IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Responsabilidad civil del oráculo: intersección entre el derecho privado y los contratos inteligentes

Eduardo Andrés Calderón Marenco
Universidad Cooperativa de Colombia

Jimmy Enrique Garzón Solano
Universidad Cooperativa de Colombia

Romina Mariela Sánchez Silveyra
Universidad de Concepción del Uruguay, Argentina

Guillermo Oscar Sal
Universidad de Concepción del Uruguay, Argentina

Gabriel Ravelo-Franco
Universidad Continental, Perú

Fecha de presentación: julio 2024
Fecha de aceptación: diciembre 2024
Fecha de publicación: marzo 2025

Resumen

Este artículo aborda la interacción entre la tecnología *blockchain*, los oráculos y el derecho privado; se centra en la responsabilidad civil de los oráculos, que proporcionan datos esenciales para los contratos inteligentes. Asimismo, destaca los desafíos de precisión y manipulación de información, con énfasis en la necesidad de regulaciones adaptativas para proteger los intereses involucrados y promover una integración tecnológica justa. Los tópicos abordados son: el problema del oráculo de *blockchain*, los desafíos de su centralización, los riesgos de errores del oráculo, el aprovechamiento malicioso del sistema y el riesgo de colusión. El estudio resalta también la importancia de una colaboración estrecha entre juristas y tecnólogos para crear un marco legal que afronte eficazmente los dilemas legales y éticos emergentes en la era digital.

Palabras clave

derecho civil; regulación; daños; blockchain (cadena de bloques); información

Oracle's civil liability: intersection between private law and smart contracts

Abstract

This paper addresses the interaction between blockchain technology, oracles, and private law. It focuses on the civil liability of oracles that provide essential data for smart contracts. It highlights the challenges of accuracy and information manipulation and underlines the need for adaptive regulations to protect the involved interests and promote fair technological integration. Likewise, it emphasizes the importance of close collaboration between legal experts and technologists to create a legal framework that effectively addresses the emerging legal and ethical dilemmas in the digital era.

Keywords

civil law; regulation; damages; blockchain; information

Introducción

Los contratos inteligentes prometen transformar la ejecución y concepción de contratos a través de una amplia gama de sectores. Estas tecnologías ofrecen un nuevo paradigma de automatización, eficiencia y transparencia, lo que puede reducir la necesidad de intermediarios tradicionales y las fricciones asociadas con la ejecución contractual.

Dichos contratos son programas autoejecutables almacenados en la *blockchain* que se activan automáticamente cuando se cumplen condiciones predefinidas. Aunque son potentes por su capacidad para facilitar, verificar o ejecutar la negociación de un contrato de manera transparente y sin intermediarios, su funcionalidad se limita al ámbito digital de la cadena de bloques en la que residen. Aquí es donde entran en juego los oráculos, que actúan como puentes que traen información del mundo real a la cadena de bloques, lo que permite que los contratos inteligentes reaccionen a eventos externos. Sin embargo, esta dependencia hace que la seguridad y la efectividad de un contrato inteligente sean tan robustas como lo sea la precisión y la integridad de los datos que recibe del oráculo.

De este modo, la integración de datos del mundo real por medio de oráculos introduce desafíos referidos a la precisión y fiabilidad de la información que alimenta a los contratos inteligentes. Este cruce entre lo digital y lo tangible abre un campo de interrogantes legales y éticos, acentuadas cuando la información proporcionada por oráculos lleva a resultados no intencionados o incluso dañinos.

Frente a estos retos, las respuestas legales tienden a seguir el ritmo de los cambios tecnológicos y sociales con cierto retraso. A menudo, la jurisprudencia enfrenta dificultades para adaptarse a estos avances, especialmente cuando se trata de integrar acontecimientos de la esfera digital en el marco legal físico sin realizar los ajustes necesarios. Desde disciplinas como el derecho civil y mercantil, se están desarrollando análisis para comprender estas nuevas realidades bajo un enfoque jurídico concreto. No obstante, se requiere que los cambios sean idóneos para hacer frente a la complejidad que presentan casos derivados de la implementación de nuevas tecnologías, como en el caso de los contratos inteligentes. Estos ejemplos evidencian la complejidad intrínseca y la deslocalización característica de la vida digital, que introduce automáticamente elementos de diversidad en situaciones anteriormente inimaginables (Diago Diago, 2024).

Por ello, aun con el refinamiento que podrían aportar las soluciones de inteligencia artificial, están lejos de poder eludir los principios fundamentales del derecho privado. Los algoritmos, por sí solos, no tienen la capacidad de sustituir la ley obligatoria ni son útiles en situaciones que requieren un juicio de valor. Aunque es cierto que las sanciones del derecho privado en el entorno de la cadena bloques podrían generar perjuicios, Kulms (2020) sugiere que el verdadero valor de la combinación entre el derecho privado, los contratos inteligentes y los procesos algorítmicos, reside en otro lado. Para él, se generaría una sinergia, a partir del análisis detallado del derecho privado y una presión moderada por parte de las autoridades del

mercado de capitales, lo que se traduciría en contratos inteligentes que refuercen y profundicen los estándares legales, tanto en escenarios públicos como en redes sujetas a permisos, así como sus híbridos.

