Introducción

El último siglo de la historia de la humanidad ha sido impactado por grandes cambios en la economía, las industrias, el consumo y el intercambio de bienes y servicios; los historiadores advierten el suceso de al menos tres revoluciones industriales (Chaves, 2004) (Rifkin, 2011) y algunos autores como Schwab (2016) incluso afirman que estamos ante una cuarta revolución industrial o una segunda era de las máquinas.

La tercera revolución industrial tuvo sus inicios a mediados de 1960 y estuvo caracterizada por el desarrollo de las telecomunicaciones, los avances en energías renovables y en especial, por las tecnologías de la información como internet (Rifkin, 2011). De acuerdo con Schwab (2016), hoy la sociedad se encuentra en los albores de una cuarta revolución industrial, con desarrollo en campos como: la robótica, la inteligencia artificial, la nanotecnología, la computación cuántica, la impresión 3D, los vehículos autónomos, el internet de las cosas, las cadenas de bloques, las criptomonedas, los contratos inteligentes, entre otros; todos estos desarrollos tecnológicos han impactado la forma

como la sociedad funciona y se interrelaciona; la diferencia entre la esfera física y digital es cada vez más difusa, pues las personas tienden a relacionarse de maneras digitales o mediante la utilización de nuevas tecnologías que implican modificación de hábitos de conducta que incluso conllevan a cuestionamientos sobre si existe una verdadera diferencia entre la realidad y la realidad virtual (García, 2002).

Evidentemente, el derecho no resulta ajeno al desarrollo y uso de las nuevas tecnologías. Todas las ramas y subramas de la ciencia jurídica han resultado implicadas, en mayor o menor medida, a problemáticas relacionadas con estas, puesto que el uso masivo de las aplicaciones tecnológicas muchas veces ha vulnerado tanto al derecho objetivo como a los derechos subjetivos de los ciudadanos, algo que ha inquietado a la doctrina jurídica. En efecto, una gran parte de las nuevas tecnologías, en especial las tecnologías de la información y las telecomunicaciones, son usadas de manera masiva y a diario porque brindan soluciones a cuestiones prácticas de la vida cotidiana; sin embargo, la totalidad de sus efectos no siempre son deseados.

La dialéctica que se genera en torno a los beneficios y perjuicios de las TIC es notoria en tecnologías como internet, la telefonía móvil, las cámaras integradas de video, las redes sociales, etcétera. Por un lado, su desarrollo ha permitido lograr una comunicación instantánea entre personas sin importar su ubicación geográfica; por otro lado, también han provocado la afectación de derechos tan importantes como a la pri-

vacidad, intimidad, buen nombre, información certera, entre otros.

Entonces, reconociendo la importancia del derecho como técnica social para la regulación de las conductas humanas, en este libro se realizará un análisis jurídico sobre los denominados *contratos inteligentes*, los cuales preliminarmente pueden definirse como protocolos computacionales que aseguran la ejecución de prestaciones de manera automática, reduciendo los riesgos de incumplimiento de las partes, anulando la intermediación de terceros (Bit2me Academy, 2016) y garantizando la seguridad suficiente para impedir que los extremos de un contrato modifiquen arbitrariamente las cláusulas desfavorables o impidan la ejecución de las prestaciones incómodas. Lo significativo del estudio reside en que este nuevo desarrollo ha sido considerado tan importante que algunos predicen que esta tecnología transformará la economía global, reinventará los sistemas financieros, reformará los modelos empresariales y creará nuevos modelos de negocios; todo esto a través de modelos de inclusión social y económica que, a su vez, permitirán reconstruir el Estado y la democracia (Tapscott y Tapscott, 2016).

Además del entusiasmo que han provocado los contratos inteligentes, estos también han incitado muchas inquietudes, sobre todo para el derecho. Si bien su aplicación promete revolucionar las relaciones de los sectores industriales modernos y las relaciones entre particulares, también ha generado cues-

tionamientos sobre su validez, naturaleza jurídica, libertad negocial, disciplina normativa, coherencia con el derecho privado, interpretación y posibilidad de revisión judicial, entre otros temas que requieren respuesta por parte de la doctrina jurídica.

