida como la facultad de la persona de controlar la circulación y el uso de su información personal[7].

5 UNIÓN EUROPEA. El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconoce expresamente el derecho fundamental a la protección de datos personales, al disponer que “toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan”, estableciendo que dichos datos deben ser tratados “de manera leal, para fines concretos y sobre la base del consentimiento de la persona afectada o de otro fundamento legítimo previsto por la ley”, y garantizando, asimismo, el derecho de acceso y rectificación, así como el control por parte de una autoridad independiente.

6 Esta capacidad de reidentificación se fundamenta en las denominadas "Tres V" del Big Data: el masivo Volumen de información, la Velocidad de procesamiento y la Variedad de fuentes. Esta convergencia permite que datos a priori inconexos (v.gr. código postal, género y fecha de nacimiento) dejen de ser anónimos al ser procesados conjuntamente.

7 Como ejercicio ilustrativo, se invita al lector a confrontar estas inferencias accediendo al Centro de Anuncios de Google (myadcenter.google.com). En la sección "Administrar

En este contexto, la protección de datos se configura no solo como una garantía de privacidad, sino como un instrumento de equilibrio frente a las asimetrías informacionales propias del ecosistema digital, donde los grandes actores tecnológicos concentran capacidades técnicas y económicas muy superiores a las de los individuos.

2.2. El Reglamento General de Protección de Datos

El Reglamento (UE) 2016/679, conocido como Reglamento General de Protección de Datos (GDPR por su sigla en inglés), constituye uno de los desarrollos normativos más acabados del derecho de la integración europeo. Su adopción como reglamento —y no como directiva[8]— implica su aplicación directa y uniforme en todos los Estados miembros, sin necesidad de transposición, lo que refuerza la coherencia del ordenamiento jurídico europeo y materializa los principios de primacía y efecto directo. La opción por la técnica del reglamento, en lugar de la directiva, implicó un cambio cualitativo en el modelo de protección de datos de la Unión Europea, al establecer normas de aplicación directa, uniforme y obligatoria en todo el territorio del bloque, reforzando así los principios de primacía y efecto directo propios del ámbito comunitario europeo.

Desde el punto de vista sustantivo, el GDPR se estructura sobre un conjunto de principios rectores —licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad— que operan como verdaderos criterios constitucionales del tratamiento de datos. Estos principios no solo orientan la actuación de los responsables y encargados del tratamiento, sino que funcionan como parámetros de control para las autoridades administrativas y jurisdiccionales.

La fortaleza del sistema se manifiesta asimismo en un régimen sancionatorio de carácter disuasorio, con multas que pueden alcanzar hasta el 4 % del volumen de negocios anual global de la entidad infractora o veinte millones de euros, lo que refuerza la eficacia normativa del reglamento incluso frente a corporaciones transnacionales[9].

---

privacidad", es posible visualizar los atributos (nivel de ingresos, educación, intereses ideológicos) que el algoritmo ha deducido sobre su perfil a partir de su actividad digital.

8 El Reglamento (UE) 2016/679 sustituyó y derogó a la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la cual requería transposición al derecho interno de los Estados miembros.

9 La solidez del régimen sancionatorio del GDPR se evidencia en la multa impuesta por la Comisión de Protección de Datos de Irlanda a Meta (Facebook) por infringir la normativa europea de protección de datos, ascendiendo a 1.200 millones de euros, la mayor sanción registrada hasta ese momento por violaciones del GDPR en el espacio comunitario.Véase Infobae, "Irlanda multa a Meta con 1.200 millones de euros por infringir la normativa de privacidad de datos", 22 de mayo de 2023, [en línea] Disponible en: https://www.infobae.com/america/agencias/2023/05/22/irlanda-multa-a-meta-con-1200-millones-euros-por-infringir-normativa-de-privacidad-datos/

No obstante, uno de los aportes más significativos del GDPR reside en la reconceptualización del consentimiento como base jurídica del tratamiento de los datos. Este debe ser libre, específico, informado e inequívoco, quedando excluidas las prácticas de aceptación tácita o presunta.

