La protección de datos a partir de la implementación de IA en *smart contracts*

Data Protection Through the Implementation of AI in Smart Contracts

Eduardo Andrés Calderón Marenco
https://orcid.org/0000-0002-7840-6495
Universidad Cooperativa de Colombia. Colombia
Correo electrónico: eduardo.calderon@campusucc.edu.c

Romina M. Sánchez Silveyra
https://orcid.org/0009-0007-1016-8623
Universidad de Concepción del Uruguay. Argentina
Correo electrónico: sanchez_romina@ucu.edu.ar

Juan Manuel Rodrigo
https://orcid.org/0009-0009-3936-7639
Poder Judicial de la Ciudad de Buenos Aires. Argentina
Correo electrónico: juanmarodrigo@hotmail.es

Gabriel Ravelo-Franco
https://orcid.org/0000-0003-0212-312X
Universidad Continental. Perú
Correo electrónico: gravelo@continental.edu.pe

Recepción: 18 de marzo de 2025
Aceptación: 2 de junio de 2025
Publicación: 1 de octubre de 2025

DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

Resumen: El artículo analiza el efecto de la inteligencia artificial en la contratación inteligente y la protección de datos personales y argumenta que la automatización mediante *smart contracts* plantea desafíos regulatorios, ante la falta de un marco normativo adecuado para garantizar la privacidad y la seguridad jurídica en Latinoamérica. A

través de un análisis comparado de los marcos normativos de Argentina, Perú, Colombia, Ecuador y la Unión Europea, se identifican avances y vacíos en la regulación de estas tecnologías, y se destaca que, aunque algunos países han reconocido la validez jurídica de los contratos inteligentes, la protección de los datos almacenados en *blockchains* sigue siendo un reto. Asimismo, se aborda el concepto de *lex criptográfica* como un sistema de autorregulación basado en la descentralización tecnológica, lo que genera tensiones con principios tradicionales del derecho. El artículo concluye que la creciente automatización contractual exige una actualización normativa que armonice la eficiencia tecnológica con la protección de los derechos fundamentales, y propone el desarrollo de un marco regulador que garantice la seguridad jurídica, la transparencia en el tratamiento de datos y la responsabilidad en la toma de decisiones automatizadas, conforme a los estándares internacionales y europeos de protección de datos.
Palabras clave: *smart contracts*; automatización contractual; protección de datos personales; regulación tecnológica; privacidad; *lex criptográfica*.

Abstract: The article analyzes the impact of artificial intelligence on smart contracting and personal data protection, arguing that automation through smart contracts poses regulatory challenges due to the lack of an adequate legal framework to ensure privacy and legal security in Latin America. Through a comparative analysis of the regulatory frameworks in Argentina, Peru, Colombia, Ecuador, and the European Union, advancements and gaps in the regulation of these technologies are identified, highlighting that, although some countries have recognized the legal validity of smart contracts, the protection of data stored on blockchains remains a challenge. Additionally, the concept of *lex criptográfica* is addressed as a self-regulation system based on technological decentralization, which creates tensions with traditional legal principles. The article concludes that the increasing contractual automation requires a regulatory update that balances technological efficiency with the protection of fundamental rights, proposing the development of a regulatory framework that ensures legal security, transparency in data processing, and accountability in automated decision-making, in line with international and European data protection standards.
Keywords: *smart contracts*; contract automation; personal data protection; technological regulation; privacy; *lex criptográfica*.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

I. Introducción

El avance tecnológico y la globalización del Internet han dado lugar a un ecosistema digital capaz de procesar millones de datos por segundo y generar una relación de creciente dependencia del ser humano hacia la tecnología. En este contexto, la Cuarta Revolución Industrial ha sido impulsada por la expansión de las capacidades de almacenamiento, la velocidad en el procesamiento de información y el desarrollo de nuevas herramientas digitales, lo que transforma múltiples ámbitos, incluido el derecho. La automatización, la seguridad y la eficiencia son factores determinantes en la interacción entre la inteligencia artificial y el mundo jurídico. Su impacto en la gestión judicial ha llevado a diversos juristas a explorar la posibilidad de extender su aplicación a la contratación, al revolucionar la forma en que se conciben, negocian y ejecutan los acuerdos jurídicos. Este planteamiento comenzó a materializarse en 1994, cuando el criptógrafo y jurista Nick Szabo acuñó el término *smart contracts*, lo que anticipó la necesidad de un estudio más profundo sobre estos instrumentos y su potencial transformación del derecho contractual.

A la par del desarrollo de los contratos inteligentes, la automatización de procesos y el uso de algoritmos de inteligencia artificial ha generado cuestionamientos sobre la suficiencia del marco regulatorio vigente para garantizar la seguridad jurídica, la protección de derechos fundamentales y la eficacia de los negocios jurídicos automatizados. En particular, es necesario analizar si los principios del derecho a la protección de datos personales, como la autodeterminación informativa, la confidencialidad y la proporcionalidad, se ven afectados por el procesamiento automatizado de información dentro de los contratos inteligentes.

El propósito de esta investigación es identificar los desafíos y oportunidades que plantea la inteligencia artificial en la regulación de la protección de datos personales dentro del ámbito contractual y establecer criterios que permitan armonizar su aplicación con los principios fundamentales del derecho a la privacidad. Para ello, se analizará la capacidad del marco normativo internacional actual para garantizar la privacidad y los derechos de los titulares de la información frente a la automatización del tratamiento de datos. Asimismo, se examinará la incidencia de los contratos inteligentes en la autonomía de la voluntad, a través de la observación de su compatibilidad con los requisitos de validez contractual y la necesidad de una regulación específica que asegure su reconocimiento jurídico.

El avance de la inteligencia artificial ha generado un debate sobre la capacidad del derecho para regular sus implicaciones en áreas fundamentales como la protección de datos personales y la contratación digital. Las norma-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

tivas tradicionales, diseñadas para un entorno en el que la intervención humana es determinante en la formación y ejecución de los negocios jurídicos, pueden no ser idóneas para enfrentar las dinámicas de los sistemas autónomos de decisión. En este sentido, el problema jurídico que se plantea es determinar si el derecho vigente dispone de herramientas normativas suficientes para regular el impacto de la inteligencia artificial en la privacidad y la autonomía contractual o si, por el contrario, es necesario desarrollar nuevos mecanismos legislativos que respondan a los desafíos que estas tecnologías presentan. A partir de este análisis, se formula la siguiente pregunta problema: ¿cómo incide el uso de la inteligencia artificial en los contratos inteligentes en relación con la protección de datos personales?

II. Metodología

La metodología utilizada en este artículo corresponde a una investigación teórica con un enfoque cualitativo, basada en el método de análisis-síntesis, el cual permitió descomponer el fenómeno estudiado en sus elementos esenciales para luego integrarlos en una visión unificada. En este estudio, el análisis se centró en la identificación de los desafíos y oportunidades que plantea la implementación de inteligencia artificial en *smart contracts*, particularmente en lo que respecta a la protección de datos personales y la regulación jurídica en diferentes jurisdicciones. Para su implementación, se llevó a cabo una fase analítica, donde se desglosaron los conceptos clave, como la automatización contractual, la descentralización tecnológica y la protección de datos en el ámbito digital. Esta fase incluyó la revisión detallada de marcos normativos en América Latina y la Unión Europea, y se identificaron similitudes y vacíos en la legislación aplicable.

Posteriormente, se realizó una fase de síntesis, en la que los hallazgos obtenidos fueron integrados para establecer relaciones entre la regulación existente y las necesidades emergentes de adaptación normativa. En esta etapa, se estudió cómo los principios tradicionales del derecho pueden armonizarse con el uso de inteligencia artificial en contratos inteligentes y cómo la regulación puede responder a los riesgos de la automatización en la toma de decisiones y el manejo de datos personales. Se empleó la recolección bibliográfica como técnica principal; para ello, se utilizaron palabras clave como inteligencia artificial, *smart contracts*, protección de datos personales, regulación tecnológica y *lex criptográfica*, para identificar fuentes relevantes en bases de datos académicas y documentos normativos.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

Como instrumento de análisis, se aplicó la ficha bibliográfica para la sistematización de la información obtenida de artículos científicos, marcos normativos y estudios comparados sobre la regulación de la inteligencia artificial y los contratos inteligentes en América Latina y Europa. Esta metodología permitió estructurar el estudio, a partir de la identificación de los principales desafíos jurídicos y regulatorios en la intersección entre la automatización contractual y la protección de datos personales.

