

**IMPLEMENTACIÓN DE CONTRATOS INTELIGENTES PARA LA COMPRAVENTA DE
INMUEBLES EN COLOMBIA; RETOS EN MATERIA DE PROTECCIÓN DE DATOS**

**Implementation of Smart Contracts for the Purchase and Sale of Real Estate in Colombia;
Challenges in Data Protection**

ANDRES MAURICIO SANCHEZ OTALORA

JULIANA BEDOYA USMA

TESIS DE MAESTRÍA

Tutor

Enrique Alberto Prieto-Ríos

Título a obtener. Magister en Derecho Corporativo



**Universidad del
Rosario**

COLEGIO MAYOR NUESTRA SEÑORA DEL ROSARIO

FACULTAD DE JURISPRUDENCIA

BOGOTÁ D.C.

JULIO DE 2025

TABLA DE CONTENIDO

CONTENIDO

CAPITULO I: CONCEPTOS BÁSICOS	3
1.1.1. Marco Teórico	3
1.1.2. El Comercio Electrónico en Colombia	3
1.1.3. Contratos Inteligentes, definición y funcionamiento	5
1.1.4. Blockchain y su aplicación en Contratos Inteligentes.	6
CAPITULO II: DERECHO COMPARADO UE Y COLOMBIA	8
2.1. Análisis de la Normativa Colombiana.....	8
2.1.1. Regulación en Colombia sobre Compraventa de Bienes Inmuebles.....	8
2.1.2. Normativa en Colombia sobre Protección de Datos Personales	9
2.2. Consideraciones sobre regulaciones en la Unión Europea- UE.....	11
2.2.1. UE y el Manejo de los Datos Personales.....	11
2.2.2. Compraventa de Inmuebles; Contratos Inteligentes en UE.....	12
2.3. Reflexiones sobre Derecho Comparado UE Y Colombia.....	14
CAPITULO III: RETOS EN LA IMPLEMENTACIÓN DE CONTRATOS INTELIGENTES PARA LA COMPRAVENTA DE INMUEBLES EN COLOMBIA; ENFOQUE EN MATERIA DE PROTECCIÓN DE DATOS	15
CAPITULO IV: CONCLUSIONES	18

RESUMEN

Este trabajo exploramos la implementación de los contratos inteligentes (smarts contracts) para la compraventa de inmuebles en Colombia, analizando su compatibilidad con la normatividad vigente en el país y de cara a los desafíos en materia de protección de datos. Abordamos aspectos como las reglas en la tradición de inmuebles, las posibilidades de automatización mediante blockchain y los restos relacionados con el tratamiento y protección de datos personales. Además, proponemos soluciones para armonizar estas iniciativas de vanguardia con el sistema jurídico colombiano, garantizando la seguridad y la transparencia de las transacciones.

ABSTRACT

In this paper we explore the implementation of smart contracts for the purchase and sale of real estate in Colombia, analyzing their compatibility with the current regulations in the country and in light of the challenges regarding data protection. We address aspects such as the rules in real estate transactions, the possibilities of automation through blockchain and the remains related to the treatment and protection of personal data. Additionally, we propose solutions to harmonize these cutting-edge initiatives with the Colombian legal system, guaranteeing the security and transparency of transactions.

PALABRAS CLAVE

Contratos inteligentes, Compraventa, Comercio electrónico, Habeas data, Tratamiento de Datos personales.

KEYWORDS

Smart contracts, Purchase and sale, Electronic commerce, Habeas data, Processing of personal data.

INTRODUCCIÓN

La creciente digitalización y el desarrollo de tecnologías emergentes viene transformando diversos sectores, entre ellos, el sector inmobiliario. En este contexto los contratos inteligentes- o smart contracts- (en adelante “Contratos Inteligentes”) basados en tecnología blockchain han surgido como una herramienta innovadora con el potencial de cambiar la forma en que se realizan las transacciones, dentro de ellas, las transacciones realizadas con la compraventa de bienes inmuebles. Los contratos inteligentes se desarrollan mediante programación, donde se integran automáticamente las obligaciones, términos y condiciones del acuerdo entre las partes. Al igual que los contratos tradicionales, su contenido puede adaptarse según el marco legal aplicable, permitiendo incluir diversas cláusulas. Así, su ejecución puede ser verificada por la misma plataforma tecnológica, sin necesidad de intervención humana directa. (Leefatt & Cieplak, 2017).

Actualmente, distintos países de la Unión Europea vienen implementando Contratos Inteligentes en la compraventa de bienes inmuebles (Clifford Chance, 2017). Uno de los países más destacados es Estonia siendo pionera en la implementación de los Contratos Inteligentes basados en blockchain en el sector público y privado, facilitando la validación digital de contratos y el registro de propiedades de manera automatizada (Sullivan & Burger, 2017). Francia también es un ejemplo reciente de como este tipo de contrato de vanguardia puede ser implementado con éxito en la compraventa dentro del sector inmobiliario.

Bajo este contexto, en el presente estudio de investigación exploramos la implementación de los Contratos Inteligentes para la compraventa de inmuebles en Colombia, analizando su compatibilidad con la normatividad vigente en el país y de cara a los desafíos en materia de protección de datos. Abordamos aspectos como las reglas en la tradición de inmuebles, las posibilidades de automatización mediante blockchain y los restos relacionados con el tratamiento y protección de datos personales. Además, proponemos soluciones para armonizar estas iniciativas de vanguardia con el sistema jurídico colombiano, garantizando la seguridad y la transparencia de las transacciones.

CAPITULO I: CONCEPTOS BÁSICOS

1.1.1. Marco Teórico

En esta sección presentamos un análisis del comercio electrónico en Colombia, incluyendo su evolución normativa, los conceptos clave establecidos en la Ley 527 de 1999 y su relevancia en la consolidación de un entorno digital seguro. A partir de esta base, se examina la figura de los contratos inteligentes como una nueva forma de manifestación de la voluntad jurídica a través de programación y automatización, y finalmente, se aborda la tecnología blockchain como la infraestructura que permite su ejecución confiable, inmutable y descentralizada. Estos elementos se analizan en conjunto para comprender su interacción dentro del contexto jurídico-tecnológico colombiano.

1.1.2. El Comercio Electrónico en Colombia

El comercio ha trascendido las fronteras físicas para expandirse al mundo digital, donde las transacciones ya no dependen de elementos tangibles, sino de la inmediatez de los datos. El comercio electrónico engloba todas las relaciones comerciales, sean contractuales o no, que se desarrollan a través de mensajes de datos o medios similares (Congreso de Colombia, Ley 527 de 1999, art.2). Esto abarca desde la compraventa de bienes y servicios, hasta acuerdos de distribución, operaciones financieras, contratos de

prestación de servicios, concesiones públicas y transporte de mercancías o pasajeros, consolidándose como un pilar fundamental de la economía moderna.

La evolución del comercio electrónico en Colombia, según Rengifo García (1999) ha estado marcada por la adaptación progresiva del marco normativo. Antes de 1999 el país carecía de una regulación específica, puntual, idónea para los contratos celebrados mediante medios electrónicos, lo que generaba una enorme incertidumbre jurídica. Mientras la tecnología avanzaba, el derecho colombiano no evolucionaba a la misma velocidad. En este contexto, el Congreso de Colombia decidió implementar la Ley Modelo de la CNUDMI sobre Comercio Electrónico por medio de la Ley 527 de 1999, que aborda aspectos claves para el comercio electrónico, como la definición de mensajes de datos, la firma electrónica, la formación de contratos por medios electrónicos, la validez jurídica de los documentos electrónicos, entre otros (Castro & Calonje, 2015; Flórez, 2014).

La Ley 527 nos permite analizar diversos conceptos relacionados. En primer lugar, el Mensaje de Datos se ha entendido como cualquier información que se crea, envía, recibe, almacena o transmite a través de medios electrónicos, ópticos o tecnologías similares (art. 2). Esto incluye entre otros, el intercambio electrónico de datos (EDI), internet, el correo electrónico, el telegrama, el telefax, etc. La Corte Constitucional (2000) en uno de sus fallos, señala que el concepto de mensaje de datos no está ligado a una tecnología particular, permitiendo la adaptación a futuras innovaciones tecnológicas (Sentencia C-662 de 2000).

En segundo lugar, otro concepto relevante que desarrolla la ley 527 es el de la Firma Digital. De acuerdo con la ley, esta firma es un código numérico asociado a un mensaje de datos que, mediante un proceso matemático específico, se relaciona con la clave del remitente y el contenido del mensaje (art. 2). Esto permite verificar que este código fue generado únicamente con la clave del remitente y que el mensaje no ha sido alterado después de su formación. La Corte Constitucional (2006) en Sentencia C-219 de 2015 consideró el alcance del concepto de firma digital al señalar, entre otras cosas que, esta constituye un mecanismo tecnológico que garantiza la autenticidad, integridad y no repudio de los mensajes de datos. Además, precisó que la firma digital debe estar vinculada de manera única al firmante y al documento, asegurando que cualquier alteración posterior pueda ser detectada, lo que otorga validez jurídica dentro del marco normativo colombiano.

De otra parte en clave de formación de contratos, la ley 527 de 1999 establece que los contratos pueden perfeccionarse a través de mensajes de datos, siempre que exista manifestación de voluntad entre las partes, garantizando así su reconocimiento legal. Asimismo, la validez de los documentos electrónicos ha sido reforzada por la jurisprudencia de la Corte Constitucional que destacó su equivalencia funcional con los documentos físicos, siempre que cumplan con los principios de autenticidad, integridad y no repudio (Sentencia C-831 de 2001) De este modo, el marco normativo viene evolucionado para propiciar la seguridad jurídica en las transacciones digitales, fomentando la confianza en el uso de tecnológicas en el ámbito comercial.