El presente estudio toma también como premisa la necesidad de que la ley controle los contratos de explotación, particularmente en el contexto del internet de las cosas (IoT), donde la personalización de bienes, servicios y contratos a través de datos personales cosechados puede beneficiar a algunos usuarios mientras expone a otros a daños, no solo por violaciones de la privacidad, sino también por contratos adaptados a sus vulnerabilidades, reveladas por esos datos. Este punto ilustra cómo la tecnología puede ser utilizada tanto para innovar como para explotar, y revela así la compleja interacción entre la tecnología, la ley y la ética en la era digital (Hacker, 2017). De este modo, ante la ausencia de un marco legislativo y jurisprudencial específico que aborde directamente estas cuestiones, este artículo explora las implicaciones legales y las cuestiones de responsabilidad que surgen.

Este enfoque nos permite navegar por las tensiones entre la autonomía tecnológica y la necesidad de establecer normativas adaptadas a las nuevas formas de interacción y responsabilidad que emergen. Se prestará especial atención a la dinámica entre las partes involucradas –desarrolladores, usuarios y proveedores de datos– y cómo esta afecta la asignación de responsabilidades, especialmente en contextos de disparidad en el poder de negociación o en el control sobre la configuración y ejecución del contrato.

1.1. El problema del oráculo de *blockchain*

Las cadenas de bloques son sistemas cerrados que operan bajo un consenso interno, lo que significa que toda la información que afecta al estado de la *blockchain* debe ser verificada por sus participantes según las reglas del protocolo de consenso. Sin embargo, muchas de sus aplicaciones, como los contratos inteligentes, requieren datos del mundo real para ejecutar sus términos de forma adecuada. Estos datos pueden incluir eventos como resultados electorales, cambios en precios de mercado, condiciones meteorológicas, entre otros.

El problema del oráculo surge porque la cadena de bloques, por su diseño, no tiene la capacidad de verificar directamente la precisión de la información externa. Introducir esta información requiere un mecanismo que actúe como puente entre el mundo exterior y el sistema automatizado, estos son los llamados *oráculos*.

Los oráculos, por lo tanto, son entidades que permiten introducir información externa: pueden ser fuentes de datos, programas informáticos o agentes. Sin embargo, este proceso introduce una vulnerabilidad en el sistema: la confianza. Aunque las cadenas de bloques están diseñadas para operar de manera descentralizada y sin necesidad de confiar en terceros, los oráculos representan una excepción, ya que el sistema debe confiar en la información proporcionada por los oráculos para ejecutar operaciones basadas en datos externos.

De este modo, la implementación de oráculos plantea preocupaciones sobre la manipulación de datos y la centralización del poder, lo cual compromete la integridad y transparencia de los sistemas en *blockchain*. La centralización de los oráculos crea vulnerabilidades, ya que introduce puntos únicos de fallo, que exponen a los contratos inteligentes a riesgos de censura, manipulación y control externo. Esto puede derivar en decisiones incorrectas con consecuencias económicas y de reputación.

Adler y otros destacan este problema (George, 2023), al señalar que cualquier solución al problema del oráculo debe abordar cómo se puede confiar en los datos externos sin comprometer los principios fundamentales de seguridad, descentralización y falta de confianza que caracterizan a las cadenas de bloques. Una de las soluciones exploradas es el uso de juegos de *Schelling* para incentivar a los oráculos a proporcionar información precisa, basándose en un juego de coordinación donde los participantes son recompensados por coincidir con la mayoría, con la esperanza de que la verdad o el dato más preciso se convierta en el punto focal alrededor del cual se coordinan las respuestas de los oráculos.

La complejidad del problema del oráculo radica en encontrar un equilibrio entre la necesidad de información externa, que sea precisa para el funcionamiento de aplicaciones *blockchain* complejas, y el mantenimiento de los principios de confianza mínima y descentralización.

Antes de continuar, se debe precisar que los contratos inteligentes no son estrictamente inteligentes, ya que son incapaces de entender el lenguaje natural (como los términos contractuales) o de verificar de forma autónoma si un evento relevante para su ejecución se ha

materializado; para esto, se necesitan oráculos. Así, los oráculos actúan como intermediarios que permiten a los contratos inteligentes interactuar con datos externos. Son esenciales porque la naturaleza cerrada de dichas cadenas impide que los contratos inteligentes accedan directamente a información del mundo real, como tasas de cambio, resultados de eventos o datos meteorológicos. Esto limitaría significativamente la aplicabilidad de los contratos inteligentes en escenarios reales sin la intervención de los oráculos.

Los estudios revisados aportan ejemplos concretos de la aplicación de los oráculos, que demuestran su versatilidad y potencial y que, al mismo tiempo, identifican las debilidades o desafíos que se deben abordar. Un estudio desarrolló una plataforma de comercio energético *peer-to-peer* (P2P) en una microred que utiliza cadena de bloques e internet de las cosas. Este caso de estudio exploró el desarrollo del sistema en un ambiente de laboratorio para facilitar transacciones seguras y eficientes. Dicha investigación presenta el uso de oráculos como puentes para datos externos, como lecturas de medidores inteligentes, y su integración con contratos inteligentes. A pesar de su éxito, se identificaron desafíos en rendimiento, escalabilidad, modelos de negocio en tiempo real, y aspectos de ciberseguridad y privacidad, que resultan útiles para marcar direcciones futuras de investigación y desarrollo (Condon *et al*., 2023).