III. Inteligencia artificial. Origen, clases y su repercusión en el derecho

Mucho se ha discutido acerca del nacimiento de la inteligencia artificial. La lucha por adjudicarse la creación y autoría de esta herramienta es algo que aún hoy en día, pasados unos veinticuatro años del siglo xxi, sigue en velo entre los distintos investigadores. Si bien algunos sostienen que para precisar su origen hay que remontarse al año 1943, no fue hasta 1956 cuando, a raíz de la Conferencia de Inteligencia Artificial en Darmouth, cobró real importancia con la presentación del primer sistema informático diseñado para hacer frente a problemas de búsqueda heurística. Fue en esa ocasión cuando John Mccarthy, ganador del Premio de Turing en 1971, también conocido como Premio Nobel de computación, acuñó por primera vez su término, bajo una definición que conjuga conocimiento científico e ingeniería para construir máquinas inteligentes. Sin embargo, en 1943 Warren McCulloch y Walter Pitts presentaron su modelo de neuronas artificiales, considerada, para muchos, la primera inteligencia artificial.

No obstante, esta primera definición fue rápidamente abandonada. La acelerada y eficiente repercusión que tuvo la inteligencia artificial en las distintas disciplinas provocó que ese primer concepto, abreviado y reducido, se extienda a un sistema que percibe su ambiente y toma decisiones que maximizan su probabilidad de éxito (Russell y Norvig, 2008; Muñoz Villarreal y Gallego Corchero, 2019). Como era de imaginarse, el avasallamiento en su aplicación provocó que, desde sus orígenes, fueran varios los opositores que, por el desconocimiento propio de las verdaderas ventajas que esta herramienta podría alcanzar, intentaran, mediante distintos métodos, frenar su evolución. Entre estos últimos, se encontraban aquellos que la relacionaban como un mecanismo de destrucción del empleo.

Su pensamiento se sustentaba en que, como mínimo, un 30 % de los puestos de trabajo se perderían por la automatización que implica el desarrollo de este programa. Otros, yendo un poco más al extremo, apuntaban que este

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

podría ser el último gran invento del ser humano, puesto que en un futuro serán las maquinas inteligentes las que superarían la inteligencia humana y la reemplazarían en su totalidad para el dominio de la raza humana (Foro Económico Mundial [WEF], 2018). Empero, y pese a las constantes oposiciones a su desarrollo, la inteligencia artificial demostró el desacierto de sus enemigos y se convirtió, hoy, en una realidad cuya contradicción resulta infundada e irrazonable. Tal evolución ha constituido un importante desafío para quienes desde la academia investigan su impacto social y para los juristas que han comenzado a plantearse la posibilidad de promulgar un nuevo derecho que incluya la inteligencia artificial.

Actualmente, no son pocos los que comienzan a implementar el concepto de derecho digital como una rama autónoma, destinada, principalmente, a regular el empleo de los avances de la tecnología digital en procura de evitar que sea utilizada por las empresas privadas e incluso por el poder público para vulnerar derechos, perjudicar la intimidad de las personas y polarizar las sociedades (Vallespino, 2022, p. 35). Resulta indudable que, tras haber pasado más de 24 años del siglo XXI, la puesta en marcha de la inteligencia artificial se ha naturalizado y extendido en distintos campos e industrias. Así, la producción textil, la logística y la industria automotriz, son claros ejemplos de su desarrollo y eficiencia con menor utilización de tiempo y recursos. Los beneficios que aportó —y puede seguir aportando— son tanto cualitativos como cuantitativos. Dentro de los primeros, podemos mencionar la posibilidad de anticipar enfermedades, cuestiones climáticas, o desenlaces evitables, entre tantos más que surgen al detenerse breves instantes a imaginar su repercusión; el otro orden, cuantitativo, se ve materializado en la cantidad de aplicaciones que se pueden utilizar en las distintas ramas (medicina, derecho, ingeniería, etcétera) (Sobrino, 2020).

Ahora bien, a partir de un seguimiento de las tantas disciplinas que imprentaron esta nueva herramienta, puede mencionarse el campo del derecho. No cabe duda que actualmente existe la inteligencia artificial en los juzgados, pues basta con nombrar el sistema *Lex 100*, los expedientes digitales, los buscadores de jurisprudencia o los procesadores de textos, para verificar —a simple vista— su implementación en los tribunales. No obstante, esta inteligencia artificial —a la que se denominará simple o débil— no puede ser suficiente si se pretende lograr en forma óptima los propósitos antes mencionados (eficacia y rapidez). Es necesario recurrir a otro tipo de inteligencia, si lo que se pretende es lograr un verdadero cambio en el derecho (Nieva Fenoll, 2016). Por ello, Searle (1980), en un influyente artículo crítico sobre la inteligencia artificial, introdujo esta importante diferenciación. En dicho trabajo, planteó que la inteligencia artificial débil consiste en sistemas diseñados para reali-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

zar tareas específicas y definidas. Estos sistemas pueden ser altamente especializados y ejecutar funciones complejas con una eficiencia y precisión superiores a las humanas, aunque carecen de comprensión general o autoconciencia. Ejemplos de esta categoría incluyen asistentes virtuales como Siri o Alexa, sistemas de recomendación empleados por Netflix o Amazon, y chatbots, entre otros.

Ahora bien, la inteligencia artificial fuerte implica sistemas capaces de desarrollar actividades intelectuales equivalentes o superiores a las humanas en todos los aspectos, caracterizándose por tener capacidades para comprender, aprender y razonar en diversas áreas del conocimiento. Estos sistemas no se limitan a tareas específicas, sino que pueden realizar cualquier actividad intelectual propia de los seres humanos. Si bien el propósito de los incentivadores del desarrollo de esta herramienta es lograr esta última faceta, lo cierto es que, aún hoy en día, por lo menos en campo de derecho y la gestión judicial en particular, no se ha conseguido. Es por ello que los autores han intentado, con buenos resultados, extender sus ámbitos de aplicación a otros campos, en la medida que no solo se vea limitada a la tramitación de las causas. Como se abordará a continuación, la órbita contractual y el tratamiento de los datos personales han sido algunos de estos campos beneficiados.

1. Tratamiento de datos. Su efecto y regularización a partir de la inteligencia artificial: experiencias suramericanas

La protección de datos personales enfrenta desafíos crecientes debido al avance de la inteligencia artificial (IA) y al desarrollo de nuevas técnicas de minería de datos. La capacidad de analizar grandes volúmenes de información ha convertido a los datos en un activo valioso para las estrategias comerciales, pero también en un riesgo para la privacidad de los individuos. Actualmente, diversas organizaciones utilizan tecnologías avanzadas para recopilar información de manera no invasiva, como la detección de señales electromagnéticas de dispositivos móviles en centros comerciales o el rastreo de ubicaciones, con el objetivo de conocer el comportamiento de los consumidores. La integración de estos datos permite a las empresas anticipar la demanda, diseñar estrategias comerciales personalizadas y generar nuevas oportunidades de negocio. La minería de datos se ha consolidado como una herramienta clave en la toma de decisiones, facilitando la creación de planes estratégicos adaptados a las necesidades del mercado.

No obstante, el procesamiento inadecuado de esta información, sea por correlaciones incorrectas o usos malintencionados, puede representar un gra-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

ve problema para la privacidad y seguridad de los usuarios. Ante estos riesgos, diversas entidades especializadas han emitido advertencias para regular el uso de datos personales y prevenir posibles vulneraciones. Se hace necesario fortalecer la supervisión de estas prácticas y desarrollar normativas que equilibren el aprovechamiento de la IA en la gestión de datos con la protección de los derechos fundamentales de los titulares de la información. Al atender lo referente al marco jurídico argentino, una de las tantas entidades que ha emitido regulación sobre IA fue la Jefatura del Gobierno de Argentina, mediante la Resolución 161/2023. Allí, se estableció el Programa de Transparencia y Protección de Datos Personales en el Uso de la Inteligencia Artificial a través de la AAIP, cuyo propósito, según se explica, consiste en promover el análisis, la regulación y el fortalecimiento de las capacidades del Estado para respaldar el desarrollo y uso de la inteligencia artificial en los sectores público y privado, y asegurar que se respeten y ejerzan de manera efectiva los derechos de los ciudadanos en cuanto a transparencia y protección de datos personales.