En este contexto, el marco normativo colombiano incluyó el principio de equivalencia funcional el cuál es crucial en el contexto de los Contratos Inteligentes, ya que este establece que los mensajes de datos y firmas electrónicas tienen la misma validez jurídica que los documentos físicos, siempre que se garantice su autenticidad e integridad. De acuerdo con Furrer y Miller (2018), de acuerdo con este principio se debe evaluar si un sistema digital puede cumplir con los objetivos de los criterios de sustancia y forma requeridos por la ley para validar una transacción. Si es así, se puede prescindir de los requisitos de forma preservando los aspectos sustanciales del acto jurídico, garantizando que los actos electrónicos tengan la misma función jurídica que los tradicionales. El objetivo principal del principio de equivalencia, en este contexto, es evitar la discriminación contra los medios electrónicos en comparación con las expresiones de voluntad tradicionales. De esta forma, busca preservar la integridad del régimen de obligaciones y contratos privados, ya que la adopción de medios electrónicos representa solo una innovación en la forma de expresar la voluntad en cualquier fase de un acto jurídico y es válida siempre y cuando se mantengan la fiabilidad,

inalterabilidad y rastreabilidad del mecanismo digital utilizado (Corte Constitucional, Sentencia C-831 de 2001)

Como se puede evidenciar, la evolución del comercio en Colombia ha estado marcada por la necesidad de adaptar el marco jurídico a los avances del medio. La Ley 527 de 1997 representa un hito importante en la historia legal de Colombia en lo relativo al manejo de lo digital, asimismo la jurisprudencia constitucional ha sido fundamental para garantizar la validez y seguridad de los documentos electrónicos. La adopción del principio de equivalencia funcional ha permitido que los actos jurídicos realizados por medios electrónicos alcancen el mismo reconocimiento que aquellos celebrados de forma tradicional, aportando al fortalecimiento de la confianza en las transacciones digitales y promoviendo su desarrollo en el ámbito comercial.

1.1.3. Contratos Inteligentes, definición y funcionamiento

En Colombia los contratos han sido entendidos como acuerdos de voluntades entre dos o más partes en donde se establecen obligaciones y derechos recíprocos. El Código Civil colombiano puntualmente establece que “[c]ontrato o convención es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa (...). Cada parte puede ser de una o de muchas personas” (Código Civil, Art. 1495). En el marco del mundo contemporáneo los Contratos Inteligentes representan la materialización de un contrato legal a través de una plataforma digital, estructurado mediante códigos y algoritmos diseñados para verificar y ejecutar de manera automatizada las condiciones de un acuerdo de voluntades (Sahai & Pandey, 2020; Veerpalu, 2019; Reed, 2007).

De esta manera, los Contratos Inteligentes representan un avance significativo en la convergencia entre las nuevas tecnologías y el derecho, permitiendo la creación de acuerdos jurídicamente válidos, pero mucho más ágiles, seguros y eficientes (Durovic & Janssen, 2018). Esta innovación se enmarca en el contexto de la globalización, la digitalización y la inteligencia artificial, que están transformando la forma en que se realizan las transacciones y se establecen las elaciones contractuales (Asaithambi et al, 2024).

Los Contratos Inteligentes se configuran a través de la programación, donde el creador específico, mediante el algoritmo incluye, obligaciones, términos, partes intervinientes, posibles acciones a ejecutar y toda la información relativa al acuerdo entre las partes, organizándola y sistematizándola de forma adecuada. Al igual que un contrato tradicional, sus condiciones pueden variar según el ámbito legal de su aplicación. De modo que, dependiendo de la complejidad o del régimen aplicable, pueden incorporar una amplia variedad de cláusulas y condiciones en su diseño. Así entonces, es posible configurar el contrato de forma que el cumplimiento de las obligaciones de las partes sea verificado por el sistema o plataforma que contiene el contrato inteligente, sin necesidad de la intervención directa de terceros en el procedimiento contractual (Leefatt & Cieplak, 2017).

De este modo, el sistema informático que alberga el contrato inteligente opera conforme a un algoritmo del tipo “*Si entonces*”, es decir, que se ejecuta automáticamente cuando se cumple una condición. Este algoritmo esquematiza anticipadamente las posibles trayectorias que puede tomar la transacción, de acuerdo con la conducta y acciones de las partes intervinientes. Las acciones de estas partes generan nueva información que se introduce en el sistema, y con base en esta información, el programa ejecutará progresivamente nuevos avances en cumplimiento de los términos contractuales pactados inicialmente (Wang et al, 2019). Una vez que el contrato ha sido programado en la plataforma seleccionada por su creador¹, este se introduce en una cadena de bloques con un número de identificación único y se activa

¹ Existen diferentes plataformas para programar contratos inteligentes, la elección depende del caso de uso, los costos y si se busca una cadena de bloques privada o pública. Actualmente la plataforma más usada es Ethereum, aunque se suelen usar otras como Solana, Cardano o BNB Smart Chain (Lawton, 2025).

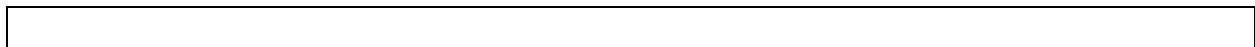
mediante la acción previamente definida por el programados (Leefatt & Cieplak, 2017). Esto permite un avance progresivo en el cumplimiento de las obligaciones y condiciones establecidas, sin necesidad de intervención de terceros.

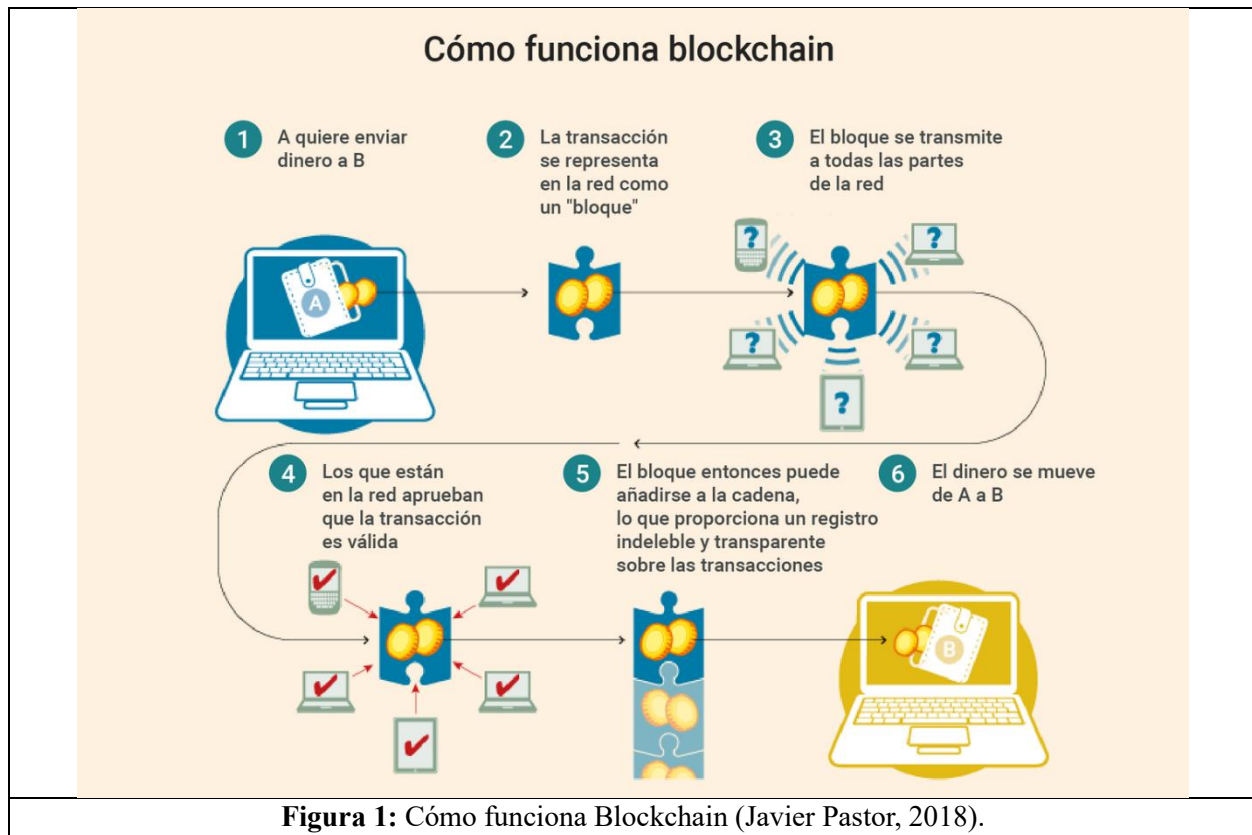
Con miras a una mayor comprensión del asunto, un ejemplo puede ser el contrato de arrendamiento de vivienda programado a través de un contrato inteligente. Las partes pueden acordar los términos y condiciones del contrato, como la duración del arrendamiento, el monto del canon y las responsabilidades asociadas al mantenimiento del inmueble. Una vez que el contrato es programado y se introduce en una plataforma segura, el sistema puede verificar automáticamente el cumplimiento de las condiciones, como el pago oportuno del canon o el cumplimiento de asuntos relativos al mantenimiento del inmueble. Si se cumplen las condiciones, el sistema puede enviar automáticamente una notificación de autorización de acceso a la vivienda a los sistemas de seguridad correspondientes al sistema del edificio si es propiedad horizontal. De igual forma, se puede programar para que, en caso de incumplimientos, el sistema puede aplicar penalidades como el débito automático de intereses moratorios de la cuenta bancaria asociada del arrendatario o del arrendador según el caso (Morales y Pulgarín, 2022).

De esta forma el contrato inteligente garantiza la transparencia, la seguridad y la eficiencia en la ejecución de un contrato de arrendamiento de vivienda. También se convierte en una herramienta innovadora que permite establecer acuerdos de voluntades vinculantes de manera segura y transparente, utilizando tecnología de vanguardia y sustentado en principios que buscan promover la autenticidad y la confianza. De esta manera, el contrato inteligente se presenta como un software que facilita el establecimiento de un acuerdo entre las partes en relación el objeto de contrato utilizando un sistema que va incorporando de manera progresiva la información en una red de blockchain. Ahora, si bien la autoejecución programada de acuerdos puede implementarse en sistemas de gestión de contratos para lograr que un contrato se desarrolle de manera automática, para los efectos que se buscan con los Contratos Inteligentes la mejor opción es implementarlo a través de una plataforma de blockchain debido a que este sistema brinda las características de inmutabilidad, descentralización y autoejecución sin necesidad de terceros, lo cual garantiza la integridad y seguridad del acuerdo de forma autónoma.

1.1.4. Blockchain y su aplicación en Contratos Inteligentes.

La tecnología conocida como “blockchain” es un registro público digital que almacena todas las transacciones efectuadas dentro del sistema que las utiliza, su fortalecimiento se basa en la verificación y el registro de todas las transacciones relacionadas con una cadena específica, sin necesidad de autoridad central que controle el sistema. La confianza se genera a través de las interacciones que se van registrando progresivamente en el programa (Wang et al, 2019).