Por otro lado, si bien existe abundante investigación sobre las criptomonedas y aplicaciones específicas, la literatura sobre la gobernanza ambiental que utilice esta tecnología es escasa y en gran medida aspiracional. Existe un consenso en sugerir que se requieren más demostraciones específicas de casos para la futura adopción de soluciones basadas en *blockchain*. La ejecución de tales sistemas está limitada por la experiencia técnica, la escalabilidad, la privacidad y la seguridad, así como los estándares regulatorios (Chung y Adriaens, 2024).

1.2. Riesgo de errores del oráculo

Es necesario seleccionar oráculos que se basen en fuentes de información confiables. Un ejemplo de la importancia de esta selección ocurrió en 2020, cuando una inexactitud en los datos de precios suministrados por un oráculo a la plataforma Compound llevó a una liquidación indebida valorada en alrededor de cien millones de dólares (Hierro Viétiez, 2021).

Otro caso real que grafica este riesgo se encuentra en el mundo de las finanzas descentralizadas (DeFi). El incidente ocurrido en junio de 2019 con la plataforma Synthetix (Warwick, 2019) evidencia los desafíos asociados con la centralización de oráculos en contratos inteligentes. Synthetix, una plataforma DeFi, permite a sus usuarios crear y comerciar *synths*, activos sintéticos que replican el valor de activos reales como divisas y acciones, sin necesidad de poseer el activo subyacente. Sin embargo, la fiabilidad y precisión en el precio de estos *synths* dependen de los datos suministrados por oráculos. El incidente involucró un error en la configuración de un oráculo que proporcionaba datos de precios para el won surcoreano (KRW) mil veces mayores que su valor de mercado, lo que fue aprovechado por un usuario para realizar operaciones que, en teoría, generaron ganancias de más de mil millones de la moneda estable de la plataforma. Aunque este evento no resultó en pérdidas financieras reales para la comunidad debido a la intervención de los administradores de Synthetix (tuvieron que pagar al hacker una recompensa para que revierta las operaciones), sirvió como una llamada de atención sobre los riesgos inherentes a la centralización de los oráculos y la necesidad de estrategias de mitigación robustas.

En respuesta a este incidente, Synthetix anunció medidas hacia la descentralización de sus oráculos; también reconocieron la importancia de diversificar las fuentes de datos para incrementar la seguridad y la confiabilidad del sistema. Aunque los detalles específicos sobre la implementación de sistemas de reputación y contratos de penalización no se detallan ampliamente en los comunicados públicos, el sector de DeFi, incluido Synthetix, ha mostrado un interés creciente en explorar tales mecanismos. Estos enfoques buscan incentivar la entrega de datos precisos y proporcionar disuasivos contra la manipulación mediante la imposición de penalizaciones a los oráculos que suministren datos incorrectos. Este caso resalta la vulnerabilidad de los sistemas DeFi a la manipulación y los fallos en oráculos centralizados, y subraya la necesidad imperante de adoptar estrategias de descentralización y seguridad más robustas. La experiencia de Synthetix ilustra cómo los desafíos pueden convertirse en oportunidades para reforzar la infraestructura y las prácticas de gobernanza en el ecosistema DeFi.

Para hacer frente a estos riesgos, es necesario garantizar la descentralización de los oráculos. Al recurrir a múltiples fuentes independientes para la recopilación de datos, se

minimizan los riesgos asociados con los puntos únicos de fallo y la manipulación de datos. Este enfoque no solo mejora la seguridad y la fiabilidad de los datos, sino que también promueve una mayor transparencia en el proceso de toma de decisiones de los contratos inteligentes.

Además, la implementación de sistemas de reputación para los oráculos es otra estrategia efectiva. Estos sistemas incentivan la provisión de datos precisos y confiables, a través de la penalización a aquellos oráculos que falten a su compromiso de honestidad. Asimismo, los contratos de penalización, que imponen sanciones económicas por la entrega de datos incorrectos, sirven como un disuasivo efectivo contra la manipulación de datos.

El escenario descrito coincide con lo afirmado por Corrales Compagnucci *et al*. (2022), quienes afirman que el jurista del futuro participará activamente en equipos transdisciplinarios, donde el mero conocimiento jurídico y la capacidad para discernir cuestiones legales no serán suficientes. Será necesaria la colaboración con expertos de diversas áreas y la generación conjunta de soluciones que sean viables tanto en términos operativos como legales.

Finalmente, la transparencia y la verificabilidad de los procesos de los oráculos son aspectos clave para construir confianza en estos sistemas. Asegurar que los métodos de recolección y procesamiento de datos sean accesibles y comprensibles para todas las partes interesadas, fortalece la integridad del ecosistema de los contratos inteligentes.