Aquí es cuando aparecen las primeras de interrogantes sobre el amparo del dato frente a la IA, ¿qué es un dato personal? ¿cuál es su diferencia con el tratamiento del resto de la información? Para responder a esta pregunta, resulta necesario observar, esencialmente, a los estándares impuestos por la Red Iberoamericana de Protección de Datos. Esta entidad ha abordado el tema al definir el tratamiento de datos personales como cualquier operación o serie de operaciones realizadas mediante métodos físicos o automatizados sobre datos personales, que incluyen —aunque sin limitarse— la obtención, el acceso o registro, así como la organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración y, en general, cualquier forma de uso o manejo de dichos datos (Red Iberoamericana de Protección de Datos [REDIPD], 2020, p. 11).

Esta relación entre la inteligencia artificial y la transferencia de datos personales fue analizada en la Declaración relativa a la Ética y Protección de datos Personales (REDIPD, 2019) y, posteriormente, estudiada en el documento llamado Recomendaciones para el Tratamiento de Datos Personales en la Inteligencia Artificial. A partir de allí, se ha transformado la manera en que se procesan grandes volúmenes de datos a nivel global, lo que, como era imaginable, ha superado con creces las capacidades de las regulaciones actuales.

La cuestión que inevitablemente se debate a partir de esto, es cómo puede la inteligencia artificial peligrar la privacidad de datos. Para esto, hay que destacar dos aspectos claves de esta herramienta, aspectos que, al estudiarla detalladamente, podemos decir que trae tanto ventajas como prejuicios. La primera, es la capacidad que tiene de tomar decisiones de forma automatizada; la segunda, y consecuencia de la anterior, es la aptitud de irse perfec-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

cionando a partir de la información y experiencia que se le proporciona. De allí que resulta imposible el avance de esta herramienta sin comprometer, al menos en alguna medida, los datos personales. Es por ello por lo que, advirtiendo esta situación, se puede ahondar en el ordenamiento jurídico peruano, que cuenta con los principios que su Ley de Protección de Datos Personales establece para efectos de lograr una protección acorde y adecuada, sin detener, en la medida de lo posible, los beneficios de la evolución (Morales Cáceres, 2020).

Dentro de estos principios puede mencionarse, en primer lugar, la legalidad. Este aspecto en particular se refiere a que el tratamiento de los datos debe realizarse en conformidad con la ley, es decir, respetar los derechos de los titulares. La legalidad es un pilar fundamental en la protección de datos, ya que garantiza que cualquier actividad relacionada con la recopilación, almacenamiento y uso de datos personales se realice dentro de un marco normativo que proteja a los individuos (Congreso de la República del Perú, 2011). Esto genera que las organizaciones basen sus actuaciones en una normativa o base legal clara. La legalidad también se relaciona con la transparencia. Las organizaciones deben informar a los titulares sobre cómo se manejarán sus datos, qué tipo de información se recopilará y con qué fines. Esta transparencia no sólo es un requisito legal, sino que también contribuye a generar confianza entre las partes.

Otro de los puntos a valorar, relacionado estrechamente con el primero, es el consentimiento. La autorización de los titulares de esos datos es una circunstancia que no puede pasarse por alto; el fundamento es evitar su obtención por medios fraudulentos. Así, la existencia del consentimiento de una persona para el tratamiento de sus datos personales en determinados casos no autoriza su uso paralelo con fines diferentes, ya que esto implicaría violar el principio de finalidad del tratamiento establecido en el artículo 4.1 y 4.3 de la Ley 25.326 sobre protección de datos personales (Congreso de la República del Perú, 2011; Basterra, 2009). La doctrina señala que la legitimidad del propósito para el cual se han recolectado datos personales constituye la base que justifica su uso, al establecer límites claros a su tratamiento (Gozaini, 2001). En este sentido, el principio de finalidad prohíbe el uso indiscriminado de datos, incluso si fueron obtenidos de manera lícita. Si se desea emplearlos para un objetivo distinto al originalmente consentido, será necesario recabar nuevamente el consentimiento del titular (Melo, 2022).

Ahora bien, la finalidad con la que se utilizan los datos es otro de los principios asentados. Es claro que deben ser utilizados conforme a los fines por los que fueron recolectados; su mantenimiento, con otros propósitos, es un riesgo que debe evitarse si lo que se pretende es lograr una adecuada protección al titular de estos. Y es que, el mantenimiento de los datos para otros propósi-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

tos no autorizados presenta amenazas que deben ser enfrentadas, si lo que se busca es lograr una protección idónea al titular de estos y la posterior y consecuente confianza de estos. Utilizar datos para fines diferentes a aquellos para los cuales fueron recolectados puede llevar a violaciones de privacidad, malentendidos y, en última instancia, daños a la reputación de la organización que, posteriormente, afecte la confianza que busca generar.

A su vez, la calidad y seguridad son los últimos puntos para destacar. La precisión y actualidad de los datos es necesario para cumplir con un debido tratamiento. También, la garantía de la protección y confidencialidad son los elementos que van a permitir que el titular preste su información. El incumplimiento de cualquier de estos elementos hace imposible un adecuado tratamiento de los datos. En consonancia con lo expuesto, es importante mencionar que el artículo 28 de la de la norma peruana regula los deberes a cargo tanto del titular y de los encargados del tratamiento de los datos personales. En este sentido, las disposiciones sobre protección de datos personales son aplicables en los casos en que la inteligencia artificial se desarrolle utilizando información que incluya datos personales. Asimismo, estas normas se extienden al uso de la IA para realizar análisis de perfiles y tomar decisiones relacionadas con personas.

En Colombia, la regulación de la inteligencia artificial ha avanzado mediante políticas públicas, directrices éticas y proyectos legislativos. Destacan el Documento CONPES 3975 de 2019, que estableció la Política Nacional para la Transformación Digital e Inteligencia Artificial, y el Marco Ético para la Inteligencia Artificial de 2021, basado en estándares de la OCDE y la UNESCO. El CONPES promueve la innovación tecnológica en sectores público y privado, mientras que el Marco Ético se enfoca en la transparencia, equidad y protección de derechos fundamentales (Vanegas *et al.*, 2024). En 2024, el país inició la elaboración de una nueva Política Nacional de Inteligencia Artificial (2024-2030), enfocada en gobernanza, ética, infraestructura y formación de talento digital. Esta política busca fortalecer la conectividad y el acceso a datos de calidad mediante alianzas entre el sector privado, la academia y organismos internacionales (Vanegas *et al.*, 2024).

El CONPES 3975 y el Marco Ético destacan la protección de datos personales como un pilar esencial, enmarcándola en la Ley 1581 de 2012. Asimismo, la Circular Externa núm. 002 de 2024 exige que los sistemas de IA cumplan con los principios de confidencialidad, integridad y proporcionalidad, además de requerir consentimiento expreso para el tratamiento de datos sensibles. Estas iniciativas, aunque relevantes, presentan vacíos normativos, especialmente en protección de propiedad intelectual y auditoría de algoritmos,

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

lo que refuerza la necesidad de adaptar el marco regulador colombiano a estándares internacionales como los de la Unión Europea (Vanegas *et al.*, 2024).

2. Recomendaciones para un uso adecuado de la transferencia de datos

La necesidad de establecer un equilibrio entre la inteligencia artificial, la protección de datos y los derechos humanos provocó, de manera casi inmediata, que la Red Iberoamericana de Protección de Datos Personales estableciera una serie de recomendaciones a fin de lograr una correcta transferencia de los datos privados sin violentar los derechos de las personas que presten su consentimiento. Esta medida, apoyada por la Organización de Naciones Unidas, permitió no sólo mitigar los riesgos de la transferencia, sino también ganar y mantener la confianza de los usuarios dispuestos a prestar sus datos. Dentro éstas, puede mencionarse el cumplimiento de las normas locales sobre el tratamiento de datos personales. Aunque la evolución de la inteligencia artificial sea tan rápida que, eventualmente, implica un cambio permanente de las normativas que la regulan, eso no obsta a que las correspondientes entidades establezcan las correspondientes disposiciones legales a fin de darle un marco jurídico que limite el campo de su utilización.

Otra recomendación importante fue la de llevar a cabo un estudio exhaustivo y minucioso sobre el impacto de la privacidad. Este análisis, no sólo permite que los datos sean utilizados de acuerdo con la regulación existente, sino también que ayudará a prevenir la eventual producción de un daño a aquellos que hayan consentido o aceptado prestar sus datos. La comprensión de las implicaciones que puede tener la recopilación y el uso de la información personal es fundamental para proteger los derechos de los individuos en un entorno digital cada vez más complejo. Es importante que las organizaciones no sólo cumplan con las normativas, sino que también actúen de manera proactiva lo fines de salvaguardar la privacidad de los agentes. Realizar un correcto análisis de impacto puede, sin lugar a duda, facilitar la identificación de riesgos potenciales y la implementación de medidas adecuadas para mitigarlos, de modo tal que contribuirá a generar confianza entre los usuarios y las entidades que manejan sus datos.