De esta manera, al incorporar la información de manera progresiva en una red de blockchain, el contrato inteligente garantiza la integridad y la inmutabilidad de los datos, lo que reduce enormemente el riesgo de fraude o manipulación. blockchain juega un papel crucial en los Contratos Inteligentes al ofrecer un registro público y descentralizado donde se documentan todas las transacciones. Esta tecnología asegura la integridad, la transparencia y la seguridad de las transacciones, creando bloques inmutables que contienen registros de datos verificables. La estructura de cadena se compone de bloques, cada uno de los cuales actúa como un contenedor de información sobre una transacción (Pérez, 2019). De este modo, cada bloque es único e inalterable, asegurando que cada transacción se registre como un nuevo dato, la transparencia de las transacciones se garantiza mediante el uso de técnicas criptográficas (Cole, 2019; AdvancedMicroDevices, 2019; Cubillos Velandia y Rincón Cárdenas, 2002).

Esto es realmente revolucionario si se considera que se secuencian progresivamente los bloques que cuentan con una marca de tiempo y cada uno hace referencia al bloque anterior, formando así una cadena vinculada, (Asaithambi et al, 2024). esto permite que la cadena este organizada y que pueda revisar su historial para verificar el estado de la transacción. De modo que, todas las partes involucradas en el contrato tienen acceso a la información en tiempo real, lo que facilita la comunicación y la colaboración. Además, el carácter inmutable de estos registros asegura que no puedan ser modificados de manera arbitraria, sino por lo previamente autorizados y en las condiciones previamente autorizadas, lo que garantiza el cumplimiento de lo pactado y reduce el riesgo de disputas o incumplimientos.

En consecuencia, la tecnología de blockchain elimina la necesidad de una autoridad que valide las transacciones y permite que los Contratos Inteligentes se ejecuten de forma automatizada y fiable, sin requerir confianza previa entre las partes o intervención de intermediarios (Ni, 2024; Werbach & Cornell, 2021, Leefatt & Cieplak, 2017). Los comandos se ejecutan tal como se ha programado (Oleksii Konashevich, 2017; Raskin, 2016)

CAPITULO II: DERECHO COMPARADO UE Y COLOMBIA

2.1. Análisis de la Normativa Colombiana

En esta sección presentamos un análisis comprometido de las normas, leyes, regulaciones, sentencias etc. de la normativa colombiana relacionadas con las áreas de interés, es decir la protección de datos personales y la tradición de inmuebles, de acuerdo con los fines de este trabajo de investigación. Este análisis se concentró en la identificación y examen de las leyes, decretos y regulaciones que rigen estos ámbitos en Colombia.

2.1.1. Regulación en Colombia sobre Compraventa de Bienes Inmuebles

La Compraventa de Bienes Inmuebles y su tradición en Colombia está regulado por el Código Civil colombiano, Ley 84 de 1973, y complementado por normas específicas en materia de registros públicos y notariado. Este marco normativo establece procedimientos, requisitos y efectos legales relacionados con este tipo particular de contrato. En línea con el artículo 1849 del Código Civil Colombiano, la compraventa de bienes inmuebles en Colombia es un contrato mediante el cual una parte (vendedor) transfiere el dominio de un inmueble a otra (comprador) a cambio de un precio determinado.

Para que una Compraventa de Bienes Inmuebles sea válida, es necesario que exista un acuerdo de voluntades entre las partes, en el cual se pacta el objeto del contrato (en este caso la tradición del inmueble) y el precio. Sin embargo, a diferencia de otros contratos, en el caso de los bienes inmuebles la compraventa debe cumplir con formalidades específicas para que tenga plena validez y efectividad.

Uno de los principales requisitos, es que el contrato se formalice mediante escritura pública, otorgada ante Notario, tal como lo exige el artículo 1857 del Código Civil. Posteriormente la escritura debe inscribirse en la Oficina de Registro de Instrumentos Públicos, de acuerdo con el artículo 756 del mismo código. Solo con esta inscripción se perfecciona la tradición y se transfiere el dominio del bien al comprador.

Además, antes de la inscripción del registro, es obligatorio cumplir con ciertos tramites adicionales, como el pago de los impuestos de registro y beneficencia y la obtención de certificados que acrediten la situación jurídica y fiscal del inmueble. Entre ellos se encuentran el Certificado de Tradición y Libertad, que contiene el historial del inmueble, y paz y salvos de impuesto predial y valorización, que certifica que no existen deudas fiscales. Si el inmueble hace parte de una propiedad horizontal, también requiere que se tramite una paz y salvo de administración.

En cuanto a los efectos jurídicos de la compraventa inmobiliaria, es importante destacar que la propiedad del inmueble solo se transfiere una vez que la escritura pública ha sido debidamente inscrita en el Registro de Instrumentos Públicos. Mientras esta diligencia no se encuentre perfeccionada el comprador no podrá ser considerado el propietario frente a terceros. Además, el vendedor tiene la obligación de entregar el bien en las condiciones pactadas y garantizar al comprador el saneamiento por evicción y por vicios ocultos, es decir que el inmueble esté libre de gravámenes ocultos o defectos que impidan su uso adecuado.

De esta manera, el marco normativo que rige la Compraventa de Bienes Inmuebles en Colombia incluye diversas disposiciones normativas. Lo preceptuado en el Código Civil que establece las reglas generales del contrato, lo establecido en el Código de Comercio, que regula aspectos específicos de la compraventa mercantil, lo indicado en la Ley 1579 de 2012, que desarrolla el Estatuto de Registro de Instrumentos Públicos, el Decreto 960 de 1970 y el Decreto 1250 de 1970, que reglamentan la función notarial y el sistema de registro inmobiliario.

En últimas, la regulación en Colombia sobre compraventa de bienes inmuebles cumple una función fundamental en la protección de los derechos de las partes y en la garantía de la seguridad jurídica en las transacciones inmobiliarias. Cumplir con los mencionados requisitos y solemnidades evita litigios, previene fraudes y asegura que la transferencia de dominio se realice de manera efectiva, legítima y transparente.

2.1.2. Normativa en Colombia sobre Protección de Datos Personales

La protección de los datos en la República de Colombia es una obligación que se ha elevado a rango legal y constitucional. En el ordenamiento jurídico colombiano el derecho al habeas data, consagrado en el artículo 15 de la Constitución Política, protege la intimidad personal y familiar, así como el buen nombre de las personas, y les otorga a los individuos la facultad de conocer, actualizar y rectificar la información que sobre ellos repose en bases de datos, tanto públicas como privadas. El habeas data ha sido desarrollado legislativamente a través de las Leyes 1266 de 2008 y 1581 de 2012, las cuales regulan el tratamiento de datos personales, la información crediticia y otros aspectos relacionados con el manejo de la información. En este contexto, el dato personal ha sido descrito en Colombia como “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables” (Ley 1581 de 2012, art.3). Concepto que debe entenderse que se amplía para que pueda asociarse a una persona natural o jurídica (Ley 1266 de 2008, art. 3). Es decir que las empresas también gozan de garantías para la protección de sus datos en lo relativo a su información financiera, crediticia, comercial, etc.

Asimismo, la Ley 1266 de 2008 categoriza los datos según su naturaleza en datos privados, semiprivados y públicos. Ello, con la finalidad de reconocer las implicaciones y retos que suscita el régimen de tratamientos de datos en el país. Conforme a la mencionada ley el dato privado es el que “por ser de naturaleza íntima o reservada solo es relevante para el titular” (Literal h, art. 3). De la misma manera, conforme a la Ley 1581 de 2012 se precisa que el dato privado puede ser entendido como aquella información que es reservada y cuyo acceso sin autorización puede generar consecuencias graves en la vida personal, laboral, financiera, entre otras, del titular de la obligación (art.3).

Frente al dato semiprivado, de conformidad con un fallo proferido por la Corte Constitucional colombiana, corresponde a “[a]quellos que no tienen naturaleza íntima, reservada, ni pública, y que, por ende, su conocimiento puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, un ejemplo de la categoría es del dato financiero y/o crediticio.” (Sentencia C-1011 de 2018). Dentro de esta categoría de datos también se encuentran los nombres, apellidos, tipo y número de identificación, dirección, teléfono (Superintendencia de Industria y Comercio, Resolución 2908 de 2019).

En relación con el dato público, la Ley 1266 de 2008, es clara al determinar que es de naturaleza pública “el dato calificado como tal según los mandatos de la Ley o de la Constitución Política o todos aquellos que no sean privados o semiprivados” (Literal f, art. 3). En este sentido se pronuncia el Decreto 1377 de 2013, al conceptuar sobre dato público, considerando, además, que serán entendidos como datos públicos los relativos a el estado civil de las personas, su profesión, su oficio, su calidad de comerciante o de servidor público (art. 3, Numeral 2). Ambas normativas coinciden en que serán considerados datos públicos los contenidos en registros públicos, documentos públicos, gacetas, boletines oficiales, sentencias judiciales, entre otros.

Ahora bien, en el entendido que la naturaleza es pública por encontrarse en documentos oficiales proferidos por el Estado, es oportuno hacer la salvedad, de que este carácter no se extiende automáticamente a la divulgación que realice el titular de la información. En tal sentido se pronunció la Superintendencia de Industria y Comercio en Colombia al determinar que “[e]s claro que el hecho de que los datos personales de los titulares se encuentren publicados en medios masivos como internet, diarios o periódicos en ninguna medida quiere indicar que los datos sean públicos y que se pueda hacer uso de estos” (Resolución 80305 de 2021). Por lo anterior pese a que la información se encuentre disponible para consulta en internet o diarios o portales abiertos a determinado público, esta no pierde su naturaleza de privada o semiprivada, según el caso. En consecuencia, solo se considera dato público aquel que ha sido expresamente puesto a disposición del público en general mediante actos o instrumentos oficiales del estado.

En lo relativo a la protección de los datos personales, son datos públicos los que ya están disponibles para el público en general como los contenidos en sentencias judiciales, datos de Cámara de Comercio sobre comerciantes y sociedad, serían entonces datos privados, por ejemplo, la dirección del domicilio, el historial médico y de salud, entre otros. Dentro de los datos semiprivados están por ejemplo la información crediticia y financiera, los datos laborales o historial académico, entre otros.