La jurisprudencia del Tribunal de Justicia de la Unión Europea ha consolidado esta exigencia, como se observa en el caso Planet49[10], donde se declaró la invalidez de las casillas premarcadas como forma válida de consentimiento. Asimismo, la consagración del denominado "derecho al olvido", a partir de la sentencia *Google Spain c. AEPD*[11], y el reconocimiento del derecho a no ser objeto de decisiones basadas exclusivamente en tratamientos automatizados, sin intervención humana significativa, configuran un bloque de garantías orientado a preservar la autonomía personal frente a lógicas algorítmicas opacas. En este sentido, el GDPR desplaza el eje desde la mera protección de la información hacia la protección integral de la persona en entornos digitales.

2.3. Transferencias Internacionales de datos y la soberanía de los datos: La Saga Schrems

La circulación transfronteriza de datos personales constituye uno de los puntos de mayor fricción entre la lógica global del mercado digital y la concepción europea de los derechos fundamentales. En un ecosistema caracterizado por flujos de información instantáneos y deslocalizados, el principio de libre circulación de datos se ve tensionado por la exigencia de garantizar que, aun fuera del Espacio Económico Europeo, los datos de los ciudadanos europeos gocen de un nivel de protección "esencialmente equivalente"[12] al asegurado por el derecho de la Unión.

En este contexto, el GDPR introduce una ruptura conceptual relevante al afirmar su vocación extraterritorial. En efecto, el artículo 3 del reglamento extiende su ámbito de aplicación no solo a los tratamientos realizados en el

10 TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (Gran Sala). Asunto C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV c. Planet49 GmbH,* sentencia de 1 de octubre de 2019, en la que se declaró que el consentimiento para el tratamiento de datos personales y el uso de cookies no es válido cuando se obtiene mediante casillas premarcadas, por no cumplir con los requisitos de consentimiento libre, específico, informado e inequívoco exigidos por el Derecho de la Unión.

11 TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (Gran Sala). Asunto C-131/12, *Google Spain SL y Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*, sentencia de 13 de mayo de 2014, en la que se reconoció el denominado "derecho al olvido", permitiendo a los interesados solicitar la desindexación de enlaces a información personal cuando esta sea inadecuada, no pertinente o excesiva en relación con el tiempo transcurrido y los fines del tratamiento.

12 El artículo 44 del Reglamento (UE) 2016/679 establece que toda transferencia de datos personales a un tercer país u organización internacional solo podrá realizarse si se cumplen las condiciones previstas en el propio Reglamento, "a fin de garantizar que el nivel de protección de las personas físicas asegurado por el presente Reglamento no se vea menoscabado". Este principio es desarrollado por los considerandos 101 y 104, que exigen que el ordenamiento del país tercero garantice un nivel de protección "esencialmente equivalente" al proporcionado por el derecho de la Unión.

territorio de la Unión, sino también a aquellos efectuados por responsables o encargados establecidos en terceros Estados, cuando el tratamiento se relacione con la oferta de bienes o servicios a personas que se encuentren en la Unión, o con el control de su comportamiento dentro de ella. De este modo, la protección de datos deja de depender exclusivamente del lugar de establecimiento del operador y pasa a vincularse con la protección de la persona como sujeto de derechos, con independencia de dónde se encuentren los servidores o los centros de decisión empresariales.

Este criterio se proyecta directamente sobre el régimen de transferencias internacionales previsto en los artículos 44 a 49 del GDPR, que configuran un sistema cerrado y jerarquizado de garantías. Toda transferencia de datos personales a un tercer país u organización internacional solo es lícita si se respeta el núcleo esencial de los derechos fundamentales reconocidos por la Carta de Derechos Fundamentales de la Unión Europea, ya sea mediante una decisión de adecuación de la Comisión, la utilización de garantías apropiadas —como cláusulas contractuales tipo— o, en supuestos excepcionales, a través de las derogaciones expresamente previstas por el propio reglamento.

Resulta particularmente relevante mencionar la evolución del régimen de transferencias internacionales de datos personales entre la Unión Europea y los Estados Unidos, proceso que se encuentra estrechamente ligado a la iniciativa individual de Max Schrems[13], entonces estudiante de Derecho de la Universidad de Viena y activista por la protección de la privacidad. A partir de sus impugnaciones ante las autoridades de control y los tribunales europeos, Schrems puso en evidencia las deficiencias estructurales de los mecanismos de adecuación adoptados por la Comisión Europea, dando lugar a una serie de pronunciamientos de alto impacto por parte del Tribunal de Justicia de la Unión Europea. Este itinerario normativo y jurisprudencial —que se extiende desde el régimen de Safe Harbor (2000), continúa con el Privacy Shield y desemboca en el actual EU–U.S. Data Privacy Framework (2023)[14]— ilustra con claridad la tensión estructural existente entre, por un lado, las exigencias de seguridad nacional y los programas de vigilancia masiva de terceros Estados, y por otro, el estándar europeo de protección de la privacidad, tutela judicial efectiva y control independiente.