A su vez, incorporar la privacidad, la ética y la seguridad desde la fase de diseño de los sistemas y procesos de tratamiento de datos es toral. Este punto de partida, conocido como *privacy by design*, genera que las consideraciones sobre la protección de datos se integren en cada etapa del desarrollo de productos y servicios. De esta manera, no sólo se aseguran prácticas

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

responsables desde el principio, sino que se fomenta y desarrolla una actividad organizacional que prioriza y enaltece la ética en el manejo de la información (Brian Nougrères, 2014). Asimismo, la materialización del "principio de responsabilidad demostrada" se convierte en una recomendación central y elemental. Este principio, que obliga a las organizaciones a demostrar que cumplen con las normativas de protección de datos, conlleva la necesidad de asentar políticas claras, auditorías regulares y registros detallados de las actividades de tratamiento. De esta forma, ineludiblemente, no sólo se protege a los individuos, sino que también se fortalece la reputación y la credibilidad de las entidades ante los reguladores y la sociedad en general; elementos que, vale precisar, son centrales para lograr una mayor utilización y confianza (Red Iberoamericana de Protección de Datos [REDIPD], 2021).

En este sentido, el artículo 20.3 de la Red Iberoamericana de Protección de Datos establece una serie de principios no taxativos que orientan a las organizaciones en la implementación de estas medidas. Por ejemplo, para asegurar el cumplimiento del principio de responsabilidad en la protección de datos personales, los responsables del tratamiento pueden adoptar diversas estrategias. Entre ellas, se incluye la asignación de recursos para el desarrollo de políticas y programas de protección de datos, así como la implementación de sistemas de gestión de riesgos vinculados al tratamiento de información personal. También es fundamental la creación de normativas internas obligatorias en esta materia y la capacitación constante del personal sobre sus responsabilidades en la protección de datos. Además, se recomienda la revisión periódica de las políticas de seguridad para introducir mejoras cuando sea necesario, la instauración de mecanismos de supervisión y auditoría que garanticen el cumplimiento de las normativas y la habilitación de canales eficaces para atender consultas y quejas de los titulares de los datos.

Ahora bien, estos principios comprenden tópicos como la transparencia, la limitación de la finalidad y la minimización de datos, entre tantos otros. Al seguir estas directrices, las entidades pueden construir un marco robusto de protección de datos que no sólo cumpla con la legislación vigente, sino que también respete y promueva los derechos fundamentales de los ciudadanos, elementos que, reiteramos, genera una mayor confianza al momento de lograr el consentimiento para el tratamiento de datos. De este modo, respecto a los derechos de los titulares de datos, la Red Iberoamericana de Protección de Datos establece que toda persona tiene derecho a no estar sujeta exclusivamente a decisiones automatizadas que produzcan consecuencias legales o efectos sobre ella, cuando dichas decisiones se basen en tratamientos automatizados orientados a evaluar aspectos personales específicos, sin intervención humana. Esto incluye el análisis o predicción sobre rendimien-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

to profesional, situación económica, salud, preferencias sexuales, fiabilidad o comportamiento (Red Iberoamericana de Protección de Datos [REDIPD], 2017).

En suma, un enfoque integral, que combine un estudio del impacto de la privacidad, la integración de principios éticos desde el diseño y la demostración de responsabilidad es trascendental para garantizar un tratamiento de datos que sea seguro y respetuoso. Así, se sientan las bases para una convivencia digital más justa y equitativa, en la que la protección de la privacidad se convierta en un pilar fundamental.

IV. *Smarts contracts*. Su concepto y la diferenciación con los contratos tradicionales

El estudio de los contratos inteligentes genera dudas terminológicas y conceptuales que crean confusión sobre su verdadera naturaleza. Su principal innovación radica en la *autogestionabilidad*, es decir, la capacidad de ejecutarse sin intervención humana una vez cumplidas ciertas condiciones programadas. A diferencia de los contratos tradicionales, donde el cumplimiento de obligaciones y la imposición de sanciones requieren la intervención de personas y del sistema judicial, los *smart contracts* operan de manera autónoma, aplicando sanciones automáticamente según los términos predefinidos en su código (Sobrino, 2020; Ibáñez Jiménez, 2018). Otra característica esencial es su completitud teórica, ya que los algoritmos intentan prever todas las posibles contingencias dentro del ciclo contractual, lo que les confiere una apariencia de perfección. Sin embargo, desde una perspectiva práctica, esta idealización es inalcanzable, pues es imposible anticipar todas las eventualidades que pueden surgir en una relación contractual. Además, funcionan bajo una lógica binaria *if-then*, donde las obligaciones y consecuencias están predefinidas en términos absolutos, lo que elimina toda posibilidad de interpretación o subjetividad al momento de su ejecución.

Finalmente, su inalterabilidad representa una ventaja en términos de seguridad y confiabilidad, ya que el código almacenado en *blockchain* impide modificaciones posteriores. Sin embargo, esta misma característica puede generar problemas en situaciones donde la flexibilidad y la adaptabilidad del contrato sean necesarias. En consecuencia, aunque los *smart contracts* aportan eficiencia y automatización, su implementación debe considerar los desafíos jurídicos y técnicos asociados a su naturaleza autoejecutable y rígida.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

1. ¿Son contratos inteligentes?

Como se mencionó al comienzo del acápite anterior, existe un malentendido terminológico que rodea a esto tipo de contrato. El error en su definición supone, equivocadamente, que la principal característica que reúne a esta herramienta es la inteligencia. Para entender el porqué de su error conceptual nos tenemos que remitir, principalmente, al concepto propio de la inteligencia artificial. Ya hemos dicho, al iniciar este trabajo, que la primera vez que se acuñó el término de IA fue cuando John McCarthy, ganador del Premio Turing en 1971, la definió como la ciencia e ingeniería de hacer máquinas inteligentes.

Si bien este concepto —como se explicó— se modificó posteriormente, lo cierto es que el elemento sustancial que identifica y diferencia a la inteligencia artificial, más allá de cualquier definición que se le quiera imputar, es la capacidad que tienen estas máquinas de aprender por sí solas. Así, se está ante la principal cuestión a resolver: ¿los contratos inteligentes aprenden por sí solos? La respuesta es, sin duda, negativa. Que los contratos se autoejecuten por sí solos, no significa que sean capaces de aprender ni desarrollarse por sí mismos. Es necesario, al momento de entender esta herramienta, que la *autoejecutabilidad* no implica autoaprendizaje. Incluso, se ha dicho, que estos contratos son tan rudimentarios que algunos autores los han llamados *dumb contracts* o contratos tontos.

En síntesis, entendemos que, contrariamente a su propia definición, se está ante un proceso informático autoejecutable que no tiene ningún tipo de razonamiento o pensamiento, sino, exclusivamente, un contrato que se base en el sistema o principio *if then*. Ahora, bien, al tener en cuenta lo comentado anteriormente, al ser los contratos inteligentes una suerte de sistemas automatizados programados, cada vez que más es certero que su desarrollo se vincule con los procesos de inteligencia artificial para potencializar su *autoejecutabilidad*, lo que lleva al núcleo problémico de este estudio.

V. Inteligencia artificial y *smart contracts*. Protección de datos personales

Como se estableció en el apartado de precedencia, son pocos los avances que se han tenido en Latinoamérica sobre la regulación de la inteligencia artificial y los contratos inteligentes, precisamente en materia de protección de datos personales. Así, se observó que se ha prestado especial atención en la

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

protección y tratamiento de datos por parte de las legislaciones nacionales y las recomendaciones de agencias internacionales, empero, no ha existido una conjugación entre la inteligencia artificial, la contratación automatizada y los datos. Particularmente, en relación con los *smart contracts*, tal como comenta Fuentes Blanco (2022), en la actualidad, la mayoría de los países de América Latina carece de un marco normativo específico que regule los contratos inteligentes y la tecnología *blockchain*.