1.3. Riesgo de colusión

El análisis de cómo las tecnologías de registro descentralizado influyen en la organización de la industria y el panorama competitivo abarca diversas dimensiones, desde la promoción de la eficiencia hasta el riesgo de fomentar prácticas colusivas (Cong y He, 2019).

La capacidad de las cadenas de bloques para proporcionar un consenso descentralizado y ejecuciones algorítmicas seguras es fundamental para su valor en la ampliación del espacio de contratación. Los contratos inteligentes automatizan las ejecuciones contractuales y reducen la necesidad de intermediarios, lo que puede disminuir los costos de transacción y mejorar la eficiencia. Sin embargo, la eficacia de los contratos inteligentes depende de la calidad de la codificación y la anticipación de posibles contingencias, lo que plantea desafíos en términos de complejidad legal y técnica.

La descentralización del consenso modifica el entorno de información en la *blockchain*, lo que potencialmente facilita una mayor transparencia. Sin embargo, esta transparencia tiene un doble filo. Por un lado, puede mejorar la eficiencia del mercado al proporcionar información confiable sobre las transacciones. Por otro lado, como se argumenta en el trabajo citado, esta transparencia puede fomentar la colusión tácita entre vendedores, especialmente en escenarios donde los actores del mercado pueden observar y reaccionar a las actividades de los demás más fácilmente que en los mercados tradicionales.

La propuesta de soluciones regulatorias y de mercado, como separar a los agentes generadores de consenso de los usuarios finales, sugiere caminos para mitigar los riesgos de colusión y maximizar los beneficios de las cadenas de bloques. Sin embargo, implementar estas soluciones plantea sus propios desafíos, incluida la definición de marcos regulatorios adecuados que no impongan cargas desproporcionadas o irrazonables a la innovación. En resumen, mientras se generan oportunidades para mejorar la eficiencia y el bienestar, también existen riesgos, especialmente en términos de colusión y competencia.

2. Responsabilidad civil del oráculo

Este apartado examina los dos enfoques de responsabilidad aplicables: la responsabilidad contractual y la extracontractual, así como la diferencia entre un régimen de responsabilidad por culpa y uno de responsabilidad objetiva. Cada enfoque presenta implicaciones distintas para los derechos de los usuarios y las obligaciones de los proveedores, especialmente en entornos descentralizados donde las relaciones entre las partes suelen ser tácitas y no reguladas por contratos explícitos. También se desarrollan los tópicos relativos a la determinación de los daños indemnizables, así como a las cláusulas de exclusión o limitación de responsabilidad.

2.1. ¿Responsabilidad contractual o extracontractual?

En este punto, es necesario abordar la cuestión de si los fallos en la provisión de datos o en la precisión de estos

deben generar una responsabilidad de carácter contractual o extracontractual. La determinación entre una y otra es crucial, pues impacta los derechos de los afectados y las obligaciones de los proveedores de oráculos, especialmente en un entorno en el que las partes involucradas a menudo interactúan sin acuerdos formales directos.

En los sistemas de *blockchain*, los oráculos cumplen un rol de intermediarios externos que suministran datos a contratos inteligentes. Esta relación se caracteriza, en muchos casos, por la ausencia de un vínculo contractual explícito entre los proveedores de oráculos y los usuarios de dichos datos, ya que estos últimos suelen ser partes de un contrato inteligente en el que el oráculo actúa como fuente de datos sin interactuar directamente con ellos. Según la doctrina europea, en escenarios donde no existe una relación contractual explícita, la responsabilidad tiende a calificarse como extracontractual, ya que no existe un acuerdo que defina las expectativas y obligaciones entre las partes (Martín-Casals, 2022).

Para que la responsabilidad contractual aplique en este contexto, sería necesario que los usuarios de *blockchain* y los proveedores de oráculos celebren un contrato específico que regule la provisión de datos. En dicho contrato, se podrían establecer estándares de calidad, precisión y responsabilidad, así como cláusulas de limitación o exclusión de responsabilidad, como sugieren los enfoques regulatorios de la UE para los servicios de IA en mercados financieros (Montagnani *et al*., 2024). Esto permitiría que cualquier fallo en los datos proporcionados por el oráculo se considere un incumplimiento de las obligaciones contractuales acordadas.

Sin embargo, debido a la estructura descentralizada de *blockchain*, es común que no exista tal contrato, y los usuarios de los contratos inteligentes confíen en los datos de oráculos de manera tácita o implícita. Por lo tanto, en ausencia de este acuerdo formal, los mecanismos tradicionales de responsabilidad contractual resultan insuficientes para abarcar los riesgos derivados del uso de datos inexactos o falsos proporcionados por los oráculos.

En los casos en que no se establezca un vínculo contractual, los usuarios de *blockchain* podrían invocar la responsabilidad extracontractual ante fallos de los oráculos. La jurisprudencia europea y las propuestas regulatorias han comenzado a reconocer la aplicabilidad de la responsabilidad extracontractual en situaciones donde un servicio o producto causa daños a terceros sin una relación contractual directa (Wagner, 2023). En este sentido, los proveedores de oráculos, al ofrecer datos que impactan en decisiones automáticas de los contratos inteligentes, asumen un rol que implica una *obligación de diligencia* hacia terceros.