En todos estos esquemas subyace un interrogante común y persistente: si el ordenamiento jurídico del país receptor garantiza un nivel de protección de los datos personales sustancialmente equivalente al exigido por el derecho de la UE. La respuesta negativa ofrecida reiteradamente por el Tribunal de

13 Véase la charla TED de SCHREMS, Max, "How Europe's data privacy laws could shape the future of the internet", 2019, en la que se expone las implicancias globales del régimen europeo de protección de datos y el impacto extraterritorial del GDPR sobre las prácticas de empresas tecnológicas y Estados terceros. Disponible en: https://www.youtube.com/watch?v=TSDHa3ydca4

14 Cabe aclarar que el análisis detallado de la evolución jurídica entre EEUU y la UE (desde el Safe Harbor de 2000 hasta el Data Privacy Framework de 2023) excede el acotado objeto de estudio de este trabajo.

Justicia en los casos Schrems I y Schrems II[15] no solo invalidó los mecanismos vigentes en cada oportunidad, sino que reafirmó la centralidad de los derechos fundamentales como límite infranqueable a la libre circulación internacional de datos, consolidando así una concepción robusta de la soberanía digital europea.

Este activismo judicial no solo reafirma el rol del Tribunal de Justicia como garante último de los derechos fundamentales en el proceso de integración, sino que consolida una concepción robusta de la soberanía digital europea, entendida no como una forma de aislamiento o proteccionismo tecnológico, sino como la capacidad del bloque regional de imponer condiciones normativas al flujo global de información. En este sentido, el GDPR opera como un instrumento de proyección normativa externa: empresas y Estados terceros se ven compelidos a adecuar sus prácticas internas si desean operar legítimamente en el mercado europeo.

La aplicación extraterritorial del reglamento y el control estricto de las transferencias internacionales convierten así a la protección de datos personales en un eje estructural del constitucionalismo digital europeo y en una manifestación concreta del denominado Brussels Effect. A través de este mecanismo, la Unión Europea logra externalizar sus estándares de tutela de derechos fundamentales, reafirmando que, incluso en un entorno digital globalizado, la innovación tecnológica debe permanecer subordinada al Estado de Derecho y a la centralidad de la persona humana

3. EL MARCO DE LOS MERCADOS DE CRIPTOACTIVOS (MICA)

El reglamento europeo conocido como Markets in Crypto-Assets Regulation (MICA por su sigla en inglés)[16], constituye la respuesta institucional de la UE a la profunda fragmentación normativa que caracterizaba al ecosistema de los criptoactivos. Hasta su adopción, el sector se encontraba regulado —cuando lo estaba— mediante soluciones nacionales dispares, generando incertidumbre jurídica, arbitraje regulatorio y riesgos sistémicos incompatibles con un mercado financiero integrado.

MICA se inscribe, así, en la lógica estructural del derecho de la integración: armonizar el mercado interior mediante normas de aplicación directa, garantizando simultáneamente la estabilidad financiera, la protección del inversor y la integridad del sistema económico digital. Al igual que el GDPR y la *AI Act*, el reglamento no se limita a ordenar el espacio europeo, sino que proyecta su influencia más allá de las fronteras del bloque, incidiendo de manera decisiva en la gobernanza global de los criptoactivos.

15 TRIBUNAL DE JUSTICIA DE LA UNION EUROPEA asuntos C-362/14 (Schrems I"), que invalidó el Safe Harbor, y C-311/18 (Schrems II) que hizo lo propio con el Privacy Shield,