No obstante, la mayoría de los países cuentan con disposiciones que otorgan validez jurídica a los actos celebrados electrónicamente y regulaciones en materia de firma digital. Esta normativa existente podría, en principio, permitir el reconocimiento legal de los contratos inteligentes dentro de los ordenamientos jurídicos de la región, a pesar de la ausencia de una regulación expresa que contemple sus particularidades y desafíos jurídico. Algunos países de América Latina, como Argentina y Ecuador, han desarrollado ciertas disposiciones normativas aplicables a los contratos inteligentes, lo que justifica un análisis particular de sus marcos jurídicos. En el caso de Argentina, aunque el Código Civil y Comercial de la Nación (2014), que regula los contratos celebrados por los particulares, no contempla expresamente a los contratos inteligentes, la doctrina jurídica ha interpretado que estos pueden ser considerados contratos válidos en la medida en que cumplan con los requisitos esenciales exigidos por la legislación para la formación y validez de los actos jurídico.

Adicionalmente, una diferencia distintiva del ordenamiento jurídico argentino, respecto de otros sistemas jurídicos latinoamericanos, radica en la incorporación de los contratos inteligentes dentro del ámbito de los servicios de confianza para la firma digital. A través del Decreto 182 de 2019, se estableció que los prestadores de servicios de confianza pueden gestionar contratos inteligentes, lo que representa un reconocimiento normativo expreso de esta tecnología y sus efectos jurídicos. Esta disposición otorga mayor certeza legal a los contratos automatizados en Argentina, situando al país en una posición avanzada dentro de la región en cuanto a la regulación de estas innovaciones tecnológicas. En otro contexto está Ecuador, quien, el 9 de mayo de 2019, a través de la Asamblea Nacional aprobó el nuevo Código de Comercio, que introdujo una definición formal de los contratos inteligentes en su artículo 77, el cual establece que el contrato inteligente facilita la expresión de voluntad y garantiza su cumplimiento mediante instrucciones previamente acordadas por las partes, que pueden ejecutarse automáticamente por el propio programa o por un tercero designado, como una entidad financiera, según lo hayan previsto. Al activarse una condición preestablecida sin intervención humana, el contrato inteligente ejecuta automáticamente la cláusula correspondiente.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

En ausencia de previsión contractual específica, la responsabilidad por las obligaciones surgidas recae sobre los administradores o quienes tengan el control del programa. En todos los casos, resultan aplicables las normas que protegen los derechos del consumidor.

Sin temor a equívocos, la inclusión de los contratos inteligentes en el Nuevo Código de Comercio del Ecuador representa un importante avance en la doctrina jurídica, ya que constituye la primera definición completa de esta figura contractual dentro de un código de comercio en Hispanoamérica. Este reconocimiento normativo no sólo establece un marco legal claro para su aplicación, sino que también delimita aspectos fundamentales sobre la responsabilidad contractual y extracontractual en caso de omisión de estipulaciones en el contrato. Además, la normativa aclara que los contratos inteligentes están sujetos a las disposiciones del derecho del consumidor, lo que garantiza la protección de las partes en relaciones comerciales donde intervengan sistemas automatizados (Fuentes Blanco, 2022).

En el plano estadounidense, varios estados han liderado la regulación de *blockchain* y contratos inteligentes, estableciendo marcos jurídicos que podrían influir en la adopción de estas tecnologías a nivel global. En Arizona, la House Bill 2417, aprobada en 2017, otorgó reconocimiento legal a los contratos inteligentes y las firmas electrónicas basadas en *blockchain*. Esta ley establece que los registros escritos y las firmas electrónicas no pueden ser rechazados legalmente por el simple hecho de estar almacenados en una *blockchai*n. Este marco normativo representó un hito en la regulación de la tecnología, al proporcionar un entorno claro y favorable para su aplicación en el ámbito contractual. Por su parte, Delaware, estado reconocido por su enfoque innovador en derecho corporativo, enmendó en 2017 su Ley General de Sociedades Anónimas y permitió a las empresas registrar sus acciones en una *blockchain* y gestionar sus relaciones corporativas mediante contratos inteligentes. Esta reforma ha incentivado la adopción de esta tecnología en la administración empresarial, atrayendo a diversas compañías tecnológicas interesadas en aprovechar su seguridad y eficiencia operativa (Mingarro Mannarino, 2024).

A pesar de los esfuerzos normativos sobre los contratos inteligentes, no se incluye lo relativo a la protección de datos, lo que queda amparado por los ordenamientos jurídicos tradicionales en la materia. La realidad es que los contratos inteligentes, al recopilar datos y operar a través de Internet, incrementan el riesgo para la privacidad de los individuos. La información registrada en estos contratos se almacena en una base de datos distribuida dentro de la cadena de bloques, lo que implica que, aunque la criptografía asimétrica protege en gran medida la confidencialidad de los datos, existen escenarios donde

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

la vulnerabilidad es mayor. En particular, cuando los contratos inteligentes se implementan en *blockchains* privadas, el riesgo se intensifica debido a que la administración del *ledger* recae en un agente particular, lo que podría comprometer la seguridad y el control sobre la información almacenada (Fuentes Blanco, 2022).

Lo anterior se potencia cuando se vincula la inteligencia artificial a los contratos inteligentes. Y es que, el avance de la inteligencia artificial generativa también ha planteado importantes desafíos en materia de protección de datos personales, particularmente debido a la falta de un marco jurídico especializado que regule su desarrollo y aplicación, tal como se expresó en el apartado anterior. La carencia de regulación clara ha permitido que las empresas tecnológicas adopten estrategias de autorregulación, comprometiendo la seguridad y privacidad de los datos personales en un entorno digital en constante evolución (Sánchez Díaz, 2024).

Uno de los principales problemas que enfrenta la protección de datos personales en el contexto de la inteligencia artificial es la asimetría de información entre las empresas tecnológicas y los usuarios. Muchas veces, los individuos no tienen conocimiento del uso que se le dará a sus datos, ni del tratamiento que recibirán dentro de los sistemas de IA. Este escenario se agrava con la automatización del análisis de perfiles y la toma de decisiones, ya que los algoritmos pueden generar consecuencias adversas para los titulares de los datos sin su conocimiento ni consentimiento explícito (Sánchez Díaz, 2024).

1. Autorregulación de los *smart contracts* y la inteligencia artificial. *Lex Criptográfica*

En este ámbito, se ha desarrollado una suerte de *lex criptográfica*, un concepto emergente que surge en el ámbito de la *blockchain* y la criptografía, proponiendo un marco de autorregulación tecnológica que opera de manera independiente a las normativas tradicionales del Estado, que debe tenerse en cuenta en los casos latinoamericanos que no se tiene una regulación concreta para la vinculación de los contratos inteligentes, la inteligencia artificial y la protección de datos personas. Los contratos inteligentes han sido incorporados dentro del ecosistema de la *lex criptográfica* como un mecanismo de autorregulación, a partir de la premisa de que el código puede sustituir a las normas legales tradicionales. Este fenómeno ha permitido la creación de sistemas contractuales descentralizados, al eliminar intermediarios y reducir costos de transacción. Sin embargo, su efecto regulatorio aún es objeto de debate, ya que la ausencia de supervisión jurídica podría generar conflictos en la in-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

terpretación de cláusulas contractuales automatizadas (Calderón Marenco *et al.*, 2024), sobre todo cuando se aborda acerca de la gobernanza de los datos.

Actualmente, su reconocimiento legal depende de la aplicación supletoria de principios generales del derecho contractual. El uso de IA en contratos inteligentes introduce una nueva discusión en la protección de datos personales porque la *lex criptográfica*, al operar en un entorno descentralizado, permite la recopilación y almacenamiento de información en redes *blockchain*, lo que genera dudas sobre la privacidad y el acceso a la información personal. Y es que, la inmutabilidad de la *blockchain* contradice principios como el derecho al olvido y la minimización de datos, fundamentales en normativas nacionales e internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (Calderón Marenco y Raúdez Hernández, 2024). Es así como, hoy en día, las regulaciones sobre protección de datos personales de los ordenamientos jurídicos nacionales no contienen especial protección sobre los datos personales cuando se implementan contratos inteligentes e inteligencia artificial.

2. La apuesta internacional y europea para la protección de datos

La inteligencia artificial, especialmente la generativa, ha puesto en evidencia la insuficiencia del marco normativo actual para garantizar la privacidad y seguridad de la información. La falta de una regulación específica ha permitido que las grandes corporaciones tecnológicas implementen mecanismos de autorregulación, lo que ha dejado la tutela de los derechos fundamentales supeditada a intereses comerciales. Esta brecha entre la evolución tecnológica y la respuesta jurídica ha expuesto a los ciudadanos a riesgos que comprometen su autodeterminación informativa, como la recopilación masiva de datos sin consentimiento y la vulnerabilidad frente a tecnologías de manipulación digital, como los *deepfakes* (Sánchez Díaz, 2024).