En el enfoque extracontractual, los proveedores de oráculos podrían ser responsables si se demuestra que un daño fue causado por su falta de diligencia al proporcionar datos inexactos o manipulados. Además, en sistemas interconectados como *blockchain*, la dificultad de rastrear el origen exacto de un error en los datos justifica, según algunos autores, la aplicación de presunciones de causalidad y defectividad que favorezcan a las víctimas (Wagner, 2018; Montagnani y Cavallo, 2021).

2.2. ¿Responsabilidad objetiva o por culpa?

La responsabilidad objetiva se fundamenta en el riesgo inherente de ciertas actividades, donde los daños potenciales son significativos y difíciles de evitar mediante un control adecuado. En el contexto de los oráculos en *blockchain*, el hecho de que estos proporcionen información que activa decisiones automáticas en contratos inteligentes sugiere una situación de alto riesgo para los usuarios, particularmente en ámbitos financieros y comerciales donde una inexactitud o manipulación de datos puede desencadenar graves pérdidas económicas.

Wagner (2018) propone que, en sistemas autónomos y de alto riesgo, la responsabilidad objetiva es un enfoque adecuado para proteger a los afectados, ya que facilita la compensación sin exigir pruebas detalladas sobre la conducta negligente del proveedor. Aplicado a los oráculos, este marco permitiría a los usuarios afectados por datos incorrectos obtener reparación por los daños sin necesidad de probar la falta de diligencia del proveedor, considerando que la complejidad técnica de *blockchain* dificulta identificar y atribuir claramente la culpa en cada caso.

La responsabilidad por culpa, en cambio, requiere demostrar que el proveedor de datos actuó con negligencia, es decir, que no cumplió con los estándares de cuidado que se esperaría razonablemente en la provisión de información para contratos inteligentes. Este enfoque sería aplicable si se espera que los proveedores de oráculos implementen medidas específicas de verificación de datos, seguridad y actualización continua, tal como sugiere

Hinteregger (2023) al analizar estándares de diligencia en entornos tecnológicos.

Sin embargo, debido a que los proveedores de oráculos no siempre tienen control completo sobre los datos externos que recogen y ofrecen a los contratos inteligentes, resulta complejo evaluar si su conducta fue negligente en cada caso. Además, Montagnani *et al*. (2024) argumentan que, en tecnologías descentralizadas, los usuarios finales tienen un acceso limitado a los procesos internos de verificación de datos, lo cual dificulta la posibilidad de comprobar una falla en la conducta del proveedor, lo que convierte la responsabilidad por culpa en una vía más complicada para los usuarios afectados.

En sistemas descentralizados y autónomos, donde el riesgo es alto y la atribución de culpa es compleja, la doctrina sugiere que la responsabilidad objetiva ofrece una solución más eficiente y protectora para las víctimas (Koch, 2020). La responsabilidad objetiva permite superar los desafíos probatorios asociados con la responsabilidad por culpa, y favorece la compensación en casos donde los proveedores de oráculos, al operar en entornos de alto riesgo, deberían prever la posibilidad de errores en los datos que ofrecen.

Además, la adopción de un régimen de responsabilidad objetiva en *blockchain* se alinea con los enfoques regulatorios recientes en la UE que buscan facilitar la reparación en tecnologías emergentes. La responsabilidad objetiva también incentivaría a los proveedores de oráculos a implementar estándares de seguridad y calidad más estrictos, conscientes de que responderán por cualquier daño derivado de sus servicios sin importar la existencia de negligencia.

2.3. Determinación de los daños indemnizables

Según Koch (2020), los daños económicos directos deberían considerarse indemnizables en sistemas tecnológicos donde los proveedores de servicios tienen un papel determinante en el resultado de las transacciones automatizadas.

Además de los daños directos, también pueden surgir daños económicos indirectos, como la pérdida de oportunidades comerciales o la interrupción de otros contratos asociados al contrato inteligente original. Montagnani *et al*. (2024) argumentan que, en sistemas de IA y automatización en los servicios financieros, los daños indirectos deben delimitarse cuidadosamente, ya que su alcance puede ser difícil de prever. En el contexto de los oráculos, es aconsejable limitar estos daños indirectos a aquellos que sean consecuencia inmediata y directa del error en los datos, para evitar una ampliación excesiva de la responsabilidad del proveedor.

El ámbito de los daños no patrimoniales, como el perjuicio moral o la afectación de la reputación, también puede ser relevante en casos donde el fallo de un oráculo afecta a individuos o entidades de manera significativa. Sin embargo, en el contexto de los contratos inteligentes y los oráculos, la mayoría de los autores sostiene que los daños no patrimoniales deberían ser considerados indemnizables solo de manera excepcional, ya que el objetivo principal de la compensación es cubrir las pérdidas económicas y patrimoniales.

En este sentido, Wagner (2018) sostiene que, en sistemas autónomos y digitales, la responsabilidad debe centrarse en los daños materiales o económicos, dejando los daños no patrimoniales fuera del ámbito indemnizable a menos que estén expresamente estipulados en el marco normativo o en el contrato, en caso de existir. Esto evita una ampliación desproporcionada de la responsabilidad en un entorno donde las relaciones entre los usuarios y los proveedores de oráculos son mayormente impersonales y automáticas.