Ahora, en este campo de la protección de los datos personales en Colombia la principal normativa es la Ley 1581 de 2012. Esta regulación establece principios fundamentales para el tratamiento de estos como la transparencia, la seguridad y la confidencialidad. De modo que, los titulares de los datos personales tienen el derecho conocer y controlar su información personal. Esto incluye el derecho de acceso, rectificación, cancelación y oposición al tratamiento de datos personales. El principio de transparencia garantiza que los titulares de los datos puedan acceder a su información personal en cualquier momento y conocer como está siendo utilizada, sin restricciones, ni demoras injustificadas. Este principio está consagrado en el artículo 4 de la mencionada ley.

Otro principio es el principio de seguridad, el cual obliga a quienes manejan datos personales e implementar medidas técnicas, humanas y administrativas para proteger la información contra accesos no autorizados. Este principio busca minimizar los riesgos asociados a la filtración o mal uso de los datos y está regulado por el artículo 4 Literal g de la ley en análisis. Asimismo, la normativa establece el principio de confidencialidad, que impone a los responsables del tratamiento la obligación de garantizar la reserva de la información, salvo autorización expresa del titular o por mandato legal que exija su divulgación. Este principio contenido en el artículo 4 literal h, protege el derecho a la privacidad y restringe el acceso a la información solo al personal autorizado.

Además de los mencionados principios, la ley reconoce derechos fundamentales a los titulares de datos como el derecho de acceso, que les permite conocer que información suya está siendo tratada y con qué finalidad, según lo dispuesto en el artículo 8 numeral 1 de la ley 1581 de 2012. También se observa el derecho de rectificación que faculta a los titulares para solicitar la corrección y actualización de datos inexactos o desactualizados, conforme al artículo 8 numeral 2 de la misma.

Otro derecho fundamental es el derecho de eliminación o supresión de datos, que permite a los titulares solicitar la eliminación de su información cuando el tratamiento no respete los principios legales o cuando ya haya cumplido su finalidad. Esta prerrogativa se encuentra regulada en el artículo 8 numeral 4 de la Ley 1581. Por último, el derecho de oposición otorga a los titulares la posibilidad de negarse al tratamiento de sus datos cuando existan razones legítimas para hacerlo, salvo que una obligación legal impida dicha oposición, conforme al artículo 8 numeral 6. La Superintendencia de Industria y Comercio SIC es la autoridad competente y encargada de velar por el cumplimiento de estas normativas, la entidad tiene la capacidad de imponer sanciones a aquellos que incumplan con las disposiciones sobre la protección de datos personales. Sobre lo relativo a los principios de protección de datos personales, la SIC se ha pronunciado, según la entidad los responsables del tratamiento de datos personales en los contratos de compraventa de inmuebles deben informar a los titulares la finalidad del tratamiento de estos, así como las obligaciones del responsable y los derechos de los titulares al respecto (Concepto 18039 de 2014). En

resumen, la protección de datos personales en el país es un tema de amplia relevancia que requiere la atención y el cumplimiento de las disposiciones legal que garanticen la privacidad y la seguridad de la información personal.

2.2. Consideraciones sobre regulaciones en la Unión Europea- UE

En este aparte presentamos observaciones sobre las regulaciones vigentes en la Unión Europea en materia de protección de datos personales, Contratos Inteligentes y compraventa de inmuebles con blockchain. En este análisis nos centramos en la identificación y examen de las directivas², reglamentos³ y normativas que rigen estas áreas en la UE, con especial atención a la Ley de Protección de Datos (GDPR) y otras regulaciones relevantes (Unión Europea, 2025).

2.2.1. UE y el Manejo de los Datos Personales

A nivel internacional, el modelo de protección de datos personales adoptado por la Unión Europea es ampliamente reconocido como un hito legislativo y un referente global en materia de privacidad. Sus altos estándares buscan garantizar una protección sólida y efectiva de la información personal, convirtiéndose en guía para otras jurisdicciones en el diseño de políticas y marcos regulatorios. Esto se debe, en parte, a que la normativa europea, particularmente la Directiva sobre protección de datos de la Unión Europea establece que el intercambio de información entre empresas europeas y organizaciones ubicadas en terceros países solo puede realizarse si estos ofrecen niveles de protección equivalentes (OEA, 2011). En consecuencia, el alcance de la protección otorgada a los datos personales originados en la Unión Europea se ha proyectado más allá de sus fronteras, extendiendo su influencia normativa a escala global.

El marco más importante de protección de datos en la UE es el Reglamento General de Protección de Datos (RGPD) conocido como GDPR (General Data Protection Regulation por sus siglas en inglés) que entró en vigor el 25 de mayo de 2018. Este reglamento establece una serie de obligaciones para las empresas, organismos públicos y cualquier entidad que maneje datos personales, tanto dentro de la UE como fuera de ella, si ofrecen bienes o servicios a los ciudadanos de la UE.

El RGPD refuerza los derechos de los individuos sobre sus datos personales, dándoles mayor control sobre cómo se recopilan, almacenan, utilizan. Los derechos incluyen: I) derecho de acceso: el individuo tiene derecho a saber que datos personales están siendo procesados. II) derecho a la rectificación: si los datos son incorrectos se puede solicitar que se corrijan. III) derecho a la eliminación: permite solicitar la eliminación de los datos, cuando ya no sean necesarios o si se retira el consentimiento, IV) derecho a la portabilidad de datos: permite obtener y transmitir a un tercero la información, y V) derecho a la oposición: los individuos pueden oponerse al procesamiento de sus datos en determinadas situaciones.

Además, el RGPD exige que las empresas y organizaciones obtengan un consentimiento explícito e informado de los usuarios antes de procesar sus datos personales. Este consentimiento debe ser fácil de retirar en cualquier momento, asimismo, las organizaciones que manejan datos personales deben ser transparentes en cuando a prácticas de procesamiento de datos y deben documentar todos los pasos que

² Las directivas son actos legislativos en los cuales se establecen objetivos que todos los países de la UE deben cumplir.

³ Los reglamentos son actos legislativos vinculantes. Deben aplicarse en su integridad en toda la UE.

toman para proteger la información personal. Esto incluye la implementación de medidas adecuadas de seguridad y la designación de un delegado de protección de datos (DPO) en ciertas circunstancias.

En casos donde el procesamiento de datos pueda suponer un alto riesgo para los derechos y libertades de los individuos (como el caso de datos sensibles) se requiere realizar una evaluación de impacto en la protección de datos (DPIA, por sus siglas en inglés). LA UE ha establecido normativas estrictas para la transferencia de datos personales fuera de la UE. Solo se permite el envío a países que aseguren un nivel adecuado de protección de datos, o bien mediante mecanismos específicos, como las cláusulas contractuales estándar, el acuerdo con el Escudo de Privacidad UE-EE. UU (que fue invalidado en 2020) o través de decisiones de adecuación por parte de la Comisión Europea.

De la misma manera, el Reglamento General de Protección de Datos establece sanciones severas en caso de incumplimiento de sus normas. Las multas pueden llevar hasta el 4% de la facturación global anual de la empresa o 20 millones de euros (el monto mayor). Esto subraya la importancia de cumplir a cabalidad con las normativas de protección de datos. Además del RGPD, existen otras normativas relacionadas como la Directiva sobre Privacidad en las Comunicaciones Electrónicas (Directiva ePrivacy) que regula aspectos específicos de la privacidad en las telecomunicaciones, como el uso de cookies en los sitios web y la gestión de la información personal en las comunicaciones electrónicas.

No obstante, el robusto fundamento normativo que acompaña la protección de dato de cara a lo electrónico en UE, la constante evolución tecnológica, el uso de la inteligencia artificial, el Big Data y las amenazas cibernéticas, requieren constantes desafíos y se exige que los marcos legales deben adaptarse rápidamente. Actualmente se estudia la posibilidad de actualizar las normativas mencionadas para hacer frente a los avances tecnológicos y garantizar que los datos personales sigan estando protegidos de manera efectiva. En resumen, la protección de datos personales en la Unión Europea UE está regulada por un marco legal, amplio y evolutivo, diseñado para garantizar la privacidad de las personas en un mundo cada vez más digitalizado y globalizado.

2.2.2. Compraventa de Inmuebles: Contratos Inteligentes en UE

La Compraventa de Bienes Inmuebles dentro de la Unión Europea se encuentra reglamentada por un marco normativo, sujeta tanto a las legislaciones nacionales de cada Estado como a las regulaciones comunitarias. Uno de los principios fundamentales en este ámbito es la libre circulación de capitales establecida en el artículo 63 del Tratado de Funcionamiento de la Unión Europea (TFUE) que permite que los ciudadanos de la UE adquirir propiedades en cualquier país miembro sin restricciones discriminatorias.

A pesar de este marco de apertura, cada país mantiene su propia legislación en materia inmobiliaria, lo que implica diferencias significativas en los requisitos administrativos y fiscales. Por ejemplo, en España la compraventa debe formalizarse mediante escritura pública ante notario en el Registro de la Propiedad (Ley Hipotecaria, Decreto 8 de 1946). En Francia, la firma de un contrato preliminar o *Compromis de Vente* es una práctica habitual, regulada por su Código Civil. En Alemania por su parte, la validez de la compraventa depende de la intervención notarial obligatoria, conforme al *Bürgerliches Gesetzbuch* (Código Civil Alemán). En términos generales, los compradores y vendedores deben cumplir con requisitos relacionados con la identificación de las partes, la transparencia en las transacciones y la verificación de legalidad del bien inmueble.

El aspecto fiscal de la compraventa también varía según el país. Existen impuestos como el Impuesto sobre Transmisiones Patrimoniales (ITP) en España, regulado por el Real Decreto Legislativo 1/1993. En el caso de las propiedades nuevas, el Impuesto sobre el Valor Añadido (IVA) se aplica en la mayoría de los países de la UE, conforme a la Directiva 2006/112/CE del Consejo sobre sistema común del

IVA. Adicionalmente, para garantizar la seguridad jurídica de las transacciones, la UE ha promovido normativas de protección al comprador, especialmente en la adquisición de viviendas transfronterizas. La Directiva 2011/83/ UE sobre los derechos de los consumidores establece ciertos derechos de cancelación y transparencia en la información contractual. Además, la jurisprudencia del Tribunal de Justicia de la Unión Europea ha reforzado la protección de las cláusulas abusivas en los contratos inmobiliarios, como en la Sentencia C- 415/11 (Caso Aziz) que se incluyó en las regulaciones de varios Estados miembros.