El uso de la inteligencia artificial en la automatización de decisiones y el análisis de perfiles ha generado incertidumbre sobre la responsabilidad legal en caso de afectaciones a los derechos fundamentales. La inmutabilidad de la tecnología *blockchain*, utilizada en contratos inteligentes, presenta tensiones con principios clave del derecho a la protección de datos, como el derecho al olvido y la minimización de datos. La ausencia de intervención humana en estos procesos dificulta la implementación de mecanismos correctivos, lo que plantea la necesidad de adaptar los marcos normativos para garantizar que el desarrollo de la inteligencia artificial se realice en un entorno regulado, que equilibre la innovación tecnológica con la protección de los derechos fundamentales (Sánchez Díaz, 2024).

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

El efecto de la inteligencia artificial en la protección de datos ha demostrado la urgencia de reformular los principios jurídicos tradicionales para responder a los desafíos de la digitalización. La regulación debe evolucionar hacia un modelo que combine la autonomía tecnológica con mecanismos de control efectivos, como auditorías algorítmicas y la exigencia de explicabilidad en la toma de decisiones automatizadas. La falta de una regulación integral ha permitido la consolidación de un entorno de vigilancia masiva y explotación de datos sin consecuencias jurídicas mayores. Es necesario desarrollar principios que permitan una integración responsable de la inteligencia artificial en los sistemas jurídicos y asegurar la tutela de los derechos fundamentales y evitando asimetrías de poder en el entorno digital (Sánchez Díaz, 2024).

Así las cosas, existen diversos pronunciamientos internacionales que se han venido configurando a partir del desarrollo de la inteligencia artificial y los contratos inteligentes. El documento principal que conjuga el abordaje de ambas tecnologías es el generado por el Grupo de Trabajo IV de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) en su 63 periodo de sesiones, en el cual se discutió la necesidad de desarrollar un régimen jurídico que regule la contratación automatizada y el uso de la IA en estos procesos. Se destacó la importancia de distinguir entre sistemas automatizados y sistemas de inteligencia artificial, al considerar que estos últimos presentan un grado de autonomía y aprendizaje adaptativo que puede generar incertidumbre jurídica. Asimismo, se señaló la necesidad de garantizar principios fundamentales como la transparencia, la no discriminación y la neutralidad tecnológica en la regulación de la contratación automatizada (CNUDMI, 2022).

El Grupo de Trabajo analizó los desafíos que plantea la atribución de responsabilidad en los contratos celebrados mediante sistemas automatizados e inteligencia artificial. Se discutió la posibilidad de que los contratos generados a través de sistemas autónomos sean considerados jurídicamente válidos, siempre que cumplan con los principios generales del derecho contractual. No obstante, la automatización plantea interrogantes sobre la capacidad de los sistemas para asumir obligaciones y la eventual necesidad de modificar las normas de atribución de responsabilidad, en caso de incumplimiento o daño. Además, se exploraron mecanismos de control para garantizar la trazabilidad de las decisiones automatizadas, con el fin de asegurar la protección de los derechos de las partes involucradas en los contratos celebrados mediante IA (CNUDMI, 2022).

Tal como comparte, Guilabert Vidal (2022), el documento en comento ha puesto énfasis en la responsabilidad y las medidas legales necesarias para enfrentar los errores en el procesamiento y resguarde de datos. Además,

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

el pronunciamiento de la CNUDMI ha impulsado debates en torno a la creación de un marco normativo que permita regular de manera conjunta el ecosistema tecnológico de los contratos inteligentes y la inteligencia artificial, en consideración de su carácter interconectado y descentralizado.

En ausencia de una normativa específica, algunos ordenamientos han incorporado disposiciones que, de manera indirecta, regulan la responsabilidad y los derechos de los contratantes en entornos automatizados. Así, en el ámbito europeo, la Propuesta de Reglamento del Parlamento y del Consejo de la Unión Europea sobre acceso y uso de datos establece requisitos esenciales para los contratos inteligentes, al garantizar su robustez técnica para evitar manipulaciones y errores funcionales, el cual se analizará en líneas posteriores. Asimismo, el documento impone la obligación de contar con sistemas de archivo de datos y estrictos controles de acceso. Estos pronunciamientos han generado un intenso debate en torno al principio de *code is law*, dado de que la regulación de la inteligencia artificial y la automatización en la contratación exige un equilibrio entre la innovación tecnológica y la seguridad jurídica, lo que hace imprescindible la formulación de un marco normativo que brinde certeza a los usuarios, sin comprometer el desarrollo de estas tecnologías (Guilabert Vidal, 2022).

Igualmente, la CNUDMI ha señalado que entre los aspectos críticos en la ejecución automatizada y la inteligencia artificial se encuentran la supervisión de los sistemas autónomos, la posibilidad de establecer estándares mínimos de transparencia y la determinación de límites a la autonomía de los algoritmos en la formación, ejecución y modificación de los contratos. Por estas razones, la necesidad de un marco jurídico flexible y adaptable se presenta como una prioridad para los organismos internacionales, dado el impacto creciente de la inteligencia artificial en el comercio global y la seguridad de las transacciones electrónicas (CNUDMI, 2022).

Así que la protección de datos personales se ha convertido en un pilar trascendental dentro del ecosistema tecnológico, dada la creciente digitalización de las transacciones y la interconectividad global. Respecto de la protección de datos, es importante resaltar que existen dos enfoques predominantes en esta materia: el específico y el integral. El primero, adoptado por Estados Unidos y reflejado en acuerdos como el Acuerdo Marco para la Facilitación del Comercio Transfronterizo sin Papel de la Comisión Económica y Social de las Naciones Unidas para Asia y el Pacífico, prioriza la libre circulación de datos con mínima intervención estatal. Este enfoque busca facilitar el comercio electrónico sin imponer restricciones trascendentes, lo que permite un intercambio fluido de información, pero a su vez genera preocupaciones sobre la privacidad y la seguridad de los datos.

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

El segundo, adoptado por la Unión Europea, presenta una perspectiva integral a través del Reglamento General de Protección de Datos (RGPD), al establecer un marco jurídico robusto que regula, de manera estricta, la recopilación, procesamiento y almacenamiento de datos personales. Esta normativa impone obligaciones estrictas a las empresas y entidades que manejan información personal, lo que garantiza un alto nivel de protección para los ciudadanos europeos (Sidorova y Sidorov, 2025). El RGPD ha servido como referencia internacional para otras jurisdicciones que buscan fortalecer la regulación de datos personales en entornos digitales. Su aplicación extraterritorial implica que cualquier entidad que procese datos de ciudadanos europeos debe cumplir con sus disposiciones, independientemente de su ubicación. Sin embargo, este modelo ha generado fricciones en el ámbito del comercio internacional, ya que las restricciones a la transferencia de datos pueden entrar en conflicto con las disposiciones de libre comercio establecidas por la Organización Mundial del Comercio (OMC).

Empero, sobre datos y contratos inteligentes, el artículo 36 establece los requisitos esenciales que deben cumplir estos en la ejecución de acuerdos de intercambio de datos. Se impone la obligación a los proveedores de aplicaciones que empleen contratos inteligentes, así como a las personas cuya actividad profesional implique su despliegue, de garantizar el cumplimiento de ciertos estándares técnicos y de seguridad. Entre estos requisitos se destacan la solidez estructural y los mecanismos de control de acceso para evitar fallos funcionales y manipulaciones externas. También se exige la incorporación de mecanismos que permitan la interrupción segura de las transacciones en caso de necesidad, lo que asegura que los contratos inteligentes incluyan funciones de *reinicialización* o terminación para evitar ejecuciones accidentales o no deseadas. Adicionalmente, se establece la obligación de archivar los datos de las transacciones finalizadas, lo que permite la trazabilidad de las operaciones previas y garantiza la auditabilidad de los contratos.

El cumplimiento de estos requisitos será objeto de evaluación por parte del proveedor del contrato inteligente o la persona responsable de su implementación, quienes deberán expedir una declaración de conformidad en el ámbito de la Unión Europea. Se presume que aquellos contratos inteligentes que se adhieran a normas armonizadas publicadas en el *Diario Oficial de la Unión Europea* cumplen con los requisitos esenciales del artículo 36. Asimismo, se faculta a la Comisión Europea para adoptar especificaciones comunes mediante actos de ejecución, en caso de que no se disponga de normas armonizadas adecuadas o estas no sean aceptadas en el proceso de estandarización. La Comisión podrá consultar a organismos especializados y expertos antes

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

de establecer estos requisitos, garantizando un proceso de deliberación técnica y jurídica que permita la adaptación de la normativa a los avances tecnológicos.