16 UNIÓN EUROPEA. Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023. Entró en vigor el 29 de junio de 2023.

3.1. Taxonomía de criptoactivos y tutela del usuario

Uno de los aportes centrales de MICA es la introducción de una clasificación jurídica uniforme de los criptoactivos, que permite abandonar enfoques meramente tecnológicos o económicos y avanzar hacia una regulación basada en el riesgo y en la función que cada activo cumple en el mercado. El reglamento distingue, en particular, entre:

a) *Tokens* de dinero electrónico[17] (*Electronic Money Tokens*)[18]: criptoactivos, comúnmente conocidos como *stablecoins*, diseñados para mantener un valor estable mediante su vinculación a una única moneda fiduciaria. Estos instrumentos cumplen una función económica análoga al dinero electrónico tradicional; sin embargo, su naturaleza tecnológica y su potencial alcance sistémico justifican un régimen regulatorio más estricto. En particular, MICA exige controles reforzados sobre las entidades emisoras, incluyendo la auditoría periódica de sus reservas y tesorerías, con el objetivo de garantizar de manera efectiva la paridad entre el criptoactivo emitido y la moneda del mundo físico que lo respalda.
b) *Tokens* referenciados a activos[19] (*Asset-Referenced Tokens)*: activos digitales cuyo valor se encuentra respaldado por una cesta de monedas, materias primas u otros activos, lo que los convierte en instrumentos con potencial impacto sistémico.
c) *Utility tokens*[20]: criptoactivos concebidos principalmente para proporcionar acceso digital a un bien o servicio específico dentro de un ecosistema determinado.

Cabe destacar que la norma no pretende abarcar de manera indiscriminada la totalidad del universo cripto, sino que delimita de forma consciente y selectiva su ámbito de aplicación.

17 Un caso real es USD Coin (USDC), emitido por Circle Internet Financial.

18 MICA dedica una porción sustantiva de su articulado —aproximadamente un tercio del texto normativo— a la regulación de los *tokens* de dinero electrónico y de los *tokens* referenciados a activos, estableciendo requisitos estrictos en materia de autorización, reservas, gobernanza, auditoría y supervisión (v. en particular, Títulos III y IV). Esta densidad regulatoria puede ser interpretada como un paso preparatorio necesario para la eventual emisión de una moneda digital del Banco Central Europeo, en la medida en que crea un entorno normativo estable y confiable para instrumentos digitales con vocación de estabilidad, que podría servir de base jurídica y técnica para el futuro euro digital.

19 Un caso real es P*ax Gold (PAXG)* es un criptoactivo emitido por Paxos Trust Company cuyo valor se encuentra referenciado al precio del oro físico, estando cada token respaldado por una onza troy de oro custodiada en bóvedas certificadas.

20 Un caso real es E*ther (ETH)*, token nativo de la red Ethereum, cumple primordialmente la función de permitir el acceso y uso de servicios descentralizados —como la ejecución de contratos inteligentes y aplicaciones descentralizadas— dentro de un ecosistema digital específico.

En este sentido, quedan expresamente excluidos del perímetro regulatorio los denominados *security tokens*, los *tokens* no fungibles auténticamente únicos (*NFTs*) y los criptoactivos plenamente descentralizados sin emisor identificable, como *Bitcoin*.

Esta opción normativa no obedece a un vacío regulatorio, sino a una estrategia deliberada del legislador europeo: los security tokens continúan sujetos a los regímenes sobre activos financieros y del derecho de los mercados de capitales; los *NFT* genuinos permanecen, por ahora, fuera del alcance de MICA salvo que su estructura económica revele fungibilidad o finalidad financiera; y *Bitcoin*, en tanto infraestructura descentralizada, no es regulado como activo, aunque sí lo son los proveedores de servicios que facilitan su acceso al mercado europeo.

De este modo, MICA busca evitar episodios de colapso financiero como los registrados en el mercado cripto global, no mediante la prohibición generalizada de tecnologías emergentes, sino a través de un enfoque prudencial y funcional, centrado en los activos con vocación sistémica y en los intermediarios que operan como puntos de entrada al ecosistema.

3.2. El *"pasaporte europeo"* y la integración al mercado de criptoactivos

Otro de los pilares estructurales de MICA es la creación del estatuto jurídico de los Proveedores de Servicios de Criptoactivos (*Crypto-Asset Service Providers – CASPs*). A través de este mecanismo, una entidad que obtiene autorización en un Estado miembro puede prestar servicios en todo el territorio de la Unión, sin necesidad de licencias adicionales, en virtud del principio de reconocimiento mutuo.

Este sistema de "*pasaporte europeo*" reproduce una técnica clásica del derecho de la integración financiera, pero adaptada a la economía digital. A la vez, se combina con un robusto esquema de supervisión y cumplimiento, que refuerza las obligaciones en materia de *Know Your Customer* (*KYC*) y normas anti lavado de dinero La innovación tecnológica, así, no queda asociada a la opacidad ni a la desintermediación irresponsable, sino integrada en un marco de control institucional que preserva la legalidad y la trazabilidad de las operaciones.