Dado que los proveedores de oráculos no tienen control directo sobre el uso que los contratos inteligentes hacen de sus datos, es fundamental delimitar los daños indemnizables a aquellos que sean previsibles. La previsibilidad se basa en que el proveedor de oráculos pueda anticipar razonablemente las consecuencias de un fallo en los datos, especialmente en aplicaciones financieras o comerciales de alto riesgo.

Ahora, de acuerdo con el enfoque de Hinteregger (2023), los daños indemnizables deberían limitarse a aquellos que el proveedor de datos pueda prever razonablemente en el momento de la provisión de información. Esto podría incluir únicamente los daños directos derivados de la inexactitud de los datos, mientras que se excluyen los daños indirectos y aquellos que resulten de usos imprevistos o atípicos de la información proporcionada. Esta delimitación reduce la carga potencial sobre los proveedores y asegura que la compensación sea proporcionada y justa.

En los casos en que exista una relación contractual entre el proveedor de oráculos y los usuarios, como podría

suceder en sistemas de *blockchain* más regulados o centralizados, se pueden incluir cláusulas de exclusión o limitación de responsabilidad que delimiten los daños indemnizables. Estas cláusulas permiten a los proveedores de oráculos controlar y anticipar sus riesgos, en particular frente a entornos donde la provisión de datos podría desencadenar consecuencias de amplio alcance.

Según el análisis de Montagnani y Cavallo (2021), en sistemas financieros, tales cláusulas pueden ser esenciales para garantizar la sostenibilidad del servicio y limitar la responsabilidad a un nivel manejable. Por ejemplo, los proveedores de oráculos podrían excluir su responsabilidad por daños indirectos o limitar el monto de la compensación a un valor predeterminado, lo cual es común en contratos de servicios digitales.

2.4. Cláusulas de exclusión o reducción de responsabilidad

Una de las cláusulas más comunes en entornos de servicios digitales es la exclusión de responsabilidad por daños indirectos y consecuenciales. Esta cláusula se justifica en el caso de los oráculos, donde un fallo en los datos puede desencadenar pérdidas económicas que van más allá de la transacción inmediata, como la interrupción de otros contratos o la pérdida de oportunidades comerciales.

Así, es previsible que se estipulen cláusulas que limiten la responsabilidad del proveedor a los daños directos derivados del error, excluyendo los daños colaterales que podrían surgir de manera inesperada o desproporcionada en aplicaciones complejas como las financieras o comerciales.

Para los proveedores de oráculos que operan en entornos de alto riesgo, como los mercados financieros, establecer una cláusula de limitación de responsabilidad a un monto máximo específico es una práctica recomendada. Esta cláusula proporciona una previsibilidad tanto para el proveedor como para el usuario en cuanto al alcance máximo de indemnización en caso de fallos. Esta disposición ayuda a mitigar el impacto financiero para el proveedor y establece un umbral claro de compensación, alineándose con enfoques regulatorios que buscan limitar la carga económica en proveedores de servicios digitales (Wagner, 2018).

Por otro lado, dado que los oráculos obtienen datos de fuentes externas sobre las cuales el proveedor no tiene control absoluto, una cláusula de exclusión de responsabilidad por inexactitudes provenientes de terceros resulta pertinente. Esta cláusula protege al proveedor en casos donde el fallo o error en los datos se debe a la fuente de información original y no a una falta de diligencia en la transmisión de estos. Esta exclusión es particularmente relevante en sistemas descentralizados, donde los proveedores de oráculos actúan como intermediarios y no como garantes de la veracidad absoluta de los datos, dado que dependen de la fiabilidad de terceros (Montagnani y Cavallo, 2021).

Asimismo, los proveedores de oráculos también pueden incluir una cláusula de exclusión de responsabilidad en casos de fuerza mayor o eventos imprevistos que escapen a su control, como fallos en la red de *blockchain*, interrupciones en la conectividad o ataques cibernéticos. Esto les permite excluir su responsabilidad cuando ocurren circunstancias extraordinarias que afectan el flujo y la precisión de los datos. Una cláusula de este tipo proporciona una protección adicional en el contexto de los oráculos, ya que los sistemas descentralizados y digitales son particularmente vulnerables a factores externos e imprevistos que pueden afectar la provisión de datos (Koch, 2020).

Finalmente, una cláusula de renuncia de garantías es útil para establecer que los datos proporcionados por el oráculo se ofrecen *tal cual* y que el proveedor no garantiza la precisión o fiabilidad absoluta de la información. Esto permite gestionar las expectativas de los usuarios y subraya que el proveedor no asume una responsabilidad absoluta sobre la veracidad de los datos.

Conclusiones

Aplicar la naturaleza extracontractual de la responsabilidad permite la protección de los usuarios y la asignación de riesgos, y habilita así una vía de reclamo para quienes sufren daños sin necesidad de una relación contractual formal.

La complejidad técnica y el riesgo inherente de los oráculos en *blockchain* favorecen la adopción de un régimen de responsabilidad objetiva que permite a las víctimas obtener compensación sin tener que probar negligencia. Este enfoque es congruente con los principios aplicados a tecnologías emergentes de alto riesgo, donde el control sobre el servicio es limitado y la atribución de culpa puede resultar difícil. La responsabilidad objetiva incentiva ade-

más la adopción de medidas preventivas por parte de los proveedores de oráculos.