Se contempla un mecanismo de supervisión a nivel de los Estados miembros, que les permite objetar una especificación común si consideran que no cumple plenamente con los requisitos esenciales. En tales casos, la Comisión evaluará la objeción y podrá modificar el acto de ejecución correspondiente. Cuando una norma armonizada sea adoptada por una organización europea de normalización y su referencia sea publicada en el *Diario Oficial de la Unión Europea,* la Comisión derogará cualquier acto de ejecución que establezca los mismos requisitos esenciales. Este marco regulatorio busca garantizar la confiabilidad y seguridad de los contratos inteligentes en el ámbito del intercambio de datos, asegurando la protección de los derechos de los usuarios y la estabilidad del ecosistema digital en la Unión Europea.

En el año 2024, nace el Reglamento de Inteligencia Artificial de la Unión Europea (RIA), y que, sin lugar a duda, la protección de datos personales ocupa un papel central en la regulación de la inteligencia artificial, al ser reconocida como un eje fundamental para garantizar el respeto a los derechos fundamentales en el desarrollo y despliegue de estas tecnologías. La normativa europea ha establecido tres aspectos clave en esta materia: el acceso a datos de calidad, la gobernanza de los datos y la garantía del derecho a la intimidad y a la protección de datos personales. El acceso a datos de calidad se considera esencial para el correcto funcionamiento de los sistemas de inteligencia artificial, en particular, aquellos clasificados como de alto riesgo. La regulación europea establece que estos datos deben ser pertinentes, representativos, completos y libres de errores, además de incorporar mecanismos que mitiguen cualquier sesgo que pueda afectar la seguridad, la salud o los derechos fundamentales.

Para garantizar este acceso, las autoridades que proporcionan datos deben asegurar la disponibilidad de información de alta calidad para el entrenamiento, validación y prueba de los sistemas de IA, al prevenir la generación de sesgos o discriminaciones prohibidas por la normativa europea (RIA, art. 10.3).

La gobernanza de los datos es otro pilar fundamental en la estrategia regulatoria europea y se ha desarrollado a través del Reglamento (UE) 2022/868, el cual establece un marco normativo para la reutilización de datos públicos y protegidos en distintos sectores. En el caso de los sistemas de IA de alto riesgo, el RIA introduce normas específicas que distinguen entre los conjuntos de datos utilizados en distintas etapas del desarrollo de la IA, incluyendo entrenamiento, validación y prueba. Estas reglas de gobernanza se centran en diversos aspectos, como el diseño del sistema, la recolección y preparación de datos, la evaluación de su idoneidad y la implementación de medidas para detectar y mitigar sesgos. La normativa también prevé la posibilidad de tratar

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

categorías especiales de datos personales con el único propósito de corregir sesgos en modelos de IA, siempre que se implementen garantías adecuadas, tales como restricciones en la reutilización, medidas de seguridad avanzadas, controles rigurosos y eliminación de los datos una vez concluido su uso, conforme al artículo 15 del RIA. Además, se reconoce la posibilidad de recurrir a terceros que ofrezcan servicios certificados de verificación y cumplimiento en materia de gobernanza de datos, asegurando la integridad del conjunto de datos y la correcta aplicación de procesos de entrenamiento, validación y prueba (RIA, art. 10.5).

La norma europea también incide en la necesidad de garantizar la protección de los datos personales durante todo el ciclo de vida de un sistema de inteligencia artificial. Para ello, se aplican los principios de minimización de datos y protección desde el diseño y por defecto, tal como establece el RGPD. Con el fin de cumplir con estos principios, se recomienda el uso de técnicas como la amonificación, el cifrado y el desarrollo de tecnologías que permitan entrenar modelos de IA sin necesidad de transferir datos entre entidades ni duplicar la información. De esta forma, la regulación europea busca asegurar un equilibrio entre la innovación tecnológica y la protección de los derechos fundamentales, al establecer obligaciones claras para los proveedores de sistemas de inteligencia artificial y promoviendo un desarrollo responsable de estas tecnologías (RIA, art. 67).

Por último, y no menos importante, se encuentra la Iniciativa de Declaración Conjunta sobre Comercio Electrónico de la Organización Mundial de Comercio (OMC, 2024), la cual ha intentado encontrar un equilibrio entre la facilitación del comercio digital y la protección de datos personales. Si bien esta iniciativa promueve la adopción de medidas para garantizar la seguridad de los datos, no impone obligaciones vinculantes ni sanciones en caso de incumplimiento, y deja en manos de cada Estado la implementación de políticas adecuadas a sus necesidades y capacidades. Este enfoque flexible ha sido criticado por no garantizar una protección homogénea a nivel global, lo que puede generar desigualdades en la seguridad y tratamiento de los datos personales según la jurisdicción de cada.

VI. Conclusiones

La implementación de inteligencia artificial en *smart contracts* genera desafíos en materia de regulación y protección de datos personales. La automatización de los contratos ha traído consigo ventajas en términos de eficiencia y seguridad, pero también ha provocado incertidumbre respecto a la suficien-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

cia del marco normativo vigente para garantizar la privacidad y la seguridad jurídica de los usuarios. A pesar de que algunos países de América Latina han avanzado en la regulación de la inteligencia artificial y la contratación digital, la falta de normativas específicas para la protección de datos en *blockchains* y sistemas descentralizados sigue siendo un obstáculo para su integración segura en los sistemas jurídicos.

En este contexto, el estudio identifica que la *lex criptográfica* ha emergido como una forma de autorregulación en entornos descentralizados, pero su alcance es limitado ante la ausencia de mecanismos de supervisión estatal y control jurisdiccional efectivo. La comparación entre las normativas de América Latina y la Unión Europea revela que, si bien en la UE existen regulaciones avanzadas como el Reglamento General de Protección de Datos (RGPD) y el Reglamento de Inteligencia Artificial (RIA), en los países latinoamericanos aún predominan enfoques dispersos que no abordan de manera integral la interacción entre inteligencia artificial, contratación digital y protección de datos personales. Esta brecha regulatoria aumenta el riesgo de vulneraciones a la privacidad y dificulta la armonización del derecho con las nuevas tecnologías.

Por lo tanto, se concluye que es prioridad desarrollar un marco regulador que contemple tanto la seguridad jurídica como la protección efectiva de los datos personales en entornos automatizados. Se requiere una actualización normativa que garantice la transparencia en el procesamiento de datos, la trazabilidad de las decisiones automatizadas y la implementación de principios como la minimización de datos y el consentimiento informado. Asimismo, se recomienda fomentar la cooperación internacional y la adopción de estándares globales que permitan equilibrar la innovación tecnológica con la protección de los derechos fundamentales, asegurando que la inteligencia artificial y los *smart contracts* puedan operar dentro de un marco legal claro y garantista.

VII. Referencias

Agencia de Acceso a la Información Pública. (2023). Resolución 161/2023: Programa de transparencia y protección de datos personales en el uso de la Inteligencia Artificial. *Boletín Oficial de la República Argentina*. https://www.boletinoficial.gob.ar/detalleAviso/primera/293363/20230904

Asamblea Nacional del Ecuador. (2019). Código de Comercio de la República del Ecuador. https://www.gob.ec/sites/default/files/regulations/2022-10/C%C3%B3digo%20de%20Comercio.pdf

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

Basterra, M. I. (2009). *Protección de datos personales para fines publicitarios: a propósito de la Disposición 4/2009 de la Dirección Nacional de Protección de Datos Personales*. Universidad Nacional de la Plata. https://sedici.unlp.edu.ar/bitstream/handle/10915/147831/Documento_completo.pdf?sequence=4&isAllowed=y

Brian Nougrères, A. (2014). *Las nuevas tecnologías en la protección de datos: "Privacy by Design"*. Presentación en el XII Encuentro Iberoamericano de la Red Iberoamericana de Protección de Datos, IFAI – Transparencia y Privacidad. https://www.redipd.org/sites/default/files/inline-files/Ana-Brian.pdf

Calderón Marenco, E. A. y Raúdez Hernández, I. (2024). Desinformación digital y democracia en Iberoamérica: retos y oportunidades de la Lex Criptográfica. *Derecho Global. Estudios sobre Derecho y Justicia*, 9(26), 377-401. https://doi.org/10.32870/dgedj.v9i26.728