3.3. Proyección extraterritorial y vocación de estándar global

Más allá de su impacto intracomunitario, MICA revela con claridad la vocación expansiva del modelo regulatorio europeo. En la medida en que el reglamento se aplica a todo emisor o proveedor de servicios que ofrezca criptoactivos o servicios vinculados a ellos en el mercado de la Unión, las plataformas y emisores establecidos fuera del territorio europeo se ven compelidos a adecuar sus estructuras globales para poder operar en uno de los mercados más relevantes del mundo.

Este fenómeno reproduce, en el ámbito financiero-digital, la lógica del denominado *Brussels Effec*t: la UE no impone formalmente su regulación al resto del mundo, pero la centralidad económica de su mercado convierte a sus normas en estándares de facto globales. En consecuencia, *exchanges*, emisores de *stablecoins* y proveedores tecnológicos extracomunitarios optan por alinear sus modelos de negocio con MICA para evitar la fragmentación de servicios, los sobrecostos regulatorios y la exclusión del mercado europeo.

Desde esta perspectiva, MICA no debe ser entendido únicamente como una regulación sectorial, sino como una herramienta de gobernanza económica global, que redefine los límites entre innovación financiera, soberanía regulatoria y protección de derechos de consumidores y usuarios.

La UE consolida así una estrategia coherente: utilizar el derecho de la integración como vehículo para proyectar valores —transparencia, estabilidad, protección del consumidor y control institucional— en un entorno tecnológico de alcance planetario.

4. LA LEY DE INTELIGENCIA ARTIFICIAL

Bajo el axioma de que el desarrollo tecnológico debe encontrarse necesariamente subordinado a la ética, al Estado de Derecho y al respeto de la dignidad humana, la Unión Europea ha adoptado el primer reglamento integral del mundo destinado a regular la inteligencia artificial. La denominada Ley de Inteligencia Artificial (AI Act por su denominación en inglés)[21] se erige así como un hito normativo sin precedentes, al abordar de manera sistemática los riesgos derivados del uso de sistemas algorítmicos avanzados en contextos sociales, económicos y estatales sensibles.

Este instrumento encuentra su fundamento jurídico en el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE)[22], relativo a la armonización del mercado interior, lo que evidencia —una vez más— la utilización del derecho de la integración como vehículo para la tutela de derechos fundamentales en entornos tecnológicos. La opción por la técnica del reglamento, de aplicación directa y obligatoria en todos los Estados miembros, responde a la necesidad de evitar fragmentaciones regulatorias que podrían socavar tanto la protección de los derechos como el funcionamiento eficiente del mercado digital europeo.

4.1. Arquitectura regulatoria basada en el riesgo

El eje estructural de la Ley de Inteligencia Artificial es la adopción de un enfoque basado en el riesgo, de carácter preventivo y proporcional,

21 UNIÓN EUROPEA. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, del 13 de junio de 2024, en vigor desde el 1 de agosto de 2024, con aplicación progresiva y plena efectividad prevista para agosto de 2027.

22 UNIÓN EUROPEA. Tratado de Funcionamiento de la Unión Europea, art. 114, que habilita al Parlamento Europeo y al Consejo a adoptar medidas de armonización de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que tengan por objeto el establecimiento y el funcionamiento del mercado interior.

que gradúa las obligaciones de los proveedores y usuarios de sistemas de IA en función impacto potencial de dichas tecnologías sobre los derechos fundamentales, la seguridad y los valores democráticos.

Este modelo rompe con enfoques tecnológicamente neutrales y reconoce que no todas las aplicaciones de IA generan los mismos riesgos sociales, lo que justifica un tratamiento jurídico diferenciado. En este sentido, la *AI Act* distingue cuatro categorías principales:

a) Riesgo inaceptable (sistemas prohibidos): Se prohíben de manera absoluta aquellos sistemas de IA que se consideran incompatibles con los valores fundamentales de la Unión. Entre ellos se incluyen las tecnologías de manipulación subliminal del comportamiento humano, los sistemas de puntuación social (*social scoring*) por parte de autoridades públicas y determinadas formas de vigilancia biométrica remota en tiempo real en espacios públicos. Estas prohibiciones reflejan una opción ética clara: existen usos de la tecnología que no pueden ser legitimados ni siquiera bajo argumentos de eficiencia o seguridad. La entrada en vigor de estas prohibiciones operó el 2 de febrero de 2025.
b) Riesgo alto: Comprende los sistemas de IA utilizados en ámbitos especialmente sensibles, como infraestructuras críticas, salud, transporte, educación, empleo y administración de justicia. Estas aplicaciones no son prohibidas, pero quedan sujetas a requisitos estrictos de gobernanza, entre los que se destacan la calidad y trazabilidad de los datos, la documentación técnica exhaustiva, la evaluación previa de riesgos, la supervisión humana efectiva y la posibilidad de auditorías. La aplicación plena de este régimen está prevista para el 2 de agosto de 2026, lo que evidencia una implementación progresiva y planificada.
c) Riesgo limitado y mínimo: Para los sistemas de menor impacto, la Ley de IA establece obligaciones fundamentalmente orientadas a la transparencia, como el deber de informar al usuario cuando interactúa con una IA o cuando el contenido ha sido generado artificialmente. En los supuestos de riesgo mínimo, el uso de IA permanece esencialmente libre, fomentando la innovación sin cargas regulatorias innecesarias.

Este esquema evidencia una lógica regulatoria sofisticada, que busca maximizar la protección de derechos sin sofocar el desarrollo tecnológico, consolidando un modelo europeo de innovación responsable.

4.2. Vocación de universalidad: la proyección extraterritorial de la norma

La Ley de Inteligencia Artificial no se limita a regular el mercado interior europeo, sino que expresa una clara vocación de universalidad que se articula a través de tres mecanismos principales.

En primer lugar, el denominado "*efecto Bruselas*"[23] al que se hiciera referencia al comienzo de este artículo. Al tratarse de un reglamento de aplicación directa que alcanza a cualquier empresa que pretenda comercializar o utilizar sistemas de IA en el mercado europeo, con independencia de su lugar de establecimiento, las grandes plataformas tecnológicas se ven compelidas a adaptar sus modelos globales a los estándares de la UE para evitar la fragmentación de servicios y costos regulatorios diferenciados.

En segundo término, la UE ejerce un liderazgo normativo en la gobernanza global de la IA, al establecer una definición jurídica de "sistema de inteligencia artificial" basada en criterios de autonomía, adaptabilidad y capacidad de inferencia (art. 3), que busca ser replicada por organismos internacionales y foros multilaterales, contribuyendo a la armonización conceptual y técnica a escala global.

Finalmente, la protección de los derechos fundamentales opera como una auténtica barrera normativa de acceso al mercado. Al prohibir determinadas aplicaciones por razones éticas y jurídicas, la UE envía un mensaje político inequívoco sobre los límites del uso legítimo de la tecnología. Este enfoque influye directamente en las legislaciones emergentes de otras regiones, que procuran alcanzar estándares de compatibilidad o "adecuación" para no quedar excluidas del ecosistema digital europeo.

En conjunto, la *AI act* consolida a la UE como un actor central del constitucionalismo digital global, demostrando que la regulación no constituye un freno a la innovación, sino una condición necesaria para su legitimidad democrática y su sostenibilidad a largo plazo.

5. CONCLUSIONES

La respuesta normativa de la UE frente a la acelerada eclosión tecnológica confirma que el derecho de la integración se ha consolidado como uno de los instrumentos más eficaces para la protección de los derechos humanos en el siglo XXI.

La armonización regional no solo optimiza el funcionamiento del mercado interior, sino que proyecta un auténtico modelo de constitucionalismo digital, en el cual el desarrollo algorítmico y tecnológico se encuentra estructuralmente subordinado al Estado de Derecho.

23 En su formulación originaria del concepto, la autora que introduce la noción —luego desarrollada de manera sistemática en una obra posterior de mayor alcance— sostiene que: "The Brussels Effect is the European Union's unilateral ability to regulate global markets." ("El denominado efecto Bruselas es la capacidad unilateral de la Unión Europea para regular los mercados globales", traducción propia). BRADFORD, Anu, op. cit., p. 2

En este marco, adquiere pleno sentido la conocida afirmación según la cual "*Estados Unidos crea, China copia y la Unión Europea legisla*". Lejos de constituir una caracterización peyorativa, esta popular expresión revela una vocación normativa vanguardista, orientada a ordenar jurídicamente terrenos aún inexplorados —verdaderas *terrae incognitae* del derecho— mediante un ejercicio consciente de regulación anticipatoria, aun asumiendo el riesgo de eventuales ajustes futuros. La propia Ley de Inteligencia Artificial refleja esta lógica evolutiva al prever instancias periódicas de revisión por parte del Parlamento y del Consejo, reconociendo explícitamente el carácter dinámico de la tecnología y la necesidad de evaluar la adecuación continua del marco normativo, aun cuando no se trate de una cláusula de caducidad en sentido estricto, pero recordándonos que siempre el derecho esta vivo.