Es útil y necesario el estudio contenido en el presente libro, porque solo en la medida que se logre un entendimiento sobre las implicaciones jurídicas de los contratos inteligentes, se podrán resolver las inquietudes de los usuarios actuales y potenciales de estas nuevas tecnologías, lo cual es necesario para lograr su escalabilidad y amplia usabilidad.

Ahora, si bien los cuestionamientos de tipo jurídico son vastos y variados, el presente texto no pretende abarcarlos todos, sino que se centra en la descripción de las características y funcionalidades técnicas de los contratos inteligentes y cómo opera la autonomía de la voluntad negocial en cuanto a la libertad contractual frente este tipo de contrato, es decir, aquella que se desarrolla en el ámbito de un ordenamiento jurídico concreto y que "permite a las partes crear normas sustanciales que constituirán el contenido del contrato" (Guerrero, 2014).

En el mismo sentido, si bien el presente libro trata como tema de estudio los contratos inteligentes, los cuales son un fenómeno global, debe aclararse que a pesar de que se reflexionará sobre algunos sistemas jurídicos extranjeros, no se realizará un análisis de derecho comparado ni de derecho internacional. Este trabajo se limitará a hacer un análisis jurídico

de estos contratos únicamente desde ordenamiento jurídico colombiano y sus instituciones, así que, en consecuencia, no se abordarán cuestiones como, por ejemplo, la autonomía de la voluntad conflictual o el orden público internacional.

En suma, la presente obra describirá los límites que tiene la autonomía privada en cuanto a la celebración y ejecución de los contratos inteligentes bajo el amparo del ordenamiento jurídico colombiano y para esto se describirán las características técnicas y funcionales de dichos contratos, se establecerá su naturaleza jurídica y se determinará el alcance y los límites de la autonomía privada en la celebración y ejecución de estos en el derecho colombiano.

Características tecnológicas y jurídicas de los contratos inteligentes

Dimensión tecnológica de los contratos inteligentes

Historia y desarrollo de las bases tecnológicas de los contratos inteligentes

Los contratos inteligentes (en inglés *smart contracts*) constituyen otro logro en el desarrollo de las tecnologías de la información y las telecomunicaciones. Las bases en las cuales se fundamenta este nuevo adelanto tecnológico como el internet, las redes P2P, la criptografía asimétrica y los algoritmos de consenso tienen muchos años de desarrollo científico y han dado soluciones prácticas a la vida en sociedad.

Hoy día, los contratos inteligentes constituyen una oportunidad para viabilizar el desarrollo adaptativo del comercio distribuido, el internet de las cosas *(Internet of Things)*, las organizaciones descentralizadas autónomas (*Descentralized Autonomous Organizations,* DAO), los registros distribuidos, entre otros, que permitirán el progreso de las

industrias a otra escala (Tapscott y Tapscott, 2016). No obstante, nada de esto fuese posible sin el previo desarrollo de las tecnologías que le preceden, como la computación y el internet.

Antes que el internet emergiera y fuese conocido, ya el mundo de la computación llevaba siglos de desarrollo. Desde el 2700 a. C. ya existían herramientas para sumar y restar como el ábaco; en el 830 se desarrolló la teoría del algoritmo; en 1642 Blaise Pascal inventó la pascalina, una máquina para sumar; en 1841 Ada Lovelace trabajó en el primer algoritmo para máquinas; en 1936 Alan Turing expuso los conceptos de algoritmo y de la máquina de Turing; en 1938 se desarrolla la Z1, la primera máquina realmente considerada como computadora; en 1944 se construyeron en Inglaterra los computadores Colossus Mark I y Colossus Mark 2 para descifrar los mensajes cifrados de los alemanes en la Segunda Guerra Mundial; en 1946 se puso en funcionamiento la ENIAC, que fue la primera computadora electrónica de propósito general, y en 1953 IBM fabricó la primera computadora a escala industrial. A pesar de todo el desarrollo histórico computacional, las computadoras individualmente consideradas no dejaron de ser una isla de procesamiento autónomo, pues, aunque podían realizar infinitud de cálculos, no tenían la capacidad de compartir información, datos y cálculos con otras computadoras (Sánchez, 2018).