De la misma manera, dentro de la Compraventa de Bienes Inmuebles dentro de la UE se exige garantizar la protección de los datos personales de las partes involucradas. De acuerdo con el Reglamento General de Protección de Datos- Reglamento UE 2016/ 678 cualquier tratamiento de información personal, como datos de identidad, situación financiera o registros disciales, debe realizarse con estrictas medidas de seguridad y con el consentimiento expreso de los titulares.

Ello implica que, notarios, bancos, agentes inmobiliarios y registros de propiedad deben cumplir con los principios de transparencia, minimización de dato y confidencialidad, evitando usos indebidos o accesos no autorizados. Asimismo, los compradores y vendedores tienen derecho a conocer, gestionar, y solicitar la corrección o eliminación de sus datos cuando resulte necesario. Adicionalmente, países como España, la Ley Orgánica de Protección de Datos Personales establece la responsabilidad de los operadores inmobiliarios en la implementación de medidas de seguridad que garanticen la integridad y veracidad de los datos procesados (Saul Bautista & Galvis Cano, 2019). En este sentido, la gestión de la información en el marco de la compraventa debe alinearse con los principios de transparencia y consentimiento informado.

Ahora, en lo relativo al uso de los Contratos Inteligentes en la compraventa de inmuebles dentro de la Unión Europea este ha avanzado en países con marcos regulatorios más abiertos a la digitalización y la tecnología, como Estonia, Francia y los países bajos (Clifford Chance, 2017). Estonia en particular, ha sido pionera en la implementación de los Contratos Inteligentes basados en blockchain en el sector público y privado, facilitando la validación digital de contratos y el registro de propiedades de manera automatizada (Sullivan & Burger, 2017). Francia ha creado normativas que permiten el uso de Contratos Inteligentes en diversas transacciones financieras e inmobiliarias, aunque con ciertas restricciones, como la obligatoriedad de intervención notarial en algunos casos (Chub, 2019). Por su parte, en los países bajos, la adopción de blockchain en el sector inmobiliario viene en aumento, con iniciativas para integrar estos contratos en los registros de propiedad (Veuger, 2020).

A nivel normativo, la Unión Europea ha impulsado el desarrollo de un marco regulatorio para la tecnología blockchain y los Contratos Inteligentes, con iniciativas como el Reglamento sobre Mercados de Criptoactivos (MiCA)- Reglamento UE 2023/ 1114 que establece directrices para la transparencia y seguridad en el uso de la tecnología blockchain en operaciones comerciales. Además, la Ley de Datos de la UE- Propuesta de Reglamento UE 2022/868 incluye disposiciones puntuales sobre la automatización de contratos digitales, con miras a que los Contratos Inteligentes cumplan con los requisitos de seguridad, interoperabilidad y acceso equitativo a la información.

Además, el RGPD desarrolla el tratamiento de datos personales en los Contratos Inteligentes exigiendo el consentimiento explícito del titular para la recopilación, almacenamiento y uso de su información (Casolari et al, 2023; Unión Europea, 2022). Esto significa que, en transacciones inmobiliarias que utilicen tecnología blockchain, los datos de compradores y vendedores no pueden ser procesados automáticamente sin una autorización clara y verificable. Además, las partes deben ser informadas sobre el propósito del tratamiento y los mecanismos para ejercer sus derechos de acceso, rectificación o eliminación de su información.

En síntesis, la Compraventa de Bienes Inmuebles dentro de la Unión Europea se encuentra amparada por un sólido marco legal que propicia la libre circulación de capitales y la seguridad jurídica, garantizando que los ciudadanos europeos de cualquier estado puedan adquirir propiedades en otro país

miembro sin restricciones discriminatorias. Sin embargo, a pesar de esta apertura subsisten diferencias importantes entre países, en cuanto a impuestos y formalidades.

De modo que, la compraventa de bienes inmuebles es un proceso complejo que involucra múltiples regulaciones en materia de transparencia, seguridad jurídica y protección de datos personales. Si bien la implementación de los Contratos Inteligentes representa una oportunidad de modernizar el sector, también plantea desafíos. Para garantizar la viabilidad de estas tecnologías, es necesario desarrollar marcos regulatorios adaptados a la era digital que equilibren la eficiencia de los Contratos Inteligentes con los derechos fundamentales de los ciudadanos.

2.3. Reflexiones sobre Derecho Comparado UE Y Colombia

En este aparte, adoptaremos el enfoque metodológico de los formantes (formants approach en inglés), propuesto por Pier Giuseppe Monateri, para analizar comparativamente los sistemas jurídicos. Este enfoque considera al Derecho como una construcción dinámica formada por diversos actores y fuentes como la legislación, la jurisprudencia, la doctrina, y otras fuentes, que interactúan entre sí en la configuración de los ordenamientos jurídicos. A través de esta perspectiva, buscamos identificar y descomponer dichos elementos en los sistemas legales de la Unión Europea y de Colombia, con el fin de alcanzar una comprensión más profunda de sus estructuras internas, así como de las similitudes y diferencias que los caracterizan en el plano comparado (Monateri, 2012).

El derecho comparado en materia de compraventa de bienes inmuebles entre Colombia y la Unión Europea revela diferencias que merecen ser examinadas, en cuanto a la regulación, formalidades y seguridad jurídica. Mientras Colombia sigue un sistema basado en la tradición jurídica del derecho civil con enfoque formalista, en la Unión Europea coexisten distintos regímenes dependiendo del país, con tendencias a la digitalización y simplificación de procesos. Estas disparidades tienen sus implicaciones en la protección de los compradores y la seguridad de las transacciones inmobiliarias.

En Colombia como se ha decantado, la compraventa de inmuebles está regulada por el Código Civil y otras normas complementarias que exigen el cumplimiento de ciertas solemnidades. A diferencia de los contratos consensuales, que se perfeccionan con la entrega de la cosa, los contratos de bienes inmuebles deben cumplir con las formalidades específicas para ser válidos, como lo establece el artículo 1500 del Código Civil. En este caso, la tradición es esencial, según lo dispuesto en el artículo 740 del mismo código.

Además, el artículo 745 exige un título traslativo de dominio que cumpla con las formalidades requeridas y esté libre de vicios de consentimiento. De la misma manera, el artículo 1857 del referido código señala que la compraventa de bienes inmuebles no se perfecciona hasta que se otorgue la escritura pública correspondiente. Finalmente, dentro de las exigencias está que una vez se efectuó la tradición de pleno derecho de dominio, es necesario inscribir el título en la Oficina de Registro de Instrumentos Públicos, esta inscripción resulta crucial para transferir la posesión efectiva del derecho al comprador.

En consecuencia, se puede concluir que la normativa y la estructura relacionada, son en su forma actual, incompatibles con la aplicación de Contratos Inteligentes en este tipo de procedimientos. Ninguna plataforma puede perfeccionar una compraventa de bienes raíces ni efectuar la tradición de pleno derecho de dominio sin realizar la correspondiente escritura pública y sin pasar por el mencionado registro, lo que imposibilita culminar con éxito la transacción.

En contraste, en la Unión Europea no existe un marco normativo unificado para la compraventa inmobiliaria, ya que cada país regula estos contratos conforme a su tradición jurídica. Sin embargo, se observa una tendencia general hacia la simplificación de procesos mediante la digitalización de los registros y la automatización de los trámites. Por ejemplo, el caso de Estonia en donde han implementado sistemas

de registro digital de propiedades que permiten transacciones rápidas y seguras a través de plataformas electrónicas, minimizando costos y tiempos de espera. En consecuencia, se ve una marcada inclinación hacia la adopción de los Contratos Inteligentes en el ámbito inmobiliario.

En conclusión, aunque tanto Colombia como la Unión Europea buscan garantizar la seguridad en las transacciones inmobiliarias, las diferencias en los avances normativos sugieren una distancia importante. Mientras Colombia mantiene un sistema de formalidades y centrado en notarías y registros, en la UE se observa una evolución en desarrollo hacia la digitalización y protección proactiva del comprador. La adopción de mejores prácticas internacionales podría beneficiar a Colombia en términos de agilidad, transparencia en la compraventa de inmuebles y modernización.

CAPITULO III: RETOS EN LA IMPLEMENTACIÓN DE CONTRATOS INTELIGENTES PARA LA COMPRAVENTA DE INMUEBLES EN COLOMBIA; ENFOQUE EN MATERIA DE PROTECCIÓN DE DATOS

En esta sección abordamos los principales retos en la implementación de Contratos Inteligentes para la compraventa de inmuebles en Colombia, con un enfoque específico en la protección de datos personales, así como, las dificultades técnicas, y jurídicas que surgen al integrar tecnologías emergentes con la normativa colombiana.

La adopción de Contratos Inteligentes en el ámbito de la compraventa de inmuebles en Colombia representa una transformación significativa en la forma de celebrar y ejecutar negocios jurídicos. Sin embargo, su implementación plantea importantes desafíos en materia de protección de datos personales, especialmente a la luz de la normativa colombiana y los estándares internacionales. En primer lugar, es imprescindible obtener una autorización válida e informada por parte del titular de los datos antes de incorporar su información personal en un contrato inteligente. Además, se evidencia una tensión normativa entre el derecho al olvido, y la naturaleza misma de los Contratos Inteligentes, caracterizados por su inmutabilidad y permanencia en el tiempo. Otro reto relevante es la transferencia internacional de datos, limitada legalmente a países que garanticen niveles adecuados de protección, lo cual se complica en entornos descentralizados y transfronterizos. Adicionalmente, se exige que, previo a la creación de este tipo de contratos, se adopten medidas técnicas y jurídicas apropiadas que permitan demostrar el cumplimiento normativo, como lo son, el uso de técnicas de cifrado.

Ahora bien, desde una perspectiva de seguridad de la información, el consentimiento refuerza la transparencia y la confianza en la gestión de datos, permitiendo a las organizaciones generar mecanismos adecuados para su protección. Su adecuada implementación reduce el riesgo de accesos no autorizados, minimiza el uso indebido de información sensible y fortalece el cumplimiento normativo. Además, al limitar el tratamiento de datos únicamente a los fines acordados, se previenen vulnerabilidades asociadas a la sobre exposición de información, como lo son la divulgación de datos de contacto, o de información financiera a terceros no autorizados.