Uno de los desafíos centrales que plantea la regulación de fenómenos tecnológicos de naturaleza inmaterial y altamente volátil consiste en evitar que el marco jurídico se convierta en un factor de desincentivo para la inversión y la innovación. En este sentido, la experiencia europea demuestra que una regulación clara y previsible no opera necesariamente como un *corset* restrictivo, sino que puede constituirse en un entorno fértil para el desarrollo de empresas tecnológicas, al ofrecer reglas estables, previsibilidad jurídica y condiciones de competencia leal, aun cuando simultáneamente introduzca barreras regulatorias de acceso orientadas a la protección del interés general.

En definitiva, la afirmación de la primacía de la dignidad humana, la seguridad jurídica y la tutela de los derechos fundamentales frente a la autonomía tecnológica pone de relieve que la integración regional emerge como un camino idóneo para que las sociedades democráticas conserven un control efectivo sobre su futuro digital. El modelo europeo se erige así como un referente global de gobernanza ética, capaz de influir y moldear los estándares regulatorios internacionales en un escenario tecnológico crecientemente interdependiente.

CONFLICTO DE INTERÉS

El autor declara que el manuscrito enviado para publicación en la revista no presenta conflicto de interés.

FINANCIAMIENTO

Se deja constancia que el artículo a publicar no cuenta con financiamiento institucional, es producto de la investigación en su expertise como docente universitario e investigador.

REFERENCIAS BIBLIOGRÁFICAS

BASALDÚA, Ricardo. *Derecho de la integración*. Buenos Aires: Abeledo Perrot, 2023.

BRADFORD, Anu. The Brussels Effect. *Northwestern University Law Review,* vol. 107, n.º 1, 2012, pp. 1–67.

BRADFORD, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020.

CIPPITANI, Roberto. "Mercosur y derechos humanos". En: CIPPITANI, Roberto (dir.). *Derechos humanos e integración regional*. Asunción: Secretaría del MERCOSUR – Instituto Social del MERCOSUR, 2011.

NEGRO, Sandra C. *Derecho de la integración*. Buenos Aires: B de F, 2013.

NEWSROUND INFOBAE. "Histórica multa a Meta por infringir privacidad de datos en Europa". *Infobae,* 22 de mayo 2023 [en línea]. Disponible en: https://www.infobae.com/america/agencias/2023/05/22/irlanda-multa-a-meta-con-1200-millones-euros-por-infringir-normativa-de-privacidad-datos/

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. *Asunto C-131/12, Google Spain SL y Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González.* Sentencia de 13 de mayo de 2014.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. *Asunto C-673/17, Planet49 GmbH*. Sentencia de 1 de octubre de 2019.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. *Asunto C-362/14, Maximillian Schrems c. Data Protection Commissioner (Schrems I)*. Sentencia de 6 de octubre de 2015.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. *Asunto C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd y Maximillian Schrems (Schrems II).* Sentencia de 16 de julio de 2020.

UNIÓN EUROPEA. *Carta de los Derechos Fundamentales de la Unión Europea.* Diario Oficial de la Unión Europea C 326, 26 de octubre de 2012.

UNIÓN EUROPEA. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016.

UNIÓN EUROPEA. Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MICA). Diario Oficial de la Unión Europea L 150, 9 de junio de 2023.

UNIÓN EUROPEA. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial). Diario Oficial de la Unión Europea L 1689, 12 de julio de 2024.

RESUMEN BIOGRÁFICO

Alfredo López Bravo. Profesor adjunto regular de grado de la Facultad de Derecho UBA. Máster por la Universidad de Palermo y postgraduado de la Facultad de Derecho de la UBA. Defensor Público de la Defensoría General de la Nación y miembro investigador del Centro Interdisciplinario de Estudios de Derecho Industrial y Económico (CEIDIE).
mail: alopezbravo@derecho.uba.ar
ORCID: https://orcid.org/0009-0009-9508-7666