Calderón Marenco, E. A., Rodríguez Palacios, T. S., Garzón Solano, J. E. y Ravelo-Franco, G. (2024). Construyendo la delimitación de la Lex Criptográfica. *Revista Jurídica Austral*, 5(1), 551-575. https://doi.org/10.26422/RJA.2024.0501.cal

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional [CNUDMI]. (2022). *Resumen de la Presidencia y la Relatoría sobre la labor realizada por el Grupo de Trabajo IV (Comercio Electrónico) en su 63er período de sesiones (Nueva York, 4 a 8 de abril de 2022)*. Naciones Unidas. https://documents.un.org/doc/undoc/gen/v22/028/09/pdf/v2202809.pdf

Congreso de la Nación Argentina. (2014). Código Civil y Comercial de la Nación (Ley 26.994). *Boletín Oficial de la República Argentina*. https://www.boletinoficial.gob.ar/detalleAviso/primera/119644/20140808

Congreso de la República del Perú. (2011). Ley núm. 29733: Ley de protección de datos personales. https://www.boletinoficial.gob.ar/detalleAviso/primera/293363/20230904

Departamento Nacional de Planeación. (2019). *CONPES 3975: Política Nacional de Transformación Digital e Inteligencia Artificial*. https://siteal.iiep.unesco.org/sites/default/files/sit_accion_files/11134.pdf

Foro Económico Mundial WEF. (2018). *El impacto de la Revolución 4.0 en el mercado laboral de las y los jóvenes en Argentina: Una perspectiva desde la sostenibilidad de la seguridad social*. https://www.argentina.gob.ar/sites/default/files/3._el_impacto_de_la_revolucion_4.0_en_el_mercado_laboral_de_las_y_los_jovenes_en_argentina.pdf

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

Fuentes Blanco, E. A. (2022). *Contratos inteligentes: un análisis teórico desde la autonomía privada en el ordenamiento jurídico colombiano*. Editorial Unimagdalena. https://elibro.net/es/ereader/upna/214513?page=1

Gozaini, O. (2001). *Hábeas data: protección de datos personales*. Rubinzal-Culzoni Editores.

Guilabert Vidal, M. R. (2022). "Smarts contracts", finanzas descentralizadas, inteligencia artificial y responsabilidad civil a propósito del protocolo de código abierto "PoolTogether". *Revista Aranzadi de Derecho y Nuevas Tecnología*, (60). https://dialnet.unirioja.es/servlet/articulo?codigo=8667751

Ibáñez Jiménez, J. (2018). Cuestiones jurídicas en torno a la cadena de bloques (blockchain) y los contratos inteligentes (*smart contracts*). *ICADE. Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, *(101)*. https://doi.org/10.14422/icade.i101.y2017.003

Melo, V. (2022). Inteligencia artificial, desinformación y protección de datos personales. *In Itinere. Revista Digital de Estudios Humanísticos de la Universidad FASTA*, *12*(1). https://repositorio.uca.edu.ar/bitstream/123456789/16405/1/inteligencia-artificial-desinformaci%c3%b3n.pdf

Mingarro Mannarino, J. (2024, septiembre 3). Blockchain y contratos inteligentes: la nueva frontera del derecho contractual en Argentina. *Legalmente al Día*. https://www.linkedin.com/pulse/blockchain-y-contratos-inteligentes-la-nueva-frontera-joaquin-2lsxf/

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Marco ético para la inteligencia artificial en Colombia*. https://minciencias.gov.co/sites/default/files/marco-etico-ia-colombia-2021.pdf

Morales Cáceres, A. (2020). *El impacto de la inteligencia artificial en la protección de datos personales*. World Compliance Association. https://www.worldcomplianceassociation.com/2767/articulo-el-impacto-de-la-inteligencia-artificial-en-la-proteccin-de-datos-personales.html

Muñoz Villarreal, A. y Gallego Corchero, V. (2019). Inteligencia artificial e irrupción de una nueva personalidad en nuestro ordenamiento jurídico ante la imputación de responsabilidad a los robots. En A. Muñoz Villarreal y E. Monterroso Casado (Coords.), *Inteligencia artificial y riesgos cibernéticos: responsabilidades y aseguramiento* (pp. 67-100). Árbol Académico.

Nieva Fenoll, J. (2016). La desburocratización de los procedimientos judiciales: reflexiones a propósito del Código Procesal Modelo para Iberoamérica. En *La ciencia jurisdiccional: novedad y tradición* (pp. 619-640).

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

Marcial Pons; Ediciones Jurídicas y Sociales. https://doi.org/10.2307/jj.2321998.36

Organización Mundial de Comercio [OMC]. (2024). Iniciativa relacionada con la declaración conjunta sobre el comercio electrónico. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/INF/ECOM/87.pdf&Open=True

Presidencia de la Nación Argentina. (2019). Decreto 182/2019: Reglamentación de la Ley núm. 25.506 sobre Firma Digital. *Boletín Oficial de la República Argentina*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/320735/norma.htm

Red Iberoamericana de Protección de Datos [REDIPD]. (2017). *Estándares iberoamericanos de protección de datos personales*. https://www.redipd.org/documento/estandares-iberoamericanos-2017.pdf

Red Iberoamericana de Protección de Datos [REDIPD]. (2019). *Guía de orientaciones específicas para la protección de datos en proyectos de inteligencia artificial*. https://www.redipd.org/documento/guia-orientaciones-especificas-proteccion-datos-ia-es.pdf

Red Iberoamericana de Protección de Datos [REDIPD]. (2020). *Guía de recomendaciones generales para el tratamiento de datos personales en proyectos de inteligencia artificial*. https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf

Red Iberoamericana de Protección de Datos [REDIPD]. (2021). *Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube*. https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf

Russell, S. y Norvig, P. (2008). *Inteligencia artificial: un enfoque moderno*. Pearson.

Sánchez Díaz, M. F. (2024). Inteligencia artificial generativa y los retos en la protección de los datos personales. *Estudios en Derecho a la Información*, 18, 179-205. https://doi.org/10.22201/iij.25940082e.2024.18.18852

Searle, J. R. (1980). Minds, brains, and programs. *Behavioral and Brain Sciences*, 3(3), 417-424. https://doi.org/10.1017/S0140525X00005756

Sidorova, E. y Sidorov, V. (2025). La carrera regulatoria del comercio electrónico en el marco de la Organización Mundial del Comercio. *Ciencia Jurídica*, *14*(27), 57-73. https://doi.org/10.15174/cj.v14i27.512

Sobrino, W. (2020). *Contratos, neurociencias e inteligencia artificial*. La Ley.

Superintendencia de Industria y Comercio. (2024). Circular Externa núm. 002 del 21 de agosto de 2024. https://sedeelectronica.sic.gov.co/trans-

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059

parencia/normativa/circular-externa-no-002-de-2024-del-21-de-agosto-de-2024-lineamientos-sobre-el-tratamiento-de-datos-personales-en-sistemas-de

Unión Europea. (2023). Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828. *Diario Oficial de la Unión Europea*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023R2854

Vallespino, C. G. (2022). *Tratado de derecho a la salud: fundamentos, principios y valores*. Rubinzal-Culzoni editores.

Vanegas, V., Angarita, A. y Arenas, H. (2024, septiembre). La inteligencia artificial como motor clave para el desarrollo social y económico de Colombia. *Planeación y Desarrollo*. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/PublishingImages/Planeacion-y-desarrollo/2024/Septiembre/PDF/inteligencia-artificial.pdf

Cómo citar

Sistema IIJ

Calderón Marenco, Eduardo Andrés; Sánchez Silveyra, Romina M.; Rodrigo, Juan Manuel, y Ravelo-Franco, Gabriel, "La protección de datos a partir de la implementación de IA en smart contracts", *Estudios en Derecho a la Información*, México, vol. 11, núm. 21, enero-junio de 2026, e20059. https://doi.org/10.22201/iij.25940082e.2026.21.20059

APA

Calderón Marenco, E. A., Sánchez Silveyra, R. M., Rodrigo, J. M., y Ravelo-Franco, G. (2026). La protección de datos a partir de la implementación de IA en smart contracts. *Estudios en Derecho a la Información*, *11*(21), e20059. https://doi.org/10.22201/iij.25940082e.2026.21.20059

e-ISSN: 2594-0082
DOI: https://doi.org/10.22201/iij.25940082e.2026.21.20059