De conformidad con la Corte Constitucional, la clasificación de datos según su naturaleza, -asunto decantando en los capítulos anteriores- tiene un efecto práctico aplicable a los “límites a su divulgación”, toda vez que, dependiendo de la naturaleza, se requerirá o no autorización para el tratamiento (Sentencia T-450 del 2022). En este sentido, en lo que respecta a datos privados y semiprivados el régimen de protección de datos personales dispone tanto para Colombia como en la Unión Europea, que, para el tratamiento de la información personal, se solicite autorización del titular. Por otro lado, los datos de naturaleza pública no se encuentran sujetos al cumplimiento de esta disposición.

En el ordenamiento jurídico colombiano, el literal a) del artículo 3 de la Ley 1581 de 2012 indica que, la autorización, se refiere al consentimiento otorgado de manera previa, expresa e informada por el

titular, permitiendo así el tratamiento de los datos personales. Por su parte el RGPD determina que el consentimiento debe ser otorgado de manera libre, específica, informada e inequívoca, a través de una solicitud redactada en lenguaje claro y comprensible.

Adicionalmente la Ley Orgánica de Protección de Datos de España, presupone que dentro de los deberes del responsable de la información se encuentra el de demostrar que se obtuvo el consentimiento del titular. Salazar Bautista & Galvis Cano (2019) al analizar esta legislación española destacan la obligación de los operadores de garantizar la seguridad de los datos y la legalidad del consentimiento. Lo que resulta interesante de esta normativa europea es que consolida la carga de la prueba al responsable del tratamiento, lo que refuerza el principio de responsabilidad proactiva en la gestión de datos personales.

En relación con el deber de solicitar la autorización para el tratamiento de datos personales, es fundamental destacar que es un requisito legal imprescindible y cuya omisión podría acarrear consecuencias graves en términos de cumplimiento normativo. Sobre el consentimiento en este contexto, la Corte Constitucional se ha pronunciado de la siguiente forma:

“El consentimiento del titular de la información es un presupuesto para la legitimidad constitucional de los procesos de administración de datos personales, tratándose de un consentimiento calificado, ya que debe ser previo, esto es, que la autorización debe ser suministrada en una etapa anterior a la incorporación del dato, expreso, en la medida que debe ser inequívoco, e informado, toda vez que el titular no solo debe aceptar el tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización” (Sentencia C-748 de 2011).

En consonancia, la autorización a través de un contrato inteligente debe garantizar que el titular tuvo pleno conocimiento de lo allí consentido, de tal forma que, el consentimiento se consolida como un presupuesto para el tratamiento de la información, lo cual implica una clara prohibición al tratamiento de información que no ha sido debidamente autorizada por su titular (Catchlove, 2017). En este sentido los contratos deben diseñarse con protocolos que aseguren la trazabilidad del consentimiento, evitando que se comprometa el derecho fundamental a la privacidad. De esta manera se logra un equilibrio entre eficiencia y garantía de derechos.

Sin embargo, esta prohibición no es absoluta, ya que como señala Cabezas Azuero (2023) los datos que se consideran públicos pueden ser procesados sin requerir la autorización de su propietario. Ello encuentra sustento en lo preceptuado en el Decreto 1377 de 2013 que señala que los datos personales en fuentes públicas, sin importar el medio a través del cual se acceda y que se entienden como datos o bases accesibles al público, pueden ser procesados por cualquier persona, siempre que, por su naturaleza, sean considerados datos públicos (art.5).

En base a lo expuesto, los requisitos que establecen la obligación de solicitar el consentimiento para el tratamiento de la información personal solo son aplicables a aquellos datos cuya naturaleza sea privada o semiprivada, es decir aquellos que no se encuentran disponibles en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva, o que su divulgación podría afectar al titular. En ese sentido, para los datos de naturaleza pública no es necesario obtener consentimiento por parte del titular, ya que su procesamiento se considera legítimo sin esta autorización.

Asimismo, el Decreto 1377 de 2013, normativa en análisis, en su artículo 7, establece de manera clara las formas en que se puede obtener la autorización que avale la voluntad incuestionable del titular de dar su permiso para el tratamiento de sus datos personales. Es así como, de acuerdo con la normativa vigente la autorización debe ser una manifestación clara y efectiva de parte del titular de los datos que

evidencie, sin lugar a duda, su consentimiento. En este sentido, “el silencio, la no acción o la inacción del individuo no constituye consentimiento” (Superintendencia de Industria y Comercio, Resolución 76538 de 2019). En consecuencia, es esencial que antes de proceder con el tratamiento de determinado dato, se obtenga una autorización que cumpla con lo ya esbozado y que se encuentre plenamente documentado por parte del titular. En lo concerniente al derecho al olvido, la Ley 1581 de 2012, entre sus preceptos consagra el derecho del titular de la información, para que tenga la posibilidad de, si a bien lo considere, solicite la supresión del dato. Esta facultad encuentra su fundamento en el derecho al olvido, que según la Corte Constitucional se consolida como una garantía que le permite al titular de la información solicitar la supresión de su información, de tal forma que esta no tenga una vigencia limitada (Sentencia C-748 de 2011).

A nivel normativo, el derecho al olvido se aplica predominantemente a la información financiera, lo anterior en la medida que, el párrafo del artículo 13 de la Ley 2157 de 2021 hace referencia únicamente a la caducidad de la información negativa reportada en los bancos de datos de los operadores de información (reporte negativo realizado ante centrales de riesgo). Sin embargo, con la finalidad de ampliar el ámbito de aplicación del mencionado derecho, la Corte Constitucional fundamentándose en el artículo 15 de la Constitución Política ha dictaminado que este derecho también debe extenderse a la información contenida en bancos de datos y archivos de entidades públicas y privadas, independientemente de si esta es de carácter financiero o no lo es (Muñoz Losada, 2020).

Actualmente, la Superintendencia de Industria y Comercio, como autoridad en la materia y en su rol de autoridad en la protección de datos personales, ha establecido un precedente en cuanto al cumplimiento de la normativa sobre Habeas Data. En este sentido ha determinado que debe garantizarse el ejercicio del derecho a la supresión de la información. Así lo señala al indicar que, conforme a los principios que rigen la gestión de datos personales, los titulares tienen la facultad de solicitar la eliminación de sus datos registrados en base de datos (SIC, Resolución 68753 de 2023).

De lo anterior es claro que, para dar cumplimiento a la normativa vigente, el titular del derecho debe poder ejercer su derecho de supresión de información, ello contrasta con los cimientos de los Contratos Inteligentes. Toda vez que, los Contratos Inteligentes son valorados especialmente por su inalterabilidad y vocación de permanecer en el tiempo, características que buscan garantizar que los datos que se almacenan en los bloques no puedan ser modificados y/o eliminados, con fines de seguridad, integridad y transparencia (Rincón Cárdenas & Martínez Molano, 2022; Rincón Cárdenas, 2006). De tal forma que un Contrato Inteligente está pensado para, una vez desplegado y validado en blockchain permanezca invariante (AEPD, 2022; Sahai & Pandey, 2020). Este choque frontal entre el derecho de modificación o supresión de datos y la inalterabilidad del dato en blockchain (Flores, 2023) representa un riesgo de incumplimiento a la normativa, en la medida de que, una vez registrados los datos en el contrato, es información será inalterable. Por otra parte, es indispensable considerar que los Contratos Inteligentes, ejecutados a través de tecnología blockchain, a menudo requieren el intercambio de datos entre múltiples jurisdicciones (Miranda Guzmán, 2023). Al respecto el ordenamiento jurídico colombiano establece la prohibición de transferencias internacionales de información personal “a países que no proporcionen niveles adecuados de protección de datos” (Congreso de Colombia, Ley 1581 de 2012, art. 26). La mencionada norma distingue que solo podrá transferirse información a países que cumplan con ciertos criterios y/o estándares señalados en la referida ley. La Corte Constitucional señaló los criterios que deben obedecerse mediante sentencia, en donde precisó que:

“(…) se entenderá que un país cuenta con los elementos o estándares de garantía necesarios para garantizar un nivel adecuado de protección de datos personales, si su legislación cuenta, con unos principios, que abarquen las obligaciones y derechos de las partes (titular del acto, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos de datos personales) y de los datos (calidad

del dato, seguridad técnica) y con un procedimiento de protección de datos que involucre mecanismos y autoridades que efectivicen la protección de la información (..) (Sentencia. C-748 de 2011)

Con la finalidad de garantizar que es de estricto cumplimiento esta obligación, en el Capítulo Tercero del Título V de la Circular Única de la Superintendencia de Industria y Comercio, se encuentra fijada la lista de países que reúnen los estándares y criterios fijados por la Corte. (SIC, 2017) como, por ejemplo, los países de la Unión Europea. Ahora bien, junto con estas directrices acompañan una serie de excepciones por ejemplo la establecida en la Ley 1581 de 2012 que establece que solo se aplicará prohibición cuando la transferencia se necesaria para la ejecución de un contrato entre titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se verifique la aprobación del titular.

3.1. El principio de responsabilidad demostrada y el cifrado con clave: medidas para garantizar el cumplimiento normativo

En Colombia y en la Unión Europea, el principio de responsabilidad demostrada es primordial dentro del análisis de la protección de datos personales. En ambos contextos, el principio exige que los responsables del tratamiento de datos se comprometan con seriedad en el desarrollo de estos procesos, cumpliendo con la normativa asociada y generando mecanismos para sustentar y demostrar su cumplimiento en cualquier tiempo, de manera verificable. Esto garantiza la seguridad jurídica y da tranquilidad a los titulares de los datos personales.

En el marco de este principio, la autorregulación cobra un papel relevante a la hora de implementar el régimen de datos personales. Por ello, para reducir los riesgos derivados al incumplimiento de la normativa en la materia, antes de la creación de los Contratos Inteligentes es fundamental considerar la adopción de medidas apropiadas y efectivas. Estas deben ser adecuadas, correctas, útiles, oportunas y eficientes, con el propósito de cumplir los requerimientos legales para el tratamiento de datos personales (Superintendencia de Industria y Comercio, 2021).

Una de las medidas que puede adaptarse es el uso de métodos de cifrado con clave secreta. De conformidad con la Superintendencia de Industria y Comercio, para la protección de la información personal es posible cifrar la información, de tal forma que se establezca una clave de propiedad de las partes para descifrar el conjunto de datos de carácter personal (SIC, 2018). Sobre el asunto se ha pronunciado la Agencia Española de Protección de Datos quien enfatizo en que la utilización del cifrado es recomendable para cubrir estos desafíos y que en ninguna manera la utilización del cifrado elimine la naturaleza de dato de carácter personal, por tanto, prevalecen todas las obligaciones en materia de protección de los datos (AEDP: 2019). No obstante, esta medida permite a la hora de realizar una transferencia internacional de datos de las partes que estas cuenten con una mayor garantía de seguridad.