Lo anterior cambió en 1964, cuando investigadores de la corporación estadounidense RAND descu-

brieron la forma de enviar y recibir paquetes de datos entre dos computadoras distintas, lo cual fue el insumo fundamental para que la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de Estados Unidos de América lograra desarrollar los proyectos ARPANET y DARPANET en 1969, las primeras redes de ordenadores que, cuando se separó la parte militar de la civil en 1983, se conocería como internet (Millán, 1999).

La criptografía asimétrica y las firmas digitales. El término *criptografía* proviene del griego *kryptós-graphé* y significa 'escritura oculta'. La criptografía consiste en una serie de técnicas para proteger los datos e impedir que terceros no autorizados puedan acceder a información o alterarla para su propio beneficio o en perjuicio de otros (Bit2Me Academy, 2018a).

La invención de la criptografía no es reciente, las personas han utilizado diferentes herramientas para proteger la información desde hace miles de años. Un ejemplo de criptografía antigua es el denominado *cifrado César*, método utilizado por el emperador romano Julio César cuando enviaba información delicada que quería mantener confidencial; esta técnica consistía en remplazar cada letra del mensaje con una letra diferente del alfabeto separada por un número particular de letras (Gates, 2017). La criptografía moderna, aunque conserva los mismos fundamentos, es distinta y su desarrollo se encuentra integrado en la ciencia de la computación, ya que luego del desarrollo de internet, nuevos algoritmos criptográficos fue-

ron creados para proteger la información en el intercambio de mensajes y archivos en la red (De Filippi y Wright, 2018).

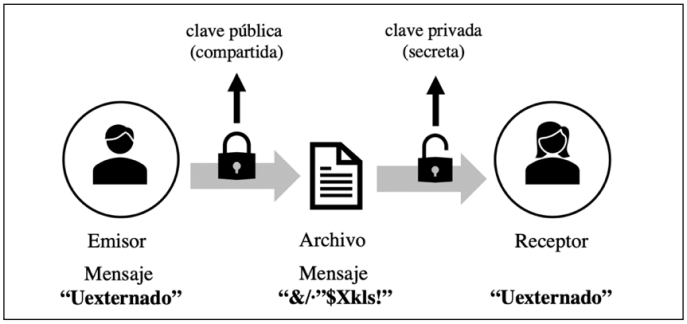
Uno de los grandes avances de la criptografía moderna fue el desarrollo de la criptografía asimétrica de autenticación de dos claves, una pública y una privada. Fue desarrollada en 1976 por Whitfield Diffie y Marty Hellman, dos criptógrafos de la Universidad de Stanford, quienes, con su invención, permitieron una distribución segura de claves en la red y establecieron las bases teóricas para las actuales firmas digitales autenticadas. De manera previa a este desarrollo, el envío y recepción de información era mucho más vulnerable a ser interceptado y decodificado por terceros. Además, con este tipo de criptografía se logró mantener un anonimato de las partes (De Filippi y Wright, 2018).

La forma como funciona es que la clave pública sirve como un punto de referencia para el envío de la información (como una dirección pública), mientras que la clave privada es una especie de contraseña única que solo conoce el receptor del mensaje; aunque, en estricto sentido, estos simplemente son códigos alfanuméricos que están integrados en los datos de la información que se envía y recibe.

Una analogía para entender la criptografía asimétrica es el buzón de correo físico que se encuentra asegurado con un candado, pues el remitente coloca la dirección del correo físico (clave pública), mientras que el destinatario es el único que tiene la llave (clave

privada) para abrir el correo. Con esto se asegura que el mensaje llegue únicamente al destinatario correcto y que este sea el único que pueda abrir el mensaje. Lo anterior puede apreciarse en la figura 1.

Figura 1. Funcionamiento del cifrado con clave pública y clave privada



Fuente: Elaboración propia.

Con un cifrado asimétrico, si un Receptor X quiere recibir un mensaje confidencial de un Emisor Y, primero, deberá compartirle la clave pública (que será como su dirección de autenticación) que estará configurada con su clave privada; luego, podrá abrir el mensaje con su clave privada.

Por tanto, si alguien intercepta el mensaje, podrá solo ver la clave pública, pero no podrá abrir el mensaje porque necesita la clave privada que solo tiene el Receptor, lo cual hace que este tipo de cifrado sea prácticamente imposible de vulnerar, debido a que "este tipo de sistemas criptográficos usa algoritmos