La delimitación de los daños indemnizables a aquellos que sean económicos directos y previsibles permite un enfoque compensatorio adecuado y evita que la responsabilidad se extienda de manera desproporcionada. La exclusión de los daños no patrimoniales y la limitación de los daños indirectos a los casos de consecuencia inmediata y directa garantizan una protección balanceada para los usuarios mientras se preserva la viabilidad del servicio de los oráculos.

Las cláusulas de exclusión y limitación de responsabilidad permiten a los proveedores definir los límites de su responsabilidad y gestionar el riesgo asociado a la provisión de datos externos. Cláusulas específicas, como la exclusión de daños indirectos y la limitación de responsabilidad a un monto máximo, ofrecen claridad y previsibilidad a ambas partes. Además, las cláusulas de exclusión de responsabilidad por datos de terceros y por fuerza mayor contribuyen a gestionar riesgos en entornos descentralizados y expuestos a eventos fuera del control del proveedor.

La experiencia europea y la normativa en desarrollo para tecnologías autónomas evidencian la necesidad de un marco regulador adaptado a la singularidad de los oráculos en *blockchain*. Un marco regulatorio específico permitiría establecer estándares de diligencia, pautas de responsabilidad objetiva y reglas claras sobre daños indemnizables y límites de compensación, brindando seguridad jurídica tanto para usuarios como para proveedores en el uso de estos servicios innovadores.

Referencias bibliográficas

CHUNG, K.H.Y.; ADRIAENS, P. (2024). «Blockchain technology for pay-for-outcome sustainable agriculture financing: implications for governance and transaction costs». *Environmental Research Communications*, n.º 6, págs. 1-11. DOI: https://doi.org/10.1088/2515-7620/ad16f0

CONDON, F.; FRANCO, P.; MARTÍNEZ, J.M.; ELTAMALY, A.M.; KIM, Y.-C.; AHMED, M.A. (2023). «EnergyAuction: IoT-Blockchain architecture for local peer-to-peer energy trading in a microgrid». *Sustainability*, vol. 15, n.º 17, págs. 1-28. DOI: https://doi.org/10.3390/su151713203

CONG, L.W.; HE, Z. (2019). «Blockchain Disruption and Smart Contracts». *The Review of Financial Studies*, vol. 32, n.º 5, págs. 1754-1797. DOI: https://doi.org/10.1093/rfs/hhz007

CORRALES COMPAGNUCCI, M.; FENWICK, M.; HAAPIO, H.; VERMEULEN, E.P.M. (2022). «Integrating law, technology, and design: teaching data protection and privacy law in a digital age». *International Data Privacy Law*, vol. 12, n.º 3, págs. 239-252. DOI: https://doi.org/10.1093/idpl/ipac012

DIAGO DIAGO, M.P. (2021). «Ciberactivismo, 'Lex' informática, 'blockchain' y oráculos: desafíos en la era digital». En: J.J. CASTELLÓ PASTOR (ed.). *Desafíos jurídicos ante la integración digital aspectos europeos e internacionales*. Thomson Reuters Aranzadi [en línea]. Disponible en: https://www.millenniumdipr.com/archivos/1624954554.pdf

GEORGE, W. (2023). «Strategic behaviour and manipulation resistance in Peer-to-Peer, crowdsourced information gathering». *Mathematical Social Sciences*, vol. 124, págs. 1-23. DOI: https://doi.org/10.1016/j.mathsocsci.2023.04.002

HACKER, P. (2017). «Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things». *International Data Privacy Law*, vol. 7, n.º 4, págs. 266-286. DOI: https://doi.org/10.1093/idpl/ipx014

HIERRO VIÉTIEZ, G. (2021). «Introducción al blockchain, los contratos inteligentes y su relación con el arbitraje». *Themis Revista de Derecho*, n.º 79, págs. 299-309. DOI: https://doi.org/10.18800/themis.202101.016

HINTEREGGER, M. (2023). «Art 4:102 Principles of European Tort Law». *Journal of European Tort Law*, vol. 14, n.º 1, págs. 61-72. DOI: https://doi.org/10.1515/jetl-2023-0005

KOCH, B. A. (2020). «Liability for Emerging Digital Technologies: An Overview». *Journal of European Tort Law*, vol. 11, n.º 2, págs. 115-136. DOI: https://doi.org/10.1515/jetl-2020-0137

KULMS, R. (2020). «Blockchains. Private law matters». *Singapore Journal of Legal Studies*, págs. 63-89 [en línea]. Disponible en: https://www.jstor.org/stable/10.2307/27032601

MARTÍN-CASALS, M. (2022). «An approach to some EU initiatives on the regulation of liability for damage caused by AI-Systems». *Revista Ius et Praxis*, vol. 28, n.º 2, págs. 3-24. DOI: https://doi.org/10.4067/S0718-00122022000200003

MONTAGNANI, M. L.; CAVALLO, M. (2021). «Liability and Emerging Digital Technologies: An EU Perspective». *Notre Dame Journal of International & Comparative Law*, vol 11, n.º 2, págs. 208-231 [en línea]. Disponible en: https://scholarship.law.nd.edu/ndjicl/vol11/iss2/4

MONTAGNANI, M. L.; NAJJAR, M. C.; DAVOLA, A. (2024). «The EU Regulatory approach(es) to AI liability, and its Application to the financial services market». *Computer Law and Security Review*, n.º 53. DOI: https://doi.org/10.1016/j.clsr.2024.105984

TANG, R.; SHEN, G.; GUO, C.; CUI, Y. (2022). «SAD: Website Fingerprinting Defense Based on Adversarial Examples». *Security and Communication Networks*, vol. 2022, art. 7330465. DOI: https://doi.org/10.1155/2022/7330465

WAGNER, G. (2023). «Liability Rules for the Digital Age - Aiming for the Brussels Effect» (Forschungsinstitut Für Recht Und Digitale Transformation). SSRN. DOI: https://doi.org/10.2139/ssrn.4320285

WAGNER, G. (2018, December 3). «Robot Liability. Münster Colloquium on EU Law and Digital Economy, Liability for Robotics and the Internet of Things». DOI: https://doi.org/10.5771/9783845294797-25

WARWICK, K. (2019). «Synthetix Response to Oracle Incident. Our response to today's Oracle incident». *Synthetix* [en línea]. Disponible en: https://blog.synthetix.io/response-to-oracle-incident/

Cita recomendada

CALDERÓN MARENCO, EDUARDO ANDRÉS; GARZÓN SOLANO, JIMMY ENRIQUE; SÁNCHEZ SILVEYRA, ROMINA MARIELA; SAL, GUILLERMO OSCAR; RAVELO-FRANCO, GABRIEL (2025). «IResponsabilidad civil del oráculo: intersección entre el derecho privado y los contratos inteligentes». *IDP. Revista de Internet, Derecho y Política*, núm. 42. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i42.43070

Sobre las autorías

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

Doctor en Derecho (Universidad Externado de Colombia) y máster en Derecho de los Negocios Internacionales (Universidad Iberoamericana de México). Investigador posdoctoral en la Universidad Pública de Navarra y la Universidad Americana. Profesor e investigador en la Universidad Cooperativa de Colombia, docente de maestría y doctorado en derecho en Nicaragua y México. Coordinador de cotutelas doctorales, evaluador de revistas indizadas y miembro de comités editoriales internacionales. Codirector de la *Revista Científica de Estudios Sociales*. Investigador junior por el SNCTeI (Colombia) y coordinador general de la Red Iberoamericana de Investigadores e Investigadoras - Nodo Socio Jurídico.

Jimmy Enrique Garzón Solano
Universidad Cooperativa de Colombia
jimmy.garzon@campusucc.edu.co
ORCID: https://orcid.org/0000-0002-6937-5906

Ingeniero de sistemas con amplia experiencia en tecnologías de la información. Graduado en 2008, especializado en Redes de Telecomunicaciones (2013) y magíster en Gestión de TI (2019). Profesor desde 2009 en la Universidad Cooperativa, donde lidera proyectos académicos e investigativos en tecnología y redes. Competente en gestión de infraestructura TI y en la formación de profesionales en el sector tecnológico.

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

Abogada por la Universidad de Concepción del Uruguay, matriculada en el Colegio de la Abogacía de Entre Ríos, Argentina. Maestranda en Derecho Privado por la Universidad Nacional de Rosario. Docente e investigadora de la carrera de Abogacía de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Concepción del Uruguay. Coordinadora por la Universidad de Concepción del Uruguay en la Red Iberoamericana Interdisciplinaria de Investigadores e Investigadoras. Nodo Socio Jurídico.

Guillermo Oscar Sal
Universidad de Concepción del Uruguay, Argentina
drguillermosal@gmail.com
ORCID: https://orcid.org/0009-0003-0292-5197

Abogado por la Universidad Nacional de Lomas de Zamora, Buenos Aires. Maestrando en Derechos Humanos en la Universidad Nacional de Lanús. Mediador Nacional por - Fundación Humanita - Entidad Capacitadora - Habilitación n.º 157 del Registro de Instituciones Formadoras en Mediación. Posgrado de Derecho Comparado entre el Derecho Argentino y el Italiano (Università Degli Studi di Bari – Universidad de Concepción del Uruguay). Docente titular de la cátedra Derecho Privado II y docente investigador en la carrera de Abogacía de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Concepción del Uruguay.

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

Abogado y maestro en Derecho Penal, con diploma de especialización en asesoría de tesis y con estudios en curso de doctorado en Derecho. Profesor a tiempo completo de investigación jurídica en la Facultad de Derecho de la Universidad Continental, de la que también es integrante del Comité de Acreditación para la Calidad. Es investigador de la Red Interdisciplinaria Iberoamericana de Investigadores e Investigadoras Nodo Socio-Jurídico. Profesor de la Maestría en Derecho Penal y Procesal Penal de la Universidad Técnica Particular de Loja (Ecuador). Forma parte del Comité Editorial de la Revista *Ius et Tribunalis*.