CAPITULO IV: CONCLUSIONES

Los contratos de compraventa de bienes inmuebles en Colombia actualmente se encuentran regulados por un marco regulatorio estricto y lleno de formalismos, con disposiciones que datan de 1973, con el Código Civil, complementado con otras normativas que también conllevan sus rigorismos. En consecuencia, el ordenamiento jurídico vigente y la estructura institucional que actualmente existe no permiten la implementación de Contratos Inteligentes en compraventas del campo inmobiliario. Dado que este tipo de contratos en el país exigen para su perfeccionamiento que el acuerdo de voluntades sea elevado a escritura pública y posteriormente dicha escritura debe ser allegada al Registro de Instrumentos Público, para que se perfeccione la transferencia del derecho de dominio. La ausencia de una herramienta que permita la digitalización del proceso impide la ejecución valida de este tipo de transacciones.

El derecho debe adaptarse a los cambios de la sociedad, toda vez que los cambios sociales son una fuente de derecho, en un mundo cada vez más hiperconectado y globalizado los Contratos Inteligentes se levantan como una conciliación entre el derecho y las nuevas tecnologías. No obstante, los formalismos exigidos en Colombia para la formalización de la compraventa de un bien inmueble demandan que se ejecuten cambios estructurales que permitan que se adopten este tipo de Contratos Inteligentes de modo progresivo y que a la postre, se establezcan mecanismos que posibiliten la interoperabilidad entre los sistemas emergentes y los sistemas tradicionales.

En Colombia, para poder lograr implementar este tipo de iniciativas de vanguardia asociadas a blockchain es necesario superar algunos desafíos en materia de protección de datos personales. Uno de los retos que se suscitan en el relacionado al consentimiento que como se decantó debe ser previo y verificable, debiéndose integral en las etapas previas al contrato, ya que por ser una plataforma en donde se consignaran los datos en bloque, para poder tratarlos ahí el consentimiento debe generarse de manera documentada previamente al inicio del ejercicio. Ello con el fin de armonizar la operatividad de los Contratos Inteligentes con las normas ya existentes en Colombia sobre protección de datos personales.

De la misma manera, el análisis reveló que, existen tensiones entre el derecho al olvido reconocido en Colombia y la inmutabilidad, característica de los Contratos Inteligentes. Una de las fortalezas de los Contratos Inteligentes es que inmutabilidad garantiza transparencia y seguridad, pero la ley colombiana ha sido enfática en que el titular tiene no solo el derecho al olvido sino el derecho a la supresión de sus datos personales. Asimismo, otro reto importante se relaciona con la transferencia internacional de datos, este principio decanta que en este tipo de ejercicios por tratarse de comercio electrónico se eliminan las distancias físicas, por lo que un Contrato Inteligente exigirá garantizar que el contrato que se origine respete y cumpla los requisitos normativos de todas las jurisdicciones relacionadas con la transacción.

REFERENCIAS BIBLIOGRÁFICAS

- AdvancedMicroDevices. (2019). *Descripción de la Cadena de Bloques*. <https://www.amd.com/es/technologies/blockchain-explained>
- AEPD. (2019, noviembre 15). *Cifrado y Privacidad: Cifrado en el RGPD* | AEPD. <https://www.aepd.es/prensa-y-comunicacion/blog/cifrado-y-privacidad-cifrado-en-el-rgpd>
- AEPD. (2022, marzo 14). *Blockchain (III): Smart contracts y datos personales* | AEPD. <https://www.aepd.es/prensa-y-comunicacion/blog/blockchain-iii-smart-contracts-y-datos-personales>
- AEPD. (2023a, noviembre 10). *Principios* | AEPD. <https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/principios>
- AEPD. (2023b, noviembre 13). *Protección de datos por defecto* | AEPD. <https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/proteccion-de-datos-por-defecto>
- AEPD. (2024, agosto 8). *Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales* | AEPD. <https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/garantias-transferencias-datos-personales>
- Alessandri Rodríguez, A., Somarriva Undurraga, M., & Vodanovic Haklicka, A. (1939). *Curso de derecho civil: Basado en las explicaciones de los profesores de la Universidad de Chile Arturo Alessandri Rodríguez y Manuel Somarriva Undurraga* (Vol. 3). Editorial Nacimiento. <https://es.scribd.com/doc/36270257/Somarriva-M-Alessandri-A-Derecho-Civil-Obligaciones>
- Alzate Patiño, V. A., & Cotta Contreras, S. L. (2020). *Estándar internacional para las transferencias de datos personales, un camino por recorrer hacia la seguridad y confianza en los negocios y entornos digitales*. <https://bdigital.uexternado.edu.co/handle/001/3904>
- Asaithambi, S., Ravi, L., Devarajan, M., Almazyad, A. S., Xiong, G., & Mohamed, A. W. (2024). Enhancing enterprises trust mechanism through integrating blockchain technology into e-commerce platform for SMEs. *Egyptian Informatics Journal*, 25. <https://doi.org/10.1016/j.eij.2024.100444>
- Cabezas Azuero, J. S. (2023). Tratamiento de datos personales y compliance en Colombia. *Revista de la Facultad de Derecho y Ciencias Políticas*, 53(138), 1-25. <https://doi.org/10.18566/rfdcp.v53n138.a2>
- Casolari, F., Taddeo, M., Turillazzi, A., & Floridi, L. (2023). How to improve smart contracts in the European Union Data Act. *Digital Society*, 2, 9. <https://doi.org/10.1007/s44206-023-00038-2>
- Castro Ayala, J. G., & Calonje Londoño, N. X. (2015). *Derecho de obligaciones: Aproximación a la praxis y a la constitucionalización*. (1.a ed.). Universidad Católica de Colombia.
- Catchlove, P. (2017). Smart Contracts: A New Era of Contract Use (SSRN Scholarly Paper 3090226). <https://doi.org/10.2139/ssrn.3090226>
- Chub, D. V. (2019). Legal regulation of smart contracts in France. *Actual Problems of Russian Law*, 2019(8), 151-158. DOI:10.17803/1994-1471.2019.105.8.151-158

Clifford Chance. (2017). ¿ARE SMART CONTRACTS CONTRACTS?
<https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2017/08/are-smart-contracts-contracts.pdf>

Cole, G. M. (2019, mayo 1). The Long Convergence: «Smart Contracts» and the «Customization» of Commercial Law. *Southern California Law Review*.
<https://southerncalifornialawreview.com/2019/05/01/the-long-convergence-smart-contracts-and-the-customizationof-commercial-law-article-by-g-marcus-cole/>

Comisión Europea. (2021, junio 4). *La protección de datos en la UE* - Comisión Europea. La protección de datos en la UE - Comisión Europea. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es

Congreso de la Republica de Colombia (2012). *Ley 1581 de 2012*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Congreso de la Republica de Colombia (2008). Ley 1266 de 2008, Pub. L. No. *Ley 1266 de 2008* (2008). <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488>

Constitución Política de 1991.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125>

Corte Constitucional de Colombia (2022). *Sentencia T-450/22*. MP. Jorge Enrique Ibáñez Najjar.
<https://www.corteconstitucional.gov.co/Relatoria/2022/T-450-22.htm>

Corte Constitucional de Colombia (2021). *Sentencia SU 139/21*. MP. Jorge Enrique Ibáñez Najjar.
<https://www.corteconstitucional.gov.co/relatoria/2021/SU139-21.htm>

Corte Constitucional de Colombia (2015). *Sentencia C-219 de 2015*. MP. Mauricio González Cuervo. <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=63575>

Corte Constitucional de Colombia (2014). *Sentencia T-699-14*. MP. Mauricio González Cuervo.
<https://www.corteconstitucional.gov.co/relatoria/2014/T-699-14.htm>

Corte Constitucional de Colombia (2011). *Sentencia C-748/11*. MP. Jorge Ignacio Pretelt Chaljub.
<https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm>

Corte Constitucional de Colombia (2008). *Sentencia C-1011-08*. MP. Jaime Córdoba Triviño.
<https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm>

Corte Constitucional de Colombia (2001). *Sentencia C-831-01*. MP. Álvaro Tafur Galvis.
<https://www.corteconstitucional.gov.co/relatoria/2001/c-831-01.htm>

Corte Constitucional de Colombia (2000). *Sentencia C-662-00*. MP. Fabio Morón Díaz.
<https://www.corteconstitucional.gov.co/relatoria/2000/C-662-00.htm>

Cubillos Velandia, R., & Rincón Cárdenas, E. (2002). *Introducción Jurídica al Comercio Electrónico*. Ediciones Jurídicas Gustavo Ibáñez Ltda.

Decreto 1377 de 2013 (2013).
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646>

Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2015, noviembre 18). Blockchain/Step by Step Towards Creating a Safe Smart Contract.pdf at master · bellaj/Blockchain. GitHub.
<https://github.com/bellaj/Blockchain/blob/master/Step%20by%20Step%20Towards%20Creating%20a%20Safe%20Smart%20Contract.pdf>

Durovic, M., & Janssen, A. (2018). The Formation of Smart Contracts and Beyond: ¿Shaking the Fundamentals of Contract Law? https://www.researchgate.net/publication/327732779_The_Formation_of_Smart_Contracts_and_Beyond_Shaking_the_Fundamentals_of_Contract_Law

Espinoza Espinoza, J. (2011). El principio de la buena fe. 24. <https://doi.org/10.26439/advocatus2011.n024.3187>

(EU) 2016/679 of 2016, Pub. L. No. (EU) 2016/679 (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

Flores, M. E. (2023). Smart contracts y protección de datos personales. PAPELES del Centro de Investigaciones de la Facultad de Ciencias Jurídicas y Sociales de la UNL, 15(26). <https://bibliotecavirtual.unl.edu.ar/publicaciones/index.php/papeles/article/download/12809/17522/45201> Smart contracts y protección de datos personales

Flórez, G. D. (2014). La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial. *Verba Iuris*, 31, Article 31. <https://doi.org/10.18041/0121-3474/verbaiuris.31.54>

Furrer, A., & Müller, L. (2018). «*Functional equivalence*» of digital legal transactions. 2-4.

Guzmán Brito, A. (2001). Causa del Contrato y Causa de la Obligación en la Dogmática de los Juristas Romanos, Medievales Y Modernos Y En La Codificación Europea Y Americana. *Revista de estudios histórico-jurídicos*, 23, 209-367. <https://doi.org/10.4067/S0716-54552001002300006>

Heaver, I. (2023). The Ultimate Crypto Legal Guide To Structuring Your DAO. *Forbes*. <https://www.forbes.com/sites/irinaheaver/2023/08/14/the-ultimate-crypto-legal-guide-to-structuring-your-dao/>

Hernández, J. C. (2012, abril 20). La protección de datos personales en Internet y el habeas data. *Revista Derecho y Tecnología*, N°13/2012, 61-85.

Hesselink, M. (2011). The Concept of Good Faith (pp. 619-649). https://www.researchgate.net/publication/228218882_The_Concept_of_Good_Faith

Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, 29(5), 509-521. <https://doi.org/10.1016/j.clsr.2013.07.004>

Jiménez, W. G., & Meneses Quintana, O. (2023). Libertad de expresión en internet y redes sociales vs. Derechos a la intimidad y el buen nombre. Prevalencia, colisión y ponderación en el Derecho constitucional (1992-2019). *Revista Derecho del Estado*, 56, Article 56. <https://doi.org/10.18601/01229893.n56.10>

Lawton, G. (2025). Top smart contract platforms to consider. TechTarget. <https://www.techtarget.com/searchcio/tip/Top-smart-contract-platforms-to-consider>

Leefatt, S., & Cieplak, J. (2017, abril 26). “Smart Contracts”: A Smart Way to Automate Performance. *Georgetown Law Technology Review*. <https://georgetownlawtechreview.org/smart-contracts-a-smart-way-to-automate-performance/GLTR-04-2017/>

Levitina, A. (2023, septiembre 10). THE LEGAL IMPLICATIONS OF AI IN SOFTWARE DEVELOPMENT. *Logan & Partners*. <https://www.loganpartners.com/the-legal-implications-of-ai-in-software-development/>

López, F. H. T. (2012). La pretensión de nulidad de contratos civiles y mercantiles en Colombia. *Revista de Derecho Privado*, 23, Article 23.

Martínez Devia, A. (2019). La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? *Revista La Propiedad Inmaterial*, 27, 5-23. <https://doi.org/10.18601/16571959.n27.01>

Meier, O., & Sannajust, A. (2021). The Smart Contract Revolution A Solution For The Holdup Problem? *Small Business Economics*, 57(2), 1073-1088.

Miranda Guzmán, D. A. (2023, octubre 17). *Los Datos Personales y su regulación en Colombia (datos sensibles, datos públicos, semiprivado y privado): Enfoque, ámbito de aplicación y contenido*. Blog Jurídico - TECH. <https://telecomunicaciones.uexternado.edu.co/los-datos-personales-y-su-regulacion-en-colombia-datos-sensibles-datos-publicos-semiprivado-y-privado-enfoque-ambito-de-aplicacion-y-contenido-2/>

Monateri P. G. (2012) Methods in comparative law: An intellectual overview. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2151819.

Morales, L. y Pulgarín, N. (2022). *Smart contracts en materia de arrendamiento de vivienda urbana a partir de los artículos 1, 3 y 22 de la Ley 820 de 2003*. (Trabajo de grado, Unilasallista Corporación Universitaria). Unilasallista Repositorio Institucional. <https://repository.unilasallista.edu.co/server/api/core/bitstreams/d81d2d2e-3989-460d-b9b9-b014045f3745/content>

Muñoz Losada, J. C. (2020). El derecho al olvido en Colombia: Análisis doctrinal y jurisprudencial. *Revista Jurídica Piélagus*, 19(1). <https://doi.org/10.25054/16576799.2807>

NACIONES UNIDAS. (1980). Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (Viena, 1980) | Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. https://uncitral.un.org/es/texts/salegoods/conventions/sale_of_goods/cisg

Ni, J. (2024). Intelligent Contracts and the Principle of Contractual Freedom: A Classical Legal Examination in the Era of Emerging Technologies. *Frontiers in Business, Economics and Management*, 14(3), Article 3. <https://doi.org/10.54097/w0gxsm83>

OEA (2011) Principios y recomendaciones preliminares sobre la protección de datos (la protección de datos personales). Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos. http://www.oas.org/es/sla/ddi/docs/CP-CAJP-2921-10_rev1_corr1.pdf.

Oleksii Konashevich. (2017). The Concept of the Blockchain-Based Governing: Current Issues and General Vision. https://www.researchgate.net/profile/Yousef-Fortin-2/publication/317638956_A_New_Model_for_E-Government_in_Local_Level_Administrations/links/5945306fa6fdccb93ab86fe6/A-New-Model-for-E-Government-in-Local-Level-Administrations.pdf#page=96

Pastor, J. (2018) Qué es blockchain: La Explicación definitiva para la Tecnología Más de Moda, Xataka. <https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda>

Pérez, I. (2019, noviembre 3). *4 plataformas de contratos inteligentes que todo desarrollador de blockchains debe conocer*. *CriptoNoticias* - Noticias de Bitcoin, Ethereum y criptomonedas. <https://www.criptonoticias.com/analisis-investigacion/contratos-inteligentes-desarrollador-blockchain-rsk-ethereum-cardano-eosio/>

RAE. (2024). Dato | Diccionario de la lengua española. «Diccionario de la lengua española» - Edición del Tricentenario. <https://dle.rae.es/dato>

Raskin, M. (2016). The Law and Legality of Smart Contracts (SSRN *Scholarly Paper* 2959166). <https://doi.org/10.2139/ssrn.2842258>

Reed, C. (2007). Taking Sides on Technology Neutrality. *SCRIPT-Ed*, 4(3), 2-13. <https://doi.org/10.2966/scrip.040307.263>

Rengifo García, E. (1999). Comercio Electrónico, Documento Electrónico y Seguridad Jurídica. *Derecho Penal y Criminología*, 21(65), 151-172.

Rincón Cárdenas, E. (2006). *Manual de Derecho de Comercio Electrónico y de Internet*. Centro Editorial Universidad del Rosario.

Rincón Cárdenas, E., & Martínez Molano, V. (2022). *Contratos inteligentes y automatización como desarrollos aplicados del legaltech en Colombia*. *REVISTA DIREITO GV*, 18(1). <https://www.scielo.br/j/rdgv/a/qWGF349kYysjJtZdKnV3zTG/?format=pdf&lang=es>

Rojas Bejarano, M. (2014, mayo 27). *Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales*. *VLEX*, 8(1), 107-139.

Rojas Tamayo, D. M. (2018). *El derecho aplicable al contrato: Estudio comparado, crítico y prospectivo en derecho internacional privado colombiano*. 1, 152-160.

Sahai, A., & Pandey, R. (2020). Smart Contract Definition for Land Registry in Blockchain. 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Communication Systems and Network Technologies (CSNT), 2020 IEEE 9th International Conference on, 230-235. <https://doi.org/10.1109/CSNT48778.2020.9115752>

Salazar Bautista, R. L., & Galvis Cano, L. (2019). Alcance del derecho al olvido en el tratamiento de datos personales en Colombia. *Revista Verba Iuris*, 41, 45-63.

Sánchez Otálora, A. M. (2024). Marco jurídico para la implementación de Smart contracts en operaciones de compraventa internacional de inmuebles. https://doi.org/10.48713/10336_42849

SEON. (2023). *Los 10 mejores softwares de verificación de identidad en 2023*. SEON ES. <https://seon.io/es/recursos/comparaciones/software-de-verificacion-de-identidad/>

Superintendencia de Industria y Comercio. (2023). *Resolución 68753 de 2023*. <https://sedeelectronica.sic.gov.co/sites/default/files/normativa/RE68753-2023.pdf>

Superintendencia de Industria y Comercio. (2021). *Resolución 80305 de 2021*, Pub. L. No. Resolución 80305 de 2021 (2021). <https://www.sic.gov.co/sites/default/files/files/2021/RE80305-2021.pdf>

Superintendencia de Industria y Comercio. (2021). *Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales*. <https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf>

Superintendencia de Industria y Comercio. (2021). *Resolución 78711 de 2021*. <https://www.sic.gov.co/sites/default/files/files/2021/RE78711-2021.pdf>

Superintendencia de Industria y Comercio. (2019). *Resolución 76538 de 2019*. <https://www.sic.gov.co/sites/default/files/boletin-juridico/Res%2076538%20del%2027XII2019%20Aseg%C3%BArate%20F%C3%A1cil%20Ltda.pdf>

Superintendencia de Industria y Comercio. (2019). *Resolución 2908 de 2019*, Pub. L. No. Resolución 2908 de 2019 (2019). [https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE2908-2019\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE2908-2019(1).pdf)

Superintendencia de Industria y Comercio. (2018). *Radicación: 18- 233185-2*. <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/ConceptosJuridicos/descargas/18/18233185>

Superintendencia de Industria y Comercio. (2017). *Radicación: 17-277107-3*. <https://www.sic.gov.co/sites/default/files/files/Boletin-juridico/2017/17277107TransferenciaINterDatos.PDF>

Sullivan, C. & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review*, 33(4), 470-481. <https://doi.org/10.1016/j.clsr.2017.03.016>

Unión Europea. (2016). Artículo 4 UE Reglamento general de protección de datos [Text]. *SecureDataService*. <https://www.privacy-regulation.eu/es/4.htm>

Unión Europea. (2022). *Protección de Datos conforme al reglamento RGPD*. Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Unión Europea (2025) Tipos de Legislación: Unión Europea, Unión Europea: Tipos de legislación. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_es

Veerpalu, A. (2019). Functional Equivalence: An Exploration Through Shortcomings to Solutions. *Baltic Journal of Law & Politics*, 12, 21-23. <https://doi.org/10.2478/bjlp-2019-0015>

Veuger, J (2020). Blockchain: kantelpunt in de vastgoedsector. *Technologie*. https://research.hanze.nl/ws/portalfiles/portal/16542880/Jan_Veuger_Blockchain_5245_.pdf

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.-Y. (2019). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(11), Article 11. <https://doi.org/10.1109/TSMC.2019.2895123>

Werbach, K., & Cornell, N. (Eds.). (2021). *Smart Contracts: Technological, Business and Legal Perspectives*. *Hart Publishing*. <https://doi.org/10.5040/9781